Skyscraper Project

version: May 12, 2023

Compiler: Hao Peng(彭淏)
hao_peng@mit.edu

Peking University
Massachusetts Institute of Technology

Preface

What is this? : At first, this is a note containing subtle or important materials I encountered while studying. I started this project in the fall of my third undergraduate year(October 2019) in Peking University, noticing that I have a poor memory and consistently forget what I thought I have already learned. So it came to me that I can compile all the proofs of theorems I cannot recall that is hard and subtle yet appearing over and over again. But gradually it turns out I want to make it as comprehensive as possible. A more accurate description of this note now is: this is a more self-contained introduction to modern(post-Grothendieck) pure mathematics that I care about.

I constantly add stuff to this note, and I regularly put them online. You can find the newest version released at `https://math.mit.edu/~hao_peng/skyscraper.pdf`. Don't be surprised to find many sections containing only titles, and the symbol "**?**" means "further work required here". If you find errors or have suggestions, please feel free to email me.

Constitutions: The following are principles of the structure of this note, but the current version is far from it. They serve as ultimate goals.

- This note should be self-contained.
- Notations should be consistent throughout the whole note.
- Propositions should be put in the (sub)section of the most advanced term appeared in the statement, or as a corollary.
- Logical order is not necessary, but vicious circles are intolerable. Although it should also be properly ordered logically in the sense that if every notion appearing is referred to its definition, the ordering has the least number of reverse cross-references(i.e. referring to definitions after it) under admissible permutation, where admissible permutation means a permutation that preserves the tree structure of this note(i.e. the tree of chapter-section-subsection-$\cdots$ ordering).
- Theories should be stated at the most generality. There's no need to give proofs for the special case but clarify the deduction from the general case, unless it is needed in the proof of the general case, then state it as a lemma.
- When facing multiple proofs, only the most elegant and essential proof should be recorded.
- References should be traced to the original author and his specific paper.
- Each section should contain less than 30 pages. Each chapter should contain less than 20 sections.

Writing Styles: The following are writing standards of this note. References are [CMOS] and [Poo]. Notice some rules of [Poo] remain to be discussed.

- Use less words and more math symbols and equations, and use plain English, so that even those who don't speak English can understand without much effort.
- Use proper cases for names of people.

- A proposition is a proven mathematical sentence.
- A theorem is a proposition of notable importance.
- A lemma is a proposition whose importance is derived from the theorem or proposition it aims to prove.
- A corollary is a proposition whose proof readily follows from its corresponding proposition or theorem.
- A conjecture is a mathematical sentence whose proof(or disproof/proof of independence) is unknown yet.
- A conjectural corollary is a mathematical sentence which is implied by the corresponding conjecture.
- A theorem & conjectural corollary is a proven mathematical sentence which can be implied by the corresponding conjecture.
- The naming of lemmas/propositions/theorems/conjectures by multiple authors follows the lexicographical order, except for historical followup works. Authors of the same paper is connected by "-" symbol, and authors of different papers are separated by a "/" symbol.
- A remark is a comment, and the book can be read independent of the remarks.(much like remarks in any programming language).

Tips: This is hardly a *readable* note. I use it as a dictionary. It only contains materials that I'm interested in and many proofs are still missing. Hopefully I can complete them later. The main reason why I have to latex all these materials together is that I need tons of cross-references. So I believe it's the best way to read this book digitally, and it's good to know how to go forwards and backwards between hyper-references on your computer. For example, on a MacOS system, the default shortcuts are ⌘+[, ⌘+] for Preview and ⌥+←, ⌥+→ for Foxit Reader. Foxit Reader is stable when handling a large file.

Acknowledgement: Sincere thanks to Yi Tian(田翊) for answering my questions when I was learning algebraic geometry and p-adic geometry in year 2020 when I was in Peking University. His help is fundamental. Thanks to Zhiyu Zhang(张志宇) for giving me directions on mathematical study and advices on mathematical life in year 2022 when I was in MIT.

There is already a great online book [Sta] maintained by de Jong that covers considerably much of the Algebraic Geometry part of this note. I haven't finish reading it but I reordered the materials that I learnt and kept track of it in my own way. I sometimes used different paths to optimize the proof. The idea to compile this note was inspired by [Sta]. One different feature of this note compared to [Sta] is that I want to make every proof as optimal and as general as possible(See Constitutions above). Any suggestion to optimize proofs or generalize statements is strongly encouraged.

The writing style of this note is imitating and influenced by various literature, including beautiful writings of J. S. Milne, especially [Mil17][Mil17d] and [Mil08], monographs of J. Lurie, especially [Lur09] and [Lur11], and also de Jong's magnificent [Sta].

In arranging the contents of this note, I consulted the AMS classification(newest version from mathscinet.ams.org).

Copyright Issue: It should be made clear that I took proofs from many different places, so only a tiny fraction of this note should be considered originated from me. I am currently too busy being a graduate student, so many references are still missing. Tell me if you think I should cite you or somebody's work. Nevertheless, I hope this note can contribute to my study and help anyone who read it. But it comes with no warranty, please use at your own risk.

Addendum March 25 2022: Recently voices are increasing asserting that it is impossible for anyone be sure of every detail of the propositions he used, and everyone has to write assertions he hasn't checked. I don't agree with this. I started to get in touch with V. Voevodsky's idea of machine-assisted proofs and type-theory. And I noticed this book becoming more like programming code inadvertently. Also I'm keeping an eye on Lean-formalized mathematics. With the releasing of ChatGPT4 last week, the future is both exalting and challenging.

Addendum March 27 2022: Today I watched Buzzard's ICM2022 talk, and this is the first time I heard of the Lean project. I am astonished to learn that the Lean project and this book share similar goals. Also, what I am writing is in fact similar to type theory based rather than set theory based. And my notes are more like Mizar. But they also differ in several ways: This book put more priority in succinctness, and proofs are only written to the degree that I can check back. I don't need absolute check of rigor. But inspired by those, I made some changes to the note to make it more like a 'pseudocode'.

"And they said, Go to, let us build us a city and a tower, whose top may reach unto heaven; and let us make us a name, lest we be scattered abroad upon the face of the whole earth."

–Genesis 11:1-9

Table of Contents

Chapter 15 – Arithmetic Geometry

Chapter 26 – Experimental Physics

Chapter 27 – Non-Commutative Geometry(Connes)

Chapter 28 – Others

Chapter – Notations

Chapter – References

Chapter – Index

1 Logics

1.1 Underlying Logics for this book

1 Philosophical Issue

References are https://us.metamath.org/mpeuni/mmset.html.

Remark (1.1.1.1). This section is not mathematics. All other sections are mathematics, and logical issues will not occur(except possibly in comments). ⌟

2 Logical Fundations

We stick to the formalism point of view that mathematics is a game of symbols with no intrinsic meaning. And this book is a possible way the game is played, and record what we have done with mathematics in a digital form. Our point of view is most similar to that of Metamath:https://us.metamath.org/mpeuni/mmset.html.

The game has a rule to label strings of symbols(given below2), and our task is to find more and more strings of symbols labeled "LEGAL", and for a given string of symbols, determine if we can label it "LEGAL".

As humans, we observe interesting patterns in these "meaningless" symbol strings as they evolve from the axioms, and we attach meaning to them. One example is the set of natural numbers, whose properties match those we observe when we count everyday objects. "2" is a set, more precisely an abbreviation of a string of symbols. So "2" can never be the two apple sitting in front of you, it just behave like those two apples, because we deliberately designed it to be.

Primitive Notions:

In essence, this book has no meaning at all, unless you attach meaning to it. And you can never truly understand what is a "set" by studying set theory. This is unavoidable, by the existence of "primitive notions".

The primitive notion we choose is the notion of "**symbols**". Alphabets in any human language is a symbol. And "(", ")", " $\implies$ ", "$\wedge$", "$\varnothing$", "$\neg$", "$=$","$\in$" and "$\forall$" are all symbols, called **connectives**.

Rules(Axioms):

There are three families of rules to label strings of symbols.

- **Propositional calculus axioms with equality**:
  - (Constant variables:)"const: $\varnothing$" can be labeled "LEGAL".

- (Inference Rules:)If φ, ψ are strings of symbols, and
  - "wff: φ" and "wff: ψ" are labeled "LEGAL".
  - "φ" and "$\varphi \to \psi$" are labeled "LEGAL".

  Then ψ can also be labeled "LEGAL".
- (Axiom for $\wedge$:)If φ, ψ are strings of symbols, then

$$\Big((\varphi \wedge \psi) \to \neg(\varphi \to \neg\psi)\Big)$$

  and

$$\Big(\neg(\varphi \to \neg\psi) \to (\varphi \wedge \psi)\Big)$$

  can be labeled "LEGAL".
- (Well-defined formulas:)
  - If x is a string of symbols, then

$$\text{wff: (const: } x)$$

    and

$$\text{wff: (var: } x)$$

    and

$$\text{wff: (wff: } x)$$

    can be labeled "LEGAL".
  - If x, y are strings of symbols, then

$$\bigg(\Big((\text{var: } x) \wedge (\text{var: } y)\Big) \to \Big((\text{wff: } x = y) \wedge (\text{wff: } x \in y)\Big)\bigg)$$

    can be labeled "LEGAL".
  - If φ, ψ are strings of symbols, then

$$\bigg((\text{wff: } \varphi) \to \Big(\text{wff: } (\neg\varphi)\Big)\bigg)$$

    and

$$\bigg(\Big((\text{wff: } \varphi) \wedge (\text{wff: } \psi)\Big) \to \Big(\text{wff: } (\varphi \implies \psi)\Big)\bigg)$$

    can be labeled "LEGAL".
- (Axioms of simplification:)If φ, ψ are strings of symbols, then

$$\bigg(\Big((\text{wff: } \varphi) \wedge (\text{wff: } \psi)\Big) \to \Big(\varphi \implies (\psi \implies \varphi)\Big)\bigg)$$

  can be labeled "LEGAL".
- (Axiom Frege:)If φ, ψ, χ are strings of symbols, then

$$\bigg(\Big((\text{wff: } \varphi) \wedge (\text{wff: } \psi) \wedge (\text{wff: } \eta)\Big) \to \Big((\varphi \implies (\psi \implies \eta)) \implies ((\varphi \implies \psi) \implies (\varphi \implies \eta))\Big)\bigg)$$

  can be labeled "LEGAL".

- (Axiom transpose:)If φ, ψ are strings of symbols, then

$$\Big(\Big((\text{wff: } \varphi) \wedge (\text{wff: } \psi)\Big) \to \Big((\neg\varphi \implies \neg\psi) \implies (\psi \implies \varphi)\Big)\Big)$$

  can also be labeled "LEGAL".

- (Axiom modus ponens:)If φ, ψ are strings of symbols, then

$$\Big(\Big((\text{wff: } \varphi) \wedge (\text{wff: } \psi) \wedge \varphi \wedge (\varphi \to \psi)\Big) \to \psi\Big)$$

  can be labeled "LEGAL".

- (Axiom of equality:)If x, y, z are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{var: } y) \wedge (\text{var: } z)\Big) \to \Big((x = y) \implies ((x = z) \implies (y = z))\Big)\Big)$$

  can be labeled "LEGAL".

- (Axiom of Substitution:)

- **Predicate calculus axioms with equality**:

  - If x, φ, ψ are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{wff: } \varphi) \wedge (\text{wff: } \psi)\Big) \to (\text{wff: } ((\forall x)\varphi)\Big)\Big)$$

    can be labeled "LEGAL".

  - (Axiom of generalization:)If x, φ are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{wff: } \varphi)\Big) \to \Big(\varphi \implies ((\forall x)\varphi)\Big)\Big)$$

    can be labeled "LEGAL".

  - (Axiom of quantified implication:)If x, φ, ψ are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{wff: } \varphi) \wedge (\text{wff: } \psi)\Big) \to \Big(((\forall x)(\varphi \to \psi)) \to ((\forall x)\varphi \to (\forall x)\psi)\Big)\Big)$$

    can be labeled "LEGAL".

  - (Axiom of distinctness:)

    * If x, y are strings of symbols, then

$$\Big((\text{var: } x) \to \Big(\text{wff: } (\text{distin: } (x, y))\Big)\Big)$$

      can be labeled "LEGAL".

∗ If x, y, z are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{distin: } (x, y)) \wedge (\text{distin: } (x, z))\Big) \rightarrow \Big(\text{distin: } (x, (y = z))\Big)\Big)$$

and

$$\Big(\Big((\text{var: } x) \wedge (\text{distin: } (x, y)) \wedge (\text{distin: } (x, z))\Big) \rightarrow \Big(\text{distin: } (x, (y \in z))\Big)\Big)$$

can be labeled "LEGAL".

∗ If x, y are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{distin: } (x, y))\Big) \rightarrow \Big(\text{distin: } (x, (\text{const: } y))\Big)\Big)$$

and

$$\Big(\Big((\text{var: } x) \wedge (\text{distin: } (x, y))\Big) \rightarrow \Big(\text{distin: } (x, (\text{var: } y))\Big)\Big)$$

and

$$\Big(\Big((\text{var: } x) \wedge (\text{distin: } (x, y))\Big) \rightarrow \Big(\text{distin: } (x, (\text{wff: } y))\Big)\Big)$$

can be labeled "LEGAL".

∗ If x, φ are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{distin: } (x, \varphi))\Big) \rightarrow \Big(\text{distin: } (x, (\neg\varphi))\Big)\Big)$$

can be labeled "LEGAL".

∗ If x, φ, ψ are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{distin: } (x, \varphi)) \wedge (\text{distin: } (x, \psi))\Big) \rightarrow \Big(\text{distin: } (x, (\varphi \rightarrow \psi))\Big)\Big)$$

can be labeled "LEGAL".

∗ If x, y, φ are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{dist: } (x, y)) \wedge (\text{distin: } (x, \varphi))\Big) \rightarrow \Big(\text{distin: } (x, ((\forall y)\varphi))\Big)\Big)$$

can be labeled "LEGAL".

∗ If x, φ are strings of symbols, then and φ are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{wff: } \varphi) \wedge (\text{distin: } (x, \varphi))\Big) \rightarrow \Big(\varphi \rightarrow ((\forall x)\varphi)\Big)\Big)$$

can be labeled "LEGAL".

- **Set theory axioms(TG)**:

– (Axiom of Existence:)If x, y are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{var: } y)\Big) \rightarrow \Big(\neg(\forall x)(\neg(x = y))\Big)\Big)$$

can be labeled "LEGAL".

– (Axiom of left equality:)If x, y, z are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{var: } y) \wedge (\text{var: } z)\Big) \rightarrow \Big((x = y) \implies ((x \in z) \implies (y \in z))\Big)\Big)$$

can be labeled "LEGAL".

– (Axiom of right equality:)If x, y, z are strings of symbols, then

$$\Big(\Big((\text{var: } x) \wedge (\text{var: } y) \wedge (\text{var: } z)\Big) \rightarrow \Big((x = y) \implies ((z \in x) \implies (z \in y))\Big)\Big)$$

can be labeled "LEGAL".

– (Tarski-Grothendieck Axiom:)

You may noticed the strings of symbols that we have labeled "LEGAL" have something in common, i.e. you can see they are 'well-formed formulas', a notion which I didn't define.

Abbreviations and definitions:

When doing mathematics, an **abbreviation** is just a new axiom. For example, the sentence

"$(\varphi \iff \psi)$" is an abbreviation for "$((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi))$"

is just suggesting adding the axiom

$$\Big(\Big((\varphi \iff \psi) \rightarrow ((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi))\Big) \wedge \Big(((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)) \rightarrow (\varphi \iff \psi)\Big)\Big).$$

A **definition** is an assertion of a variable followed by an abbreviation, used to save space. All theorems using this definition can be reduced to wffs, where the defined new string disappears.

For example, the sentence "the power set of a set X is defined to be the set of all subsets of X" is just suggesting adding the axioms

$$\text{var: (the power set of } X)$$

and

$$\mathscr{M}(\text{the power set of } X)$$

and

$$\Big(y \in (\text{the power set of } X)\Big) \iff (y \subset X).$$

Notice adding definition may make the axioms inconsistent. Thus whenever we use definitions, we need to make sure that definitions names are different.

Whenever we substitute abbreviates, we will use $\overset{\text{subst}}{\iff}$.

3 Other Choice of Foundations

Instead of using the foundations given by ZFC+TG, we can also change it to either

- A family of type theory axioms with equality as the only primitive notions, as in HOL Light, or
- A family of calculus of inductive constructions axioms, as in Coq or Lean.

I haven't try these, but may change the setup in the future.

4 Proofs

A Sample Proof:

2 Mathematical Logic and Computer Science

2.1 Mathematical Logic

References are [Logic for mathematicians, Hamilton], [Axiomatic Set Theory] and [Mathematical Logic, Mendelson]. We mostly follow Mendelson's approach.

Notation (2.1.0.1).

- Beginning this section, we will be talking doing mathematics obeying the rules stated in 2. Our task is to write and only write strings of symbols and label them "LEGAL". Our writing style is most similar to that of Mizarhttp://mizar.org.
- You may see definitions like propositional calculus/predicate calculus which already appeared in the former section, REMEMBER: this has nothing to do with them, and only can be seen as a formal representation of them. The things in the last section belongs to real world, and the things in this section and all the following belongs to this game called "mathematics"(If you are drawing papers on a paper, what you draw are not real papers). Of course you can argue truth can be learned about the real world by doing this "game", but that depends on you attaching meaning to it.(This point has already been illustrated in the last section.)
- Don't worry, you can still prove that the axiom of choice is independent with the ZF system by giving a model, essentially the same way proving that the Euclid's fifth axiom is independent of the other four(in the frame of propositional calculus axioms and predicate calculus axioms, of course, everything is happening in the "game").

⌟

1 Peano's Postulates for Natural Numbers

After settling Philosophical Issue, I can start expressing now. In fact, I already started when I am explaining philosophical issue to you.

the Primordial Systems

Def. (2.1.1.1) [the Primordial Languages]. The **primordial language** $\mathcal{L}_0$ consists of

- **free variable symbols** a, b, c, d, m, n.
- **bound variable symbols** x, y, z, w.
- **constant variable symbol** 0.
- **function symbols** $S, +, \cdot,$

- **predicate symbols** $=$.
- **punctuations symbols** "(", "...". ")".
- **connective symbols** $\neg$ and $\implies$.
- **quantifier symbol** $\forall$.

⌟

Def. (2.1.1.2) [the (Blank)Peano Arithmetic system]. The (blank)**Peano arithmetic system** PA consists of the following data:

- the primordial language $\mathcal{L}$(2.1.1.1).
- A procedure called a **grammer** to specify which thing are called **well-formed formulas**(wffs):
  - There is a procedure to specify which things are called **terms**:
    * 0 and free variable symbols are terms.
    * If t, s are terms, then $S(t), (t+s), t \cdot s$ are terms.
  - There is a procedure to specify which things are called **atomic formulas**: If t, s are terms, then $t = s$ is an atomic formula.
  - The procedure to determine wffs:
    * Atomic formulas are wffs.
    * if φ, ψ are wffs and x is a bound variable not appearing in φ, then $\neg\varphi, (\varphi \implies \psi), (\forall x)\varphi(x/a)$ are wffs, where $\varphi(x/a)$ is obtained from φ by replacing each occurrence of some free variable a by a bound variable x that doesn't appear in φ.
- A procedure to specify which well-formed formulas are called **axioms**: The following are axioms:
  - Logical Axioms: If φ, ψ, η are wffs,
    * $(\varphi \implies (\psi \implies \varphi))$.
    * $((\varphi \implies (\psi \implies \eta)) \implies ((\varphi \implies \psi) \implies (\varphi \implies \eta)))$.
    * $((\neg\varphi \implies \neg\psi) \implies (\psi \implies \varphi))$.
    * $(\varphi \implies (\psi \implies \varphi))$.
    * $(\varphi \implies (\psi \implies \eta)) \implies ((\varphi \implies \psi) \implies (\varphi \implies \eta))$.
    * $((\neg\varphi \implies \neg\psi) \implies (\psi \implies \varphi))$.
    * $((\forall x)\varphi \implies \varphi(a/x))$ where $\varphi(a/x)$ is obtained from φ by replacing each occurrence of the bound variable x in $\varphi(x)$ by the free variable a.
    * $((\forall x)(\varphi \implies \psi) \implies (\varphi \implies (\forall x)\psi))$, if the free variable a in φ which are quantifying with x doesn't appear.
    * (Modus Ponuns or MP)$\varphi \wedge (\varphi \implies \psi) \to \psi$.
    * (Generalizations)$\varphi \to (\forall x)\varphi(x/a)$, where x is a bound variable symbol that doesn't appear in φ, and $\varphi(a/x)$ is obtained from φ by replacing each occurrence of some free variable a by x.
  - Non-Logical Axioms: If a, b, c are any free variables, x, y, z are any bound variables and φ a wff., then
    * $(a = b) \implies ((a = c) \implies (b = c))$.
    * $(a = b) \implies (S(a) = S(b))$.
    * $\neg(0 = S(a))$.

* $(S(a) = S(b)) \implies (a = b)$.
* $(a + 0) = a$.
* $a + S(b) = S(a + b)$.
* $a \cdot 0 = 0$.
* $a \cdot S(b) = a \cdot b + b$.
* (Principle of mathematical induction) $\varphi(0/a) \implies ((\forall x)(\varphi(x/a) \implies \varphi(S(x)/a)) \implies (\forall x)\varphi(x))$.

terms in the Peano arithmetic system will be called **natural numbers**. ⌟

Remark (2.1.1.3) [Metaphysical Issue].

- From now any definition/proposition/rem we make should be regarded as wffs in a formal sufficiently high order system containing the blank PA system(2.1.1.2) and the class system to be defined in(2.1.3.2) and we can quantify over any other systems. In other words, I assume will can comprehend everything in this book. Such a language is called a **metasystem** for it. The symbols in this metalanguage is called a **metavariable**.
- I assume it has an axiom which is a stronger form of the mathematical induction(2.1.1.2)(i.e. Induction can apply to properties of classes).
- If you don't agree with the axioms and assumptions I made so far, you should close this file and leave right now.

⌟

Remark (2.1.1.4) [Logical Issue]. Pedantically, by our construction of our mathematical system, in order for propositions to be defined in a lower order system, we should have defined symbols exclusively each time we enlarge the system, and never say something like "let n be a natural number, $n + 1 > 0$", because this is not a wff. In stead, we should write $(\forall n)(n + 1 > 0)$, because this is a wff. in Peano's system PA, and n is born to be representing a natural number, i.e. a symbol in the system PA.

But in practice, it is annoying to do so, so we will be more tolerant on this kind of usage. Just remember always this kind of sentence can be formalized. ⌟

2 Languages

Def. (2.1.2.1) [Languages]. A **language** $\mathcal{L}$ is a countable set of symbols. There may be subsets of symbols such as free symbols, bound symbols, function symbols, logical symbols, etc.. ⌟

Remark (2.1.2.2) [Formal System]. A **formal system** $\mathcal{L}$ consists of the following data:

- A language L(2.1.2.1), or equivalently, a set of symbols.
- A set of **well-formed formulas** or wffs.
- A set of **axioms**.

⌟

Remark (2.1.2.3) [Class System as a Metasystem]. Notice for any language or system, the class system is a metasystem of it. So we can formalize talking about everything about this system in the class system, like consistency, completeness...

Given a formal system L, we will typically use metavariables a, b, c, x, y, z whose domain is the collection of symbols in L, and use metavariables φ, ψ, η to describe wffs in L. ⌟

Meta Thm. (2.1.2.4). The primordial language $\mathscr{L}_0$(2.1.1.1) is a language(2.1.2.1). In fact a first order language to be defined in(2.1.5.1). The class system $\mathscr{L}_C$ is a formal system(2.1.2.2). (i.e. they are sets). ⌟

Remark (2.1.2.5). Until now I settled all the logical issues, but remember I made several assumptions that is metaphysical and cannot be settled by logic or math:

- There is a representation of will called the primordial language(2.1.1.1),
- There is a "talking system" that is a representation of will that can describe all other systems can enables the presence of this book(2.1.1.3).

⌟

3 Class System(ZF)

Def. (2.1.3.1). In fact this theory is a theory that lies between ZF and NBG. I think it is better to just change everything to NBG**?** ⌟

Def. (2.1.3.2) [Class System]. The **class system** ZF is a formal system(2.1.2.2) with

- Language: A first order language(2.1.5.1) with
  - Free variable symbols:
    - $0, a_0$ are free variable symbols.
    - For any natural number n, if a_n is a free variable symbol, then a_{n+1} is also a free variable symbol.
  - Bound variable symbols:
    - $x(0)$ is a bound variable symbol.
    - For any natural number n, if x_n is a bound variable symbol, then x_{n+1} is also a bound variable symbol.
  - Predicate symbol: $\in, =$.
  - Punctuation symbols: "(", ")", "...", "," and "{", "}", "|", ":".
  - Connective symbols: $\neg$ and $\to$.
  - Quantifier symbol: $\forall$.
- Grammar:
  - A procedure to specify wffs:
    - If a, b are free variable, then $a \in b$ is a wff..
    - If φ, ψ are wffs, a, b are free variables and x is a bound variable, then

$$(a \in \{x|\psi(x/a)\}), \quad (\{x|\psi(x/a)\} \in b), \quad (\{x|\varphi(x/a)\} \in \{x|\psi(x/b)\})$$

      are wffs, where $\psi(x/a)$(resp. $\varphi(x/b)$) is obtained from ψ(resp. φ) by replacing a free variable a(resp. b) by a bound variable x that doesn't appear in ψ(resp. φ).
    - If φ, ψ are wffs, then $\neg\varphi$ and $\varphi \to \psi$ are wffs.
    - If φ is a wff. and x is a bound variable, then $(\forall x)\varphi(x/a)$ is a wff.
  - A procedure to specify terms:
    - Variables are terms.

    * If φ is a wff., then $\{x|\varphi\}$ is a term, called a **class**.

- Axioms:
  - Logical Axioms: If φ, ψ, η are wffs,
    * $(\varphi \implies (\psi \implies \varphi))$.
    * $((\varphi \implies (\psi \implies \eta)) \implies ((\varphi \implies \psi) \implies (\varphi \implies \eta)))$.
    * $((\neg\varphi \implies \neg\psi) \implies (\psi \implies \varphi))$.
    * $((\forall x)\varphi \implies \varphi(a/x))$ where $\varphi(a/x)$ is obtained from φ by replacing each occurrence of the bound variable x in $\varphi(x)$ by the free variable a.
    * $((\forall x)(\varphi \implies \psi) \implies (\varphi \implies (\forall x)\psi))$, if the free variable a in φ which are quantifying with x doesn't appear.
    * (Modus Ponuns or MP)$\varphi \wedge (\varphi \implies \psi) \to \psi$.
    * (Generalizations)$\varphi \to (\forall x)\varphi(x/a)$, where x is a bound variable symbol that doesn't appear in φ, and $\varphi(a/x)$ is obtained from φ by replacing each occurrence of some free variable a by x.
  - Non-logical axioms: If φ, ψ are wffs, then

    C1: $(a \in \{x|\varphi\}) \iff \varphi(a/x)$, where $\varphi(a/x)$ is φ with all occurrence of x replaced by a.

    C2: $(\{x|\varphi(x)\} \in a) \iff ((\exists y)((y \in a) \wedge (\forall z)((z \in y) \iff \varphi(z/x))))$, where $\varphi(z/x)$ is φ with all occurrence of x replaced by z.

    C3: $(\{x|\varphi(x)\} \in \{x|\psi\}) \iff ((\exists y)(\psi(y/x) \wedge (\forall z)((z \in y) \iff \varphi(z/x))))$, where $\varphi(z/x)$ is φ with all occurrence of x replaced by z and $\psi(y/x)$ is ψ with all occurrence of x replaced by y.

    C4: (Equality)$(a = b) \iff (\forall x)((x \in a) \iff (x \in b))$.

    C5: (Axiom of Extensionality)(2.1.3.3).

    C6: (Axiom of Pairing)(2.1.3.20).

    C7: (Axiom of Union)(2.1.3.26).

    C8: (Axiom of Power Set)(2.1.3.30).

    C9: (Axiom Schema of Replacement)(2.1.3.31).

    C10: (Axiom of Regularity/Foundation)(2.1.3.40).

    C11: (Axiom of Infinity)?.

⌟

<u>**Equalities**</u>

Axiom (2.1.3.3) [Axiom of Extensionality]. $((a = b) \wedge (a \in c)) \to (b \in c)$. ⌟

Meta Thm. (2.1.3.4) [Reduce Class to Sets]. For any wff φ in the class system, there exists a wff φ^* in the set system s.t. φ is deducible from φ^* and φ^* is deducible from φ.(2.1.4.1)? ⌟

Proof: Use induction.? □

Remark (2.1.3.5). This tells us that the extension from set system to class system is conservative.? ⌟

Meta Thm. (2.1.3.6). The set system? is a subsystem(2.1.4.4) of the class system(2.1.3.2). Moreover, every term in set system is a term in the class system. ⌟

Def. (2.1.3.7).
- If φ is a wffs, define $\{x : \varphi\} \triangleq \{x|\varphi\}$.
- If A, B are classes, then define $A \notin B \triangleq \neg(A \in B)$.
- If A is a class and φ is a wff., define $(\forall x \in a)\varphi \triangleq (\forall x)(x \in a)(\wedge\varphi)$

⌟

Def. (2.1.3.8) [Equality between Classes]. If A, B are classes, then

$$A = B \triangleq (\forall x)((x \in A) \iff (x \in B)), \quad A \neq B \triangleq \neg(A = B)$$

⌟

Meta Thm. (2.1.3.9). If A, B, C are classes, then
- $(A = B) \iff (\exists x)((x = A) \wedge (x \in B))$.
- $(A = A)$.
- $(A = B) \to (B = A)$.
- $(A = B) \wedge (B = C) \to (A = C)$.

⌟

Proof: Cf.[Axiomatic Set Theory]P13. □

Meta Thm. (2.1.3.10). $(a = b) \to (\varphi(a/x) \iff \varphi(b/x))$, where $\varphi(a/x)$ is constructed from φ by replacing every free occurrence of x by a. ⌟

Proof: Cf.[Axiomatic Set Theory, P8]. The proof used induction on the number of logical symbols in φ.? □

Thm. (2.1.3.11) [Every Set is a Class]. $a = \{x|x \in a\}$. ⌟

Proof: This follows from axiom (C2) and the fact $(\forall x)((x \in a) \iff (x \in a))$. □

Def. (2.1.3.12) [Set Predicate]. If A is a class, $\mathscr{M}(A) \triangleq (\exists x)(x = A)$. This predicate formally indicate that "A is a set". ⌟

Prop. (2.1.3.13). $\mathscr{M}(a)$. ⌟

Proof: $a = a$. □

Meta Thm. (2.1.3.14). If A is a class, then $(A \in \{x|\varphi(x)\}) \iff (\mathscr{M}(A) \wedge \varphi(A))$. ⌟

Proof: Use induction on A? □

Thm. (2.1.3.15) [Russell's Paradox]. Define $\mathrm{Ru} \triangleq \{x|x \notin x\}$. Then $\neg\mathscr{M}(\mathrm{Ru})$. ⌟

Proof: By considering the wff. $\varphi : x \notin x$, it follows from(2.1.3.14) that

$$(\mathscr{M}(\mathrm{Ru}) \wedge (\mathrm{Ru} \notin \mathrm{Ru})) \rightarrow (\mathrm{Ru} \in \{x|x \notin x\}) \overset{\text{subst}}{\iff} (\mathrm{Ru} \in \mathrm{Ru})$$

so

$$\mathscr{M}(\mathrm{Ru}) \rightarrow ((\mathrm{Ru} \notin \mathrm{Ru}) \rightarrow (\mathrm{Ru} \in \mathrm{Ru})).$$

so

$$\mathscr{M}(\mathrm{Ru}) \rightarrow (\mathrm{Ru} \in \mathrm{Ru}).$$

Then by axiom (C3),

$$(\mathrm{Ru} \in \mathrm{Ru}) \rightarrow ((\exists y)(\psi(y/x) \wedge (\forall z)((z \in y) \iff z \notin z)))$$

which is false. So $\neg\mathscr{M}(\mathrm{Ru})$. □

Def. (2.1.3.16) [Definable Sets]. If φ is a wff., then we say that $\{x|\varphi(x)\}$ is a **definable set** if $\mathscr{M}(\{x|\varphi(x)\})$. ⌟

<u>**Properties of Classes**</u>

Def. (2.1.3.17) [Pairs and Ordered Pairs].

- $\{a, b\} \triangleq \{x|(x = a) \vee (x = b)\}$.
- $\{a\} \triangleq \{a, a\}$.
- $(a, b) \triangleq \{x|(x = \{a\}) \vee (x = \{a, b\})\}$.
- $a_n \triangleq (a, n)$.(notice n is a natural number).

⌟

Meta Def. (2.1.3.18) [MultiPairs]. For any free variable a_0 and a natural number n, define a term $\{a_1, \ldots, a_n\}$. For any bound variable x_0, define a bound term $\{x_1, \ldots, x_n\}$. ⌟

Prop. (2.1.3.19).

- $(c \in \{a, b\}) \iff ((c = a) \vee (c = b))$.
- $(c \in \{a\}) \iff (c = a)$.
- $(c \in (a, b)) \iff ((c = \{a\}) \vee (c = \{a, b\}))$.
- $(\{a\} = \{b\}) \iff (a = b)$.
- $(\{a\} = \{b, c\}) \iff ((a = b) \wedge (b = c))$.
- $((a, b) = (c, d)) \iff ((a = c) \wedge (b = d))$.
- $((\forall x)((a \in x) \rightarrow (b \in x))) \rightarrow (a = b)$.

⌟

Axiom (2.1.3.20) [Axiom of Pairing]. $\mathscr{M}(\{a, b\})$. ⌟

Cor. (2.1.3.21). $\mathscr{M}((a, b))$. ⌟

Meta Thm. (2.1.3.22) [Objects of Classes are Sets]. For classes A, B, $(A \in B) \rightarrow \mathscr{M}(A)$. ⌟

Def. (2.1.3.23) [Unions]. For classes A, B, define

- $A \cup B \triangleq \{x|(x \in A) \vee (x \in B)\}$.
- $A \cap B \triangleq \{x|(x \in A) \wedge (x \in B)\}$.
- For a class A, define $\cup(A) \triangleq \{x|(\exists y)((x \in y) \wedge (y \in A))\}$.

⌟

Prop. (2.1.3.24). $(a \cup b) = \cup(\{a, b\})$. ⌟

Proof: Cf.[Axiomatic Set Theory, P16]. □

Prop. (2.1.3.25).
- $(a \in (b \cup \{b\})) \iff (a \in b) \vee (a = b)$.
- $A \cup B = B \cup B$.
- $A \cap B = B \cap A$.
- $(A \cup B) \cup C = A \cup (B \cup C)$.
- $(A \cap B) \cap C = A \cap (B \cap C)$.
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

⌟

Proof: □

Axiom (2.1.3.26) [Axioms of Union]. $\mathscr{M}(\cup(a))$. ⌟

Cor. (2.1.3.27). $\mathscr{M}(a \cup b)$. ⌟

Proof: □

Def. (2.1.3.28) [Subclasses]. For classes A, B, define
- $A \subset B \triangleq (\forall x)((x \in A) \to (x \in B))$.
- $A \subsetneq B \triangleq ((A \subset B) \wedge (A \neq B))$.

⌟

Def. (2.1.3.29) [Power Sets]. $\mathscr{P}(a) \triangleq \{x|x \subset a\}$, called the **power set** of a. ⌟

Axiom (2.1.3.30) [Axiom of Power Set]. $\mathscr{M}(\mathscr{P}(a))$. ⌟

Axiom (2.1.3.31) [Axiom Schema of Replacement]. For each wffs φ, there is an axiom

$$((\forall x)(\forall y)(\forall z)((\varphi(x/a, y/b) \wedge \varphi(x/a, z/b)) \to (y = z)) \to \mathscr{M}(\{y|(\exists x \in a)\varphi(x/a, y/b)\})).$$

⌟

Meta Cor. (2.1.3.32). For any class A, $\mathscr{M}(a \cap A)$. ⌟

Proof: Cf.[Axiomatic Set Theory, P20]. □

Def. (2.1.3.33) [Setminus]. For classes A, B, define $A \setminus B \triangleq \{x|(x \in A) \wedge (x \notin B)\}$. ⌟

Meta Thm. (2.1.3.34). If A is a class, then $\mathscr{M}(a \setminus A)$. ⌟

Proof: $\mathscr{M}(a \setminus A) \overset{\text{subst}}{\iff} \mathscr{M}(\{x \in a | x \notin A\})$ is a theorem by(2.1.3.32). □

Def. (2.1.3.35) [Empty Class]. $0 \triangleq \{x | x \notin x\}$. ⌟

Prop. (2.1.3.36). $a \setminus a = 0$. ⌟

Proof: $a \setminus a \overset{\text{subst}}{\iff} \{x | (x \in a) \wedge (x \notin a)\} = \{x | x \notin x\}$? □

Cor. (2.1.3.37) [Empty Set]. $\mathscr{M}(0)$. ⌟

Prop. (2.1.3.38).
- $(\forall x)(x \notin 0)$.
- $(a \neq 0) \iff (\exists x)(x \in a)$.

⌟

Proof: 1: $(\forall x)(x = x)$.
2: By axiom (Equality),

$$(a \neq 0) \iff (\exists x)((x \in 0) \wedge (x \notin a)) \vee ((x \in a) \wedge (x \notin 0)).$$

Then it follows from item1 that $(a \neq 0) \iff (\exists x)(x \in a)$. □

Meta Def. (2.1.3.39). We define $\{a_1 \in a_2 \in \ldots \in a_n\}$ as in(2.1.4.3).? ⌟

Axiom (2.1.3.40) [Axiom of Regularity(Foundation)]. $(a \neq 0) \to (\exists x \in a)((x \cap a) = 0)$. ⌟

Cor. (2.1.3.41). $(a \notin a)$. ⌟

Proof: If $(a \in a)$, then $\{a\} \neq 0$ by(2.1.3.38), and unwinding the definition?,

$$(\forall x)((x \in \{a\}) \to (x \cap \{a\}) \neq 0),$$

contradicting axiom of regularity(2.1.3.40). □

Meta Cor. (2.1.3.42). For any natural number $n > 0$, $\neg(a_1 \in a_2 \in \ldots \in a_n \in a_1)$. ⌟

Proof: If $(a_1 \in a_2 \in \ldots \in a_n \in a_1)$, then $\{a_1, \ldots, a_n\} \neq 0$ by(2.1.3.38), and

$$(\forall x)((x \in \{a_1, \ldots, a_n\}) \to (x \cap \{a_1, \ldots, a_n\}) \neq 0),$$

contradicting axiom of regularity(2.1.3.40). □

Prop. (2.1.3.43) [von.Neumann Universe]. Define $\mathscr{V} \triangleq \{x | x = x\}$, then $\neg\mathscr{M}(\mathscr{V})$. And in fact $\mathscr{V} = \mathrm{Ru}$(2.1.3.15). ⌟

Proof: Since $\mathscr{V} = \mathscr{V}$, if $\mathscr{M}(V)$, then $V \in V$, by(2.1.3.14), then this together with $\mathscr{M}(V)$ contradicts(2.1.3.41) after unwinding definition?. (Notice that metathm(2.1.3.14) is a wff. when restricted to V).

For the last assertion,? □

Meta Thm. (2.1.3.44). For classes A, B,
- $0 \subset A$.

- $A \subset \mathscr{V}$.
- $(\forall x)(x \notin A) \to (A = 0)$.
- $(A \subset a) \to \mathscr{M}(A)$.
- $\mathscr{M}(A) \to \mathscr{M}(A \cap B)$.
- $A \notin A$.

⌟

Meta Thm. (2.1.3.45) [Strong Regularity]. The axiom of regularity(2.1.3.40) implies a stronger form of regularity: For any class A,

$$(A \neq 0) \to (\exists x \in A)((x \cap a) = 0).$$

⌟

Proof: Cf.[Axiomatic Set Theory]P80. □

Meta Cor. (2.1.3.46). For any class A,

$$(\forall x)((x \subset A) \to (x \in A)) \to (A = \mathscr{V})$$

(In words, if every set a has a property(a wff. φ) whenever every element of a has this property, then every set has this property.) ⌟

Proof: If $(\forall x)((x \subset A) \to (x \in A))$, denote $B = V \setminus A$, if $B \neq 0$, then by strong regularity(2.1.3.45),

$$(\exists a)((a \in B) \wedge (a \cap B) = 0).$$

So

$$(\forall y)((y \in a) \to (y \notin B)).$$

But $y \in V$, so

$$(\forall y)((y \in a) \to (y \notin A)).$$

And then $a \subset A$, and the hypothesis on A implies $a \in A$, contradicting the fact $a \in B$. So $A = V$, by(2.1.3.44). □

Meta Cor. (2.1.3.47) [Inclusion Induction]. There are no infinite descending $\in$-chains of sets. ⌟

Proof: The property $\mathscr{P}$ of not having infinite descending $\in$-chain is a wff., so $A = \{x|\mathscr{P}(x)\}$ is a class. And it can be shown $(a \subset A) \to (a \in A)$. Thus by(2.1.3.46), $A =$ Ru, so every set has no infinite descending $\in$-chains. □

4 Formal Propositional Calculus

Meta Def. (2.1.4.1) [Deductions]. Let L be a formal system(2.1.2.2), a **proof** is a finite sequence of wffs s.t. every wffs appearing is either an axiom or a wedge of two wffs before it.

A **theorem** in L is a wffs that is deducible from an axiom η of L. A proof(resp. theorem/defi) in the metasystem is called a **metaproof**(resp. **metatheorem**/defi). ⌟

Meta Def. (2.1.4.2) [Multiple Deduction]. Let L be a formal system and ψ a wff. in L, then for any natural number $n > 0$ and any $\{\eta_1, \dots, \eta_n\}$(2.1.3.18), then introduce metaterms

$$\{\eta_1\} \vdash_L \psi, \quad \{\eta_1, \eta_2\} \vdash_L \psi, \quad \{\eta_1, \dots, \eta_n\} \vdash_L \psi$$

and metaaxioms:

$$\{\eta_1\} \vdash_L \psi \triangleq \vdash_L (\eta_1 \to \psi).$$

$$\{\eta_1, \dots, \eta_{n+1}\} \vdash_L \psi \triangleq \{\eta_1, \dots, \eta_n\} \vdash_L (\eta_{n+1} \to \psi)$$

It reads: ψ is **deducible form** η_1 **to** η_n. ⌟

Remark (2.1.4.3). This definition of multiple deduction shows that we have the ability to handle multiple definition involving "...". But due to limit of space, we will not do so again, and leave it to the future to formalize it.**?** ⌟

Meta Def. (2.1.4.4)[Subsystem]. A formal system L is called a **subsystem** of another formal system L' or L' is an **extension system** of L if:

- There is a procedure to assign a wff. in L' for each wff. in L such that
  - Every proof in L is assigned to a proof in L'.
  - Every axiom in L is a theorem in L'.

⌟

Propositional Calculus

Def. (2.1.4.5) [Formal System of Propositional Calculus]. The formal system(2.1.2.2) of **propositional calculus** $\mathscr{L}$ is defined by the following:

- Symbols:
  - A procedure to specify which things are **variable symbols**.
  - **punctuation symbols** "(", ")".
  - **connective symbols**: $\neg$, $\implies$.
- Grammer:
  - Symbols are wffs.
  - If φ, ψ are wffs, then $\neg\varphi$ and $(\varphi \implies \psi)$ are wffs.
- Axioms: If φ, ψ, η are wffs, then the following are axioms:
  L1: $(\varphi \implies (\psi \implies \varphi))$.
  L2: $((\varphi \implies (\psi \implies \eta)) \implies ((\varphi \implies \psi) \implies (\varphi \implies \eta)))$.
  L3: $((\neg\varphi \implies \neg\psi) \implies (\psi \implies \varphi))$.
  L4: (Modus Ponuns or MP)If φ, ψ are wffs, then $\varphi \wedge (\varphi \to \psi) \to \psi$.

From now on, this system is the foundation of the book, and every language follows will contain $\mathscr{L}$.
⌟

Def. (2.1.4.6) [Logical Abbreviations]. For wffs φ, ψ,

- $(\varphi \vee \psi) \triangleq (\neg\varphi \implies \psi)$,
- $(\varphi \wedge \psi) \triangleq \neg(\varphi \implies \neg\psi)$,

- $(\varphi \iff \psi) \triangleq \neg((\varphi \implies \psi) \implies \neg(\psi \implies \varphi))$,
- $[\triangleq \{$,
- $] \triangleq \}$.

⌟

Meta Thm. (2.1.4.7). let L be a language and φ, ψ, η be wffs in L

- Axioms of L are theorems in L.
- $\{(\varphi \implies \psi), (\psi \implies \eta)\} \vdash_L (\varphi \implies \psi)$.
- $\vdash_L (\neg\psi \implies (\psi \implies \varphi))$.
- $\vdash_L ((\neg\varphi \implies \varphi) \implies \varphi)$.

⌟

Proof: Cf.[Hamilton, Chap2]. □

Meta Thm. (2.1.4.8) [Deduction Theorem]. Let φ, ψ be wffs in L,

- If $\Gamma \cup \{\varphi\} \vdash_L \psi$, then $\Gamma \vdash_L (\varphi \implies \psi)$.
- If $\Gamma \vdash_L (\varphi \implies \psi)$, then $\Gamma \cup \{\varphi\} \vdash_L \psi$.

⌟

Proof: Cf.[Hamilton, P32].**?** □

Adequacy Theorem for $\mathscr{L}$

5 First Order Systems

Formal Predicate Calculus

Def. (2.1.5.1) [First Order Languages]. A **first order language** $\mathcal{L}$ is a language(2.1.2.1) with

- a countable set of **bound variable symbols**.
- a countable set of **free variable symbols**.
- a countable set of **constant symbols**.
- a countable set of **predicate(relation) symbols**.
- a countable set of **functions symbols**.
- the **punctuations symbols** "(", ")" and ",".
- the **connective symbols** $\neg$ and $\implies$.
- the **quantifier symbol** $\forall$.

⌟

Def. (2.1.5.2) [Formal System of Predicate Calculus]. Given a first order language L(2.1.5.1), we can define a formal system(2.1.2.2) of **predicate calculus** $\mathscr{K}_{\mathcal{L}}$ as follows:

- Symbols: symbols in L.
- Grammar:
  - There is a countable set of **terms**:
    - Constant symbols and free variable symbols are terms.

    * For any natural number n, If f^n is a function symbol, and for any $m < n$, t_m is a term, then $f(t_1, \dots, t_{n_f})$ is a term.
  - There is a set of **atomic formulas**: If R^k is a predicate symbol and $t_1, \dots, t_k$ are terms, then $R^k(t_1, \dots, t_k)$ are atomic formulas.
  - There is a countable set of wffs:
    * Atomic formulas are wffs.
    * if φ, ψ are wffs and x is a bound variable not appearing in φ, then $\neg\varphi, (\varphi \implies \psi), (\forall x)\varphi(x/a)$ are wffs, where $\varphi(x/a)$ is obtained from φ by replacing each occurrence of some free variable a by a bound variable x that doesn't appear in φ.

- Axioms: If φ, ψ, η are wffs in $\mathscr{K}_L$ and x is a variable, then There the following countably many axioms:

  K1: $(\varphi \implies (\psi \implies \varphi))$.

  K2: $((\varphi \implies (\psi \implies \eta)) \implies ((\varphi \implies \psi) \implies (\varphi \implies \eta)))$.

  K3: $((\neg\varphi \implies \neg\psi) \implies (\psi \implies \varphi))$.

  K4: $((\forall x)\varphi \implies \varphi(a/x))$ where $\varphi(a/x)$ is obtained from φ by replacing each occurrence of the bound variable x in $\varphi(x)$ by the free variable a.

  K5: $((\forall x)(\varphi \implies \psi) \implies (\varphi \implies (\forall x)\psi))$, if the free variable a in φ which are quantifying with x doesn't appear.

  K6: (Modus Ponuns or MP)$\varphi \wedge (\varphi \implies \psi) \to \psi$.

  K7: (Generalizations)$\varphi \to (\forall x)\varphi(x/a)$, where x is a bound variable symbol that doesn't appear in φ, and $\varphi(a/x)$ is obtained from φ by replacing each occurrence of some free variable a by x.

⌟

Meta Def. (2.1.5.3) [Sentences and Theories]. A **sentence** is a formula without free variables.
A **theory** is a set of sentences in a language $\mathcal{L}$. ⌟

Meta Thm. (2.1.5.4) [Tautologies are Theorems]. if φ is a wff. in a language L and it is a tautology**?**, then φ is a theorem(2.1.4.1) of $\mathscr{K}_L$(2.1.5.2). ⌟

Proof: Cf.[Hamilton]P72. □

Meta Thm. (2.1.5.5) [Soundness Theorem for $\mathscr{K}_L$]. If φ is a wff. in a language L and $\vdash_{\mathscr{K}_L} \varphi$, then φ is locally valid**?**, ⌟

Proof: Cf.[Hamilton]P74. □

Meta Cor. (2.1.5.6) [Consistence for $\mathscr{K}_L$]. $\mathscr{K}_L$ is consistent. ⌟

Proof: Cf.[Hamilton]P74. □

Meta Cor. (2.1.5.7). For any wffs φ, ψ, η of L,

$$\{(\varphi \implies \psi), (\psi \implies \eta)\} \vdash_{\mathscr{K}_L} (\varphi \implies \eta)$$

⌟

Proof: Cf.[Hamilton]P76. □

Adequacy Theorem for $\mathscr{K}_L$

Def. (2.1.5.8). ┘

Satisfaction and Truth

See[Hamilton].

6 Models and Examples of Systems

Def. (2.1.6.1) [(Mathematical) Languages]. A **mathematical language** $\mathcal{L}$ is a first order language(2.1.5.1) given by the following data:

- A set $\mathcal{F}$ of **function symbols**.
- A set $\mathcal{R}$ of **relations symbols**.
- A set $\mathcal{C}$ of **constant symbols**.

Function symbols, relations symbols, constant symbols consists of all symbols in $\mathcal{L}$. For simplicity, we call a mathematical language simply a language. ┘

Example (2.1.6.2) [(Mathematical)Languages].

- $\mathcal{L}_0$ is the basic language of logics.
- $\mathcal{L}_r = (+, \cdot)$ is defined to be the language of rings.
- $\mathcal{L}_{or} = (+, \cdot, <)$ is defined to be the language of ordered rings.
- $\mathcal{L}_{\omega_1,\omega}(Q)$ is defined to be the language which is an extension of $\mathcal{L}_0$ in which we can form countable conjunctions and add a quantifier Q : there exists uncountably many.

┘

Def. (2.1.6.3) [Theories].

- ACF is defined to be the theory of alg.closed fields, w.r.t $\mathcal{L}_r$.
- ACF_p is defined to be the theory of alg.closed fields of char$p$.
- DAG is defined to be the theory of non-trivial torsion-free divisible Abelian groups, w.r.t. $\mathcal{L}_r$.
- DLO is the theory of dense linear orders without endpoints.
- $ODAG$ is the theory of nontrivial divisible Abelian groups.
- RCF is the theory of real closed fields w.r.t $\mathcal{L}_{or}$.

┘

2.2 Set Theory

Main references are [Jec03], [Model Theory Marker], [Axiomatic Set Theory], [Hamilton],

Notation (2.2.0.1).

- Use notations from Mathematical Logic.
- We build theories based on the class system(2.1.3.2).
- As in(2.1.1.3), all propositions are regarded as theorems in a system that is an extension of all other systems defined in this book, in particular it is an extension of the blank PA system(2.1.1.2) and the class system $\mathscr{L}_C$(2.1.3.2).
- We will rebuild PA system and NBG/ZFC set theory inside primordial ZFC.(This new ZFC should be regarded as a representation of the primordial ZFC inside itself), so the logic section will no longer be cited other than this section.?

⌟

1 Von.Neumann-Bernays-Gödel Set Theory(NBG)

Def. (2.2.1.1) [Inductive Sets]. A set I is called **inductive** if $0 = \varnothing \in I$ and if $n \in I$, then $n+1 \in I$, where $n+1 = S(n)$ the successor. ⌟

Axiom (2.2.1.2) [Axiom of infinity]. An inductive set(2.2.1.1) exists. ⌟

Def. (2.2.1.3) [Set of Natural Numbers]. The **set of natural numbers** $\mathbb{N}$ is defined to be

$$\mathbb{N} = \{x \in I_0 | x \in I \text{ for all inductive set } I\},$$

where I_0 is an inductive set given by(2.2.1.2). Elements of $\mathbb{N}$ are called **natural numbers**. ⌟

Cor. (2.2.1.4) [Inductive Principle]. If $P(x)$ is a property that $P(0)$, and $P(n)$ implies $P(n+1)$, then $P(n)$ for each natural number n. ⌟

Proof: By definition $B = \{n \in \mathbb{N} | P(n)\}$ is an inductive set, so $\mathbb{N} \subset B$. □

Prop. (2.2.1.5). $\mathbb{N}$(2.2.1.3) is a linearly ordered set. ⌟

Proof: Cf.[Set Theory Jech P43]. □

Cor. (2.2.1.6) [Inductive Principle Second Version]. If $P(x)$ is a property that $P(0)$, and $P(k)$ holds for all $k < n$ implies $P(n)$, then $P(n)$ for each natural number n. ⌟

Proof: Use induction principle(2.2.1.4) for the property $Q(n) : P(k)$ for all $k < n$. Then $Q(n)$ implies $Q(n+1)$. □

2 Relations and Functions

Def. (2.2.2.1) [Products]. For classes A, B, $A \times B$ is the class

$$\{x | (\exists y \in A)(\exists z \in B)(x = (y, z))\},$$

called the **product of A and B**. ⌟

Prop. (2.2.2.2). $\mathscr{M}(a \times b)$. ⌟

Proof: Cf.[Axiomatic Set theory]P23. □

Def. (2.2.2.3). Inductively define**?** class terms

- $A^1 \triangleq A$,
- $A^{n+1} \triangleq A^n \times A$,
- $A^{-1} \triangleq \{(x,y)|(y,x) \in A\}$.

And define ⌟

Def. (2.2.2.4) [Relations and Functions]. Define the following predicates:

- $\mathrm{Rel}(R) \triangleq R \subset A^2$.
-

⌟

Def. (2.2.2.5) [Bijections]. ⌟

Def. (2.2.2.6) [Finite and Infinite Sets]. For $n \in \mathbb{N}$ and a set X, we use the sentence "X has n elements" to mean there is a bijection from n to X. We use the sentence "X is a **finite set**" to mean X has n elements for some $n \in \mathbb{N}$, and say it is an **infinite set** otherwise. ⌟

3 Orderings

Def. (2.2.3.1) [Ordering]. A **partial ordering** on a set A is a relation(2.2.2.4) $<$ on A, or equivalently a subset $C \subset A \times A$ that

- For no $x \in A$, $x < x$ holds.
- If $x < y$ and $y < z$, then $x < z$.

It is called a **total ordering** if moreover it satisfies

- For every $x, y \in A$ that $x \neq y$, either $x < y$ or $y < x$.

A **poset** is defined to be a partially ordered set. ⌟

Def. (2.2.3.2) [Reverse Orderings]. The **reverse ordering** A^{op} of an ordered set A is the same set A with the ordering reversed. ⌟

Def. (2.2.3.3) [Cofinality]. The **cofinality** of or a poset(2.2.3.1) α is the is the smallest cardinality δ of a cofinal subset of α. ⌟

Def. (2.2.3.4) [κ-Filtered Poset]. For a cardinal κ, a poset is called **κ-filtered** if for any subset unbounded from above has cardinality$\geq \kappa$. ⌟

Def. (2.2.3.5) [Directed Sets]. A **directed set** is a poset that 3-filtered and non-empty. ⌟

Def. (2.2.3.6). In a poset P, two element p, q are called **compatible** if there is an $r \in P$ that $r < p, r < q$. ⌟

Def. (2.2.3.7) [κ-Chain Condition]. For a cardinal κ, a poset P is said to satisfy the **κ-chain condition** if for any subset $A \subset P$ that elements of A are pairwise incompatible(2.2.3.6), then $|A| \leq \kappa$. ⌟

Total Ordering

Def. (2.2.3.8) [Well-Orderings]. A **linear ordering** is defined to be a total ordering.

A linear ordering is called a **well-ordering** if every nonempty subset has a minimal element. ⌟

Def. (2.2.3.9) [Lexicographical Ordering]. If given a family of linearly ordered set A_i indexed by a well-ordered set I, then there is a linear ordering on $\prod_I A_i$, where $(f_i) < (g_i)$ iff $(f_i) \neq (g_i)$ and for the minimal i_0(well-ordering used) that $f_{i_0} \neq g_{i_0}$, $f_{i_0} < g_{i_0}$. It is called the **lexicographical ordering**. ⌟

Def. (2.2.3.10). An ordered set X is called **dense** iff for each $a < b$, there is a x that $a < x < b$. ⌟

Def. (2.2.3.11) [Least Upper Bound]. An ordered set A is said to have the **least upper bound property** if any subset $A_0 \subset A$ bounded above has a least upper bound. It is said to satisfy the **greatest lower bound property** if A^{op} satisfies the least upper bound property. ⌟

Prop. (2.2.3.12) [Cantor]. Any two ordered set that is countable, dense and has no endpoints are isomorphic. In particular, any of these is isomorphic to the set of rational numbers $\mathbb{Q}$. ⌟

Proof: We will built the isomorphism by extending partial embeddings. Let $a_0, \ldots, a_n, \ldots$ be an ordering of A, $b_0, \ldots, b_n, \ldots$ be an ordering of B, and we can alternatively extend mapping on a_n and b_n, as A, B are complete without endpoints. Then we get an isomorphism of A and B. □

Cor. (2.2.3.13). Any countable linearly ordered set can be mapped isomorphically into $\mathbb{Q}$. ⌟

Def. (2.2.3.14). A **initial segment** of an ordered set W is the ordered set $W[a] = \{x \in W | x < a\}$. ⌟

Lemma (2.2.3.15). If W is a well-ordered set, then any increasing function $f : W \to W$ satisfies $f(x) \geq x$. ⌟

Proof: If the set $\{x | f(x) < x\}$ is not empty, then it has a minimal element a, then $f(f(a)) < f(a)$, contradiction. □

Cor. (2.2.3.16). A well-ordered set cannot be isomorphic to an initial segment of itself, and an automorphism of a well-ordered set must be identity. ⌟

Proof: Use the above lemma(2.2.3.15), if it is isomorphic to $W[a]$, then $f(a) < a$, contradiction. For any automorphism, $f(x) \geq x, f^{-}(x) \geq x$, so $f(x) = x$. □

Prop. (2.2.3.17) [Comparison of Well-Orderings]. A cut of a well-ordered set is well-ordered. And for any two well-ordered sets W_1, W_2, either they are isomorphic, or one of them is isomorphic to a initial segment of another. ⌟

Proof: The three cases are mutually exclusive by(2.2.3.16), So it suffices to show one of them holds.

Define a set $f = \{(x, y) \in W \times W | W_1[x] \cong W_2[y]\}$. (2.2.3.16) shows f is injective and monotone in both coordinates. Now we want to prove that if the domain of f is not all W_1, then it is an initial segment, and the image is all W_2, this will finish the proof.

It is clearly an initial segment $W_1[a]$ because it is well-ordered and if $h : W_1[x] \cong W_2[y]$ and $x' < x$, then $h : W_1[x'] \cong W_2[h(y)]$. If the image is not all of W_2, then similarly the image of f is an initial segment of W_2, $= W_2[b]$. But this means $W_1[a] \cong W_2[b]$, so a, b is also in the domain(image), which is a contradiction. □

Well-Quasi-Orderings

Def. (2.2.3.18)[Well-quasi-orderings]. A **well-quasi-ordering** on a set A is a partial ordering $\leq$ on A satisfying the following: For any infinite sequence $(x_i) \in A^{\mathbb{N}}$, there exists $i < j \in \mathbb{N}$ s.t. $x_i \leq x_j$. ⌟

Prop. (2.2.3.19). A partial ordering on a set A is a well-quasi-ordering if X contains neither an infinite incomparable subset or an infinite decreasing chain $x_0 > x_1 > \ldots$.

Moreover, for a well-quasi-ordering, in any infinite sequence, there exists an infinite ascending chain $x_{i_0} \leq x_{i_1} \leq \ldots$ where $i_0 < i_1 \ldots$. ⌟

Proof: This follows from the infinite Ramsey theorem(25.4.0.2). □

Prop. (2.2.3.20). If X is a quasi-well-ordered set, then we can define a quasi-well-ordering on the set $[X]^{\leq\aleph_0}$ of finite subsets of X: for any $A, B \in [X]^{\leq\aleph_0}$, define $A \leq B$ if there is an injection $f : A \to B$ s.t. $a \leq f(a)$ for any $a \in A$. Then this is a quasi-well-ordering on $[X]^{\leq\aleph_0}$. ⌟

Proof: Suppose $[X]^{\leq\aleph_0}$ is not quasi-well-ordered, and call the counterexamples bad sequences. Then we can choose a bad sequence $(A_n) \in ([X]^{\leq\aleph_0})^{\mathbb{N}}$ s.t. for any $n \in \mathbb{N}$, A_n is the subset with minimum cardinality s.t. $(A_0, A_1, \ldots, A_n)$ is the start of a bad sequence. Clearly $A_n \neq \varnothing$ for any $n \in \mathbb{N}$.

Choose an element a_i from each A_i, and denote $B_i = A_i \setminus \{a_i\}$. By hypothesis, the sequence $(a_0, a_1, \ldots)$ contains a infinite ascending sequence $a_{n_0} \leq a_{n_1} \leq \ldots$. By the choice of A_i, the sequence

$$A_0, A_1, \ldots, A_{n_0-1}, B_{n_0}, B_{n_1}, \ldots$$

is not a bad sequence. Clearly such an ascending pair can only be $B_{n_i} \leq B_{n_j}$ for some $i < j$. But extending any injection $f : B_{n_i} \to B_{n_j}$ to an injection $\overline{f} : A_{n_i} \to A_{n_j}$ by $f(a_{n_i}) = a_{n_j}$, we get that $A_{n_i} \leq A_{n_j}$, contradiction. □

Complete Linear Ordering

Def. (2.2.3.21) [Complete Ordering]. A **cut** of an ordered set X consists of two disjoint nonempty subsets $A \cup B = X$ that $a < b$ for any $a \in A, b \in B$.

It is called a **Dedekind cut** if A doesn't has a maximal element. It is called a **gap** if A doesn't have a maximal element and B doesn't have a minimal element.

An ordered set is called **complete** if there are no gaps. ⌟

Prop. (2.2.3.22). Any complete ordered set R has the least upper bound property and greatest lower bound property. ⌟

Proof: Consider the cut $A = \{x|x < a \text{ for some element in } T\}, B = \mathbb{R} - A$, if T is bounded above, B is not empty, so this is truly a cut, and A doesn't has a maximal element, because if $x < a \in \mathbb{R}$, then $x < \frac{x+a}{2} < a$. So by completeness of R, B has a minimal element, that is, the supremum of A exists. Similarly for the case A bounded from below. □

Prop. (2.2.3.23)[Completion of Ordering]. There is an obvious ordering on the set C of all Dedekind cuts of X, and X embeds into C by $b \mapsto \{x|x < b\} \cup \{x|x \geq b\}$.

C is complete and has no endpoints, P is dense in C, which is called a **completion** of P. ⌟

Proof: Cf.[Set Theory Jech P88]. □

Prop. (2.2.3.24) [Real Numbers]. $\mathbb{Q}$ has a unique completion ordering $\mathbb{R}$, called the **set of real numbers**. ⌟

Proof: $\mathbb{R}$ is a dense linear ordering without endpoints, so by(2.2.3.12) if it is countable then it is isomorphic to $\mathbb{Q}$, but this is not possible because $\mathbb{Q}$ is not complete. □

4 Ordinals(Cantor)

Def. (2.2.4.1) [Ordinal Numbers]. A set is called **transitive** iff each element of T is a subset of T. A set α is called a **ordinal number** iff α is transitive and well-ordered by inclusion. ⌟

Prop. (2.2.4.2). If α is an ordinal, then $S(\alpha) = \alpha \cup \{\alpha\}$ is also an ordinal, obviously. Thus any natural number is an ordinal by definition.

An ordinal is called a **successor ordinal** iff $\alpha = S(\beta)$ for some β, and a **limit ordinal** otherwise. ⌟

Lemma (2.2.4.3).

1. If α is an ordinal, then $\alpha \notin \alpha$.
2. Every element of an ordinal is an ordinal.
3. If ordinals $\alpha \subsetneq \beta$, then $\alpha \in \beta$. That is, for ordinals, $\subsetneq$ is the same as $\in$.

⌟

Proof:

1. If $\alpha \in \alpha$, then contradiction to the fact $\in$ is a ordering(2.2.4.1).
2. To show $x \in \alpha$ is transitive, it suffices to show that if $u \in v \in x$, then $u \in x$, because then v is a subset of x. But this follows from the fact $\in$ is an ordering. And because $x \subset \alpha$, the inclusion of x is the restriction of inclusion in α, so it is a well-ordering.
3. Consider $\beta - \alpha$, it has a minimal element γ. Notice $\gamma \subset \alpha$, because otherwise there is an element of $\beta - \alpha$ smaller than γ, by definition(2.2.4.1).
   Now we show $\gamma = \alpha$, then it will follow that $\alpha \in \beta$. For this, if $\delta \in \alpha$ and $\delta \notin \gamma$, then $\gamma \in \delta$ or $\gamma = \delta$. But then this implies that $\delta \in \alpha$ because α is an ordinal, contradicting the fact $\gamma \in \beta - \alpha$.

□

Prop. (2.2.4.4) [Ordinal is Well-Ordered]. Define the ordering of ordinal by $\alpha < \beta$ iff $\alpha \in \beta$. The ordering of ordinals is a total ordering and is a well-ordering. ⌟

Proof: If $\alpha\beta \in \gamma$, then $\alpha \in \gamma$ because γ is transitive. If $\alpha \in \beta \in \alpha$, then $\alpha \in \alpha$, contradicting(2.2.4.3).

Given any two ordinals, $\alpha \cap \beta$ is also an ordinal by definition. If $\alpha \cap \beta = \beta$ or α, then $\alpha \subset \beta$, hence $\alpha \in \beta$ by(2.2.4.3). If $\alpha \cap \beta \subsetneq \alpha$ and $\alpha \cap \beta \subsetneq \beta$, then $\alpha \cap \beta \in \alpha \cap \beta$, contradiction.

Well-ordering: Given a set of ordinals, take $\alpha \in A$ and consider the set $\alpha \cap A$. If $\alpha \cap A = \varnothing$, then α is minimal in A, because otherwise some $\beta \in \alpha \cap A$. If $\alpha \cap A \neq \varnothing$, then it has a minimal element β in the inclusion because α is an ordinal. Then β is the minimal element of A. □

Cor. (2.2.4.5) [Supremum Ordinal]. Any set of ordinals has a supremum ordinal, it is just $\cup_{\alpha \in X}\alpha$. ⌟

Proof: Firstly $\cup_{\alpha\in X}\alpha$ is transitive and it is well-ordered(for each subset $A\subset X$, choose an $\alpha\in X$ that $\alpha\cap A\neq 0$, then the minimal element of $\alpha\cap A$ is just the minimal element of A.) so it is an ordinal.

Now if $\alpha\in X$, then $\alpha\subset\cup X$, so $\alpha\leq\cup X$ by(2.2.4.3). And if $\alpha\in\gamma$ for some ordinal γ, then $\cup X\subset\gamma$. So $\cup X$ is truly the supremum. □

Cor. (2.2.4.6). For any set X of ordinals, there is an ordinal α that is not in X, just choose $S(\cup X)$. ⌟

Prop. (2.2.4.7). Every well-ordered set is isomorphic to a unique ordinal.

So we can regard an ordinal as an equivalence class of isomorphic well-ordered sets. ⌟

Proof: Cf.[Set Theory Jech P111]. □

Cor. (2.2.4.8) [Cardinal as Initial Ordinal]. The axiom of choice together with(2.2.4.4) asserts that every cardinal has a unique smallest ordinal, called the **initial ordinal**. So we can identify cardinal number α as an ordinal that is the initial ordinal ω_α of α. Anyway, cardinal number is fewer than ordinal numbers.

The first infinite cardinal number(or the first initial ordinal) is denoted by ω or $\aleph_0$. ⌟

Prop. (2.2.4.9) [Transfinite Induction/Recursion]. If a property defined for the set of ordinals satisfies:

1. $P(0)$.
2. $P(\alpha+1)$ if $P(\alpha)$.
3. $P(\lambda)$ if $P(\beta)$ for all $\beta<\lambda$.

then P is true for all ordinals.

Transfinite recursion: ⌟

Proof: □

Ordinal Arithmetic

Cf.[Set Theory Jech Chap5.5].

Def. (2.2.4.10). We use infinite recursion to define **addition of ordinals** as

- $\beta+0=\beta$
- $\beta+(\alpha+1)=(\beta+\alpha)+1$, where $\alpha+1$ is the successor of α.
- $\beta+\alpha=\sup\{\beta+\gamma|\gamma<\alpha\}$ for a limit ordinal α.

The **multiplication of ordinals** and **exponentiation of ordinals** are defined similarly. ⌟

Remark (2.2.4.11) [Cardinal and Ordinal Arithmetics]. Note that the ordinal arithmetics may be smaller than the ordinal sum of the corresponding initial ordinal(2.2.4.8), because operations of initial ordinals may not be initial, the deeper reason is that the cardinal case, we can rearrange the order to get a smaller ordinal. ⌟

Prop. (2.2.4.12). The addition and multiplication of ordinals are of the order type of $\alpha\coprod\beta$ in adjunction order and $\alpha\times\beta$ in lexicographical order respectively, Cf.[Set Theory Jech P120,122] ⌟

Cantor Normal Form

Prop. (2.2.4.13) [Cantor Normal Form]. Any ordinal α can be expressed uniquely as the form $\alpha = \sum_{i<n} \omega^{\beta_i}$, where $\beta_0 \geq \beta_1 \geq \dots \beta_{n-1}$ are ordinals. ⌟

Proof: Cf.[Jech Set Theory P124]. □

Prop. (2.2.4.14) [Goodstein Sequence]. The **weak Goodstein sequence** is a sequence that m_2 is any positive integer, m_{k+1} is m_k written in k-basis and replacing the base by $k+1$, and then minus 1.

The **Goodstein sequence** is a is a sequence that m_2 is any positive integer, m_{k+1} is m_k written in k-basis and even the exponents in k-basis and and replacing the base by $k+1$, and then minus 1.

Then for each Goodstein sequence and weak Goodstein sequence, it reaches 1 in a finite number of times. ⌟

Proof: Let $m_k = \sum k^{a_i} b_i$, then let the ordinal $\alpha_k = \sum \omega^{a_i} b_i$. Then it is clear that $\alpha_2 > \alpha_3 > \dots$. But if the weak Goodstein sequence doesn't terminate, we constructed a descending sequence of ordinals that doesn't terminate, contradiction(choose a minimal element).

Similarly for Goodstein sequences, just replace every base k by ω. □

5 The Axiom of Choice

Def. (2.2.5.1) [Choice Functions]. Let S be a system of sets, a function g defined on S is called a **choice function** iff $g(X) \in X$ for each $X \in S$. ⌟

Axiom (2.2.5.2) [the Axiom of Choice, Zermelo1904]. Any system of sets has a choice function. ⌟

Thm. (2.2.5.3) [Zermelo1904]. The following are equivalent:

1. the axiom of choice.
2. (the well-ordering principle)Every set can be well-ordered.
3. (Zorn's lemma)If every chain in a partially ordered sets has a upper bound, then the partially ordered set has a maximal element.

⌟

Proof: $2 \to 1$: If A is well-ordered, then $P(A)$ clearly has a choice function, that is the minimal element of a set.

$1 \to 2$: Use transfinite recursion, Cf.[Set Theory Jech P137].

$2 \to 3, 3 \to 2$: Cf.[Set Theory Jech P142]. □

Prop. (2.2.5.4). Every infinite set X has a countable subset, if the axiom of choice holds. ⌟

Proof: Choose a well-ordering of it(2.2.5.3), then it is an infinite ordinal. Then the initial segment of the first ordinal $X[\omega]$ is a countable subset. □

Prop. (2.2.5.5). For every infinite set S, there exists a unique aleph $\aleph_\alpha$ that $|S| = \aleph_\alpha$. ⌟

Proof: choose a well-ordering of S(2.2.5.3), then it is an infinite ordinal, and it has the same cardinality as an initial cardinal by(2.2.4.8), thus the result. □

Cor. (2.2.5.6). For any sets A and B, either $\#A \leq \#B$ or $\#B \leq \#A$. ⌟

Proof: Because the ordinal is totally ordered(2.2.4.4). □

6 Cardinals

Thm. (2.2.6.1) [Cantor-Schröder-Bernstein]. If there is an injection from A to B and an injection from B to A, then there is a bijection from A to B. Thus the ordering of the cardinal is well-defined.

So we can denote $\#A \leq \#B$ iff there is an injection from A to B. Then if $\#A \leq \#B$ and $\#B \leq \#A$, then $\#A = \#B$. In particular, this is a well-defined order relation. ⌟

Proof: It $f : A \to B$, $g : B \to A$ be injection, then use lemma(2.2.6.2) for $g \circ f(A) \subset g(B) \subset A$. □

Lemma (2.2.6.2). If $A_1 \subset B \subset A$ with $\#A = \#A_1$, then $\#A = \#B$. ⌟

Proof: Let f be a bijection from A to A_1. Define inductively $A_{n+1} = f(A_n), B_{n+1} = f(B_n)$. Then $A_{n+1} \subset B_n \subset A_n$. Let $C_n = A_n - B_n$, $C = \cup C_n$, then $f(C_n) = C_{n+1}$, so $f(C) = \cup_{i>0} C_i$.

Now define $g : A \to B = f(x)$ on C and x on $A \backslash C$, then it is a bijection from A to B. □

Def. (2.2.6.3) [Cardinal Numbers]. A **cardinal number** is an equivalence class of sets, where equivalence is given by bijections. it is used to describe the 'size' of a set. We use the sentence $\kappa \in \mathfrak{Card}$ to mean that κ is a cardinal.

It is by the axiom of choice that any two cardinal number can be compared.?

Denote $\aleph_0 = \#\mathbb{N}$(2.2.1.3). ⌟

Peano Arithmetics

Countable and Uncountable Sets

Def. (2.2.6.4) [Countable Sets]. A set is called **countable** iff it has cardinality $\aleph_0$(2.2.6.3). It is called a **finite set** if it has the cardinality of n for some natural number $n \in \mathbb{N}$. It is called an **uncountable set** iff it is not countable or finite. It is called an **at most countable set** if it is finite or countable. ⌟

Prop. (2.2.6.5). The subset or image of an at most countable set is at most countable. ⌟

Proof: □

Prop. (2.2.6.6). The product of two at most countable sets is at most countable. (Use diagonal enumerating). ⌟

Proof: □

Prop. (2.2.6.7). A countable union of almost countable subsets is almost countable. ⌟

Proof: It suffices to prove the countable case, the rest follows from(2.2.6.5). For this, choose an enumerating $a_n(k)$ for each A_n, the $\cup A_n$ is the image of $\mathbb{N} \times \mathbb{N} : (n, k) \mapsto a_n(k)$. Then it is countable by(2.2.6.6). □

Prop. (2.2.6.8). The set of finite sequences and hence the set of finite subsets of a countable set is countable. ⌟

Proof: The desired set equals $\cup_k A^k$, which is countable by(2.2.6.6) and(2.2.6.7). □

7 Cardinal Arithmetics

Def. (2.2.7.1). The **sum**, **multiplication** and **exponentiation** of two ordinal is the cardinality of the set $A\coprod B$, $A\times B$ or A^B respectively.

It is easily verified to be associative and commutative, just as usual operations. ⌟

Prop. (2.2.7.2). $\aleph_0\times\aleph_0=\aleph_0$ by(2.2.6.6). And $\kappa\times\kappa=\kappa$ for any infinite cardinal, if one uses the axiom of choice by(2.2.8.3). ⌟

Prop. (2.2.7.3). The image of a set X has cardinals no more than X, if axiom of choice holds. ⌟

Proof: Use axiom of choice to choose an element from each inverse image $f^{-1}(\{x\})$, then it is an injection from $f(X)$ to X. □

Prop. (2.2.7.4) [Cantor]. $\#\mathscr{P}(X)=2^{\#X}$, and $\#X<\#\mathscr{P}(X)$. ⌟

Proof: The first is obvious, for the second, the function $x\to\{x\}$ is an injection of X into $P(X)$. And there are no mapping from X onto $P(X)$, because if f is one, the consider $S=\{x|x\notin f(x)\}$, then S is not in the range of f, because if $f(z)=S$, then $z\in S$ iff $z\notin S$, contradiction. □

Prop. (2.2.7.5) [Cardinality Arithmetic of $\aleph_0$]. For cardinality arithmetics involving $\aleph_0$, Cf.[Set Theory Jech P98]. ⌟

Proof: □

Prop. (2.2.7.6)[Cardinality of $\mathbb{R}$]. $\#\mathbb{R}=\#\mathscr{P}(\mathbb{N})=2^{\aleph_0}$. In particular, by(2.2.7.4), $\mathbb{R}$ is uncountable. ⌟

Proof: The first equality is by(2.2.7.4). Now by the construction of $\mathbb{R}$, it can be embedded into $P(\mathbb{N})$, so $\#\mathbb{R}\leq\#\mathscr{P}(\mathbb{Q})=\#\mathscr{P}(\mathbb{N})$. Conversely, $|2^{\mathbb{N}}|\leq|\mathbb{R}|$ by decimal representation, so they are equal by bernstein(2.2.6.1). □

Prop. (2.2.7.7). if $\#B=2^{\aleph_0}$ and $\#A\leq\aleph_0$, then $|B\setminus A|=2^{\aleph_0}$. In fact, $|B-A|=|B|$ for any $\#A<\#B$, if one uses the axiom of choice. ⌟

Proof: By(2.2.7.5), we can assume $B=\mathbb{R}\times\mathbb{R}$, then project A onto the coordinate axis, then $\pi(A)$ has cardinality$\leq\aleph_0$, so there is a $x_0\notin\pi(A)$, so $x_0\times\mathbb{R}\subset B-A$, so $|B-A|=2^{\aleph}$.

For the general case, **?** □

Conj. (2.2.7.8)[The Continuum Hypothesis, Cantor1878]. There is no cardinal κ that $\aleph_0<\kappa<2^{\aleph_0}$.

Notice $2^{\aleph_0}\geq\aleph_1$ by Cantor's theorem(2.2.7.4), and this hypothesis is equivalent to $2^{\aleph_0}=\aleph_1$. ⌟

Proof: □

For Infinite operation of Cardinal Arithmetics, Cf.[Jec03]Chap9.

8 Alephs

Prop. (2.2.8.1). For any set A, there is a least ordinal that is not equipotent to any subset of A, called the **Hartogs number** of A. This is clearly an initial ordinal. ⌟

Proof: By axiom schema of replacement, any well-ordered subsets of A is equipotent to an ordinal, and also by axiom schema of replacement, there is a set H that for any well-ordering of subsets of A in $P(A\times A)$, this ordered sets is equipotent to a $\alpha\in H$. Then use(2.2.4.6) to find a minimal ordinal that is not equipotent to any subset of A. In fact, this is just $h(A)=\{\alpha\in H|\alpha$ equipotent to some subset of A$\}$. □

Def. (2.2.8.2)[Aleph]. The **alephs** for ordinal numbers are defined recursively: $\aleph_0=\omega$, $\aleph_{\alpha+1}=h(\aleph_\alpha)$, and $\aleph_\alpha=\sup\{\aleph_\beta|\beta<\alpha\}$ for a limit ordinal α. By definition $\alpha_\alpha<\aleph_\beta$ when $\alpha<\beta$.

Then $\aleph_\alpha$ are all infinite initial ordinal numbers, and any infinite ordinal number is of the form $\aleph_\alpha$ for some ordinal α. So natural numbers together with alephs are just all the cardinal numbers.

Notice: to avoid confusion, when do arithmetic of ordinal numbers, $\aleph_\alpha$ is written as ω_α. ⌟

Proof: Use transfinite induction on α. The only nontrivial case is when α is a limit ordinal, where if $\gamma<\aleph_\alpha$ and $|\gamma|=|\aleph_\alpha|$, then there is a $\beta<\alpha$ that $\gamma\le\aleph_\beta$ by definition, so $|\aleph_\alpha|<|\gamma|\le|\aleph_\beta|<|\aleph_\alpha|$ as $\aleph_\beta$ is an initial ordinal.

To prove that any infinite initial ordinal is an aleph, first notice that $\alpha<\aleph_\alpha$ by a simple transfinite induction. So we may use transfinite induction on the following assertion for α: if $\Omega<\aleph_\alpha$, then there is a $\gamma<\alpha$ that $\Omega=\aleph_\gamma$. For this, $\alpha=0$ is trivially true, if $\alpha=\beta+1$, then $\Omega<h(\aleph_\alpha)$ implies that $|\Omega|<|\aleph_\alpha|$ by definition. Because Ω is initial, $\Omega=\aleph_\beta$ or $\Omega<\aleph_\beta$, so by induction hypothesis it is true. If α is a limit ordinal, then $\Omega<\omega_\beta$ for some $\beta<\alpha$, so also by induction hypothesis it is true. □

Aleph Arithmetics

Prop. (2.2.8.3). $\aleph_\alpha\cdot\aleph_\alpha=\aleph_\alpha$. ⌟

Proof: Cf.[Set Theory Jech P134]. □

Cor. (2.2.8.4). $\aleph_\alpha\cdot\aleph_\beta=\aleph_\beta$ for $\alpha\le\beta$, and $n\cdot\aleph_\beta=\aleph_\beta$.

So $\aleph_\alpha+\aleph_\beta=\aleph_\beta$ for $\alpha\le\beta$, and $n+\aleph_\beta=\aleph_\beta$. ⌟

9 Natural Numbers and Real Numbers

Prop. (2.2.9.1). $\mathbb{R}$ is the unique ordered field in which every non-empty bounded set has a least upper bound. ⌟

Proof: □

Prop. (2.2.9.2). $(\mathbb{N},<)$(2.2.1.5) is a well-ordered set. ⌟

Proof: □

Example (2.2.9.3) [Examples of Countable Sets].

- $\mathbb{Z}$.
- $\mathbb{Q}$.

⌟

Arithmetic of Real numbers

Prop. (2.2.9.4). The set of real numbers $\mathbb{R}$(2.2.3.24) can be endowed with a field structure, making it an ordered field. ⌟

Proof: Cf.[Set Theory Jech P175]. □

Prop. (2.2.9.5). $\mathbb{R}$ satisfies the least upper bound hypothesis. ⌟

Proof: □

10 Filters and Ultrafilters

Def. (2.2.10.1)[Filter]. For a poset P, a **filter** on P is a subset F that

- If $p < q$ and $p \in F$, then $q \in F$.
- If $p, q \in F$, then there is an $r \in F$ that $r < p, r < q$.

⌟

Def. (2.2.10.2) [Filter on Sets]. Let S be a non-empty set, a **filter** on S is a filter F on $\mathcal{P}(S)$ that $\varnothing \notin F$.

an **ideal** on S is a collection F of subsets of S that:

- $\varnothing \in F$ and $S \notin F$.
- If $X, Y \in F$, then $X \cup Y \in F$.
- If $X \in F, X \supset Y$, then $Y \in F$.

An ideal is just the dual(complement) of a filter. ⌟

Def. (2.2.10.3)[Finite intersection property]. A family of subsets of a set is said to have the **finite intersection property** if any finite collection of elements of this family is non-empty. ⌟

Lemma (2.2.10.4). let G be a collection of subsets of S that has the finite intersection property(2.2.10.3), then there is a smallest filter F that $G \subset F$. It is just the collection of subsets of S that contain some finite intersection set of elements of G. ⌟

Def. (2.2.10.5)[Ultrafilter]. An **ultrafilter** is a filter F that for every subset X, $X \in F$ iff $S - X \notin F$. A **prime ideal** is an ideal that for every subset X, $X \in F$ iff $S - X \notin F$.

A ultrafilter is equivalent to a maximal filter. And it is equivalent to a $\{0, 1\}$-valued finitely additive measure on S. ⌟

Proof: If F is an ultrafilter, then it is maximal, because any larger filter will have some $X, S - X$, thus has $\varnothing$, contradiction.

Conversely, if F is maximal filter but not ultra, then there is a X that $X \notin F$, $S - X \notin F$. Let $G = F \cup \{X\}$, then any finite intersection of elements of G is not empty: $X_1 \cap \ldots \cap X_n \cap X \neq 0$ otherwise $S - X \in F$. So there is a filter containing G by(2.2.10.4), contradiction. □

Prop. (2.2.10.6) [Pushforward of Filters]. If $\mathcal{F}$ is a(n) (ultra)filter on X and $f : X \to Y$ is a function, then $f_*(\mathcal{F}) = \{A \subset Y | f^{-1}(A) \in \mathcal{F}\}$ is a(n) (ultra)filter on X, called the **pushforward filter** of $\mathcal{F}$. ⌟

Prop. (2.2.10.7). For an ultrafilter $\mathcal{F}$ on X , if $U_i \notin \mathcal{F}$, then $\sum_{i=1}^n U_i \notin \mathcal{F}$. ⌟

Proof: As $X - U_i \in \mathcal{F}$, there intersection are in $\mathcal{F}$, so its complement is not in $\mathcal{F}$. □

Prop. (2.2.10.8). Any filter can be extended to an ultrafilter(maximal filter), if the axiom of choice is used. ⌟

Proof: Use Zorn's lemma(2.2.5.3). It suffices to prove that a union of a chain of filters is a filter, which is trvial. □

Cor. (2.2.10.9). Non-principal ultrafilter exists on any infinite set. And in fact, any non-principal ultrafilter contains all the cofinite sets.

For any non-principle ultrafilter, it cannot contains a single pt $\{x\}$, so it contains every cofinite set. ⌟

Proof: Consider any ultrafilter containing the filter of cofinite sets of S, then it is non-principal. □

Def. (2.2.10.10) [κ-Completeness]. Let κ be an uncountable cardinal, then a field F on a set S is called **κ-complete** if for every cardinal $\lambda < \kappa$, if $X_\alpha \in F$ for every $\alpha < \lambda$, then $\cap_{\alpha<\lambda} X_\alpha \in F$.

An $\aleph_1$-complete filter is also called a σ-complete filter. ⌟

Closed unbounded and Stationary Set

Silver's Theorem

11 Models

Cf.[Axiomatic Set Theory]P12.

Def. (2.2.11.1). ⌟

Absoluteness

12 Large Cardinals

Def. (2.2.12.1) [Abstract Measures]. Let S be a non-empty set, then an **abstract measure** on S is a non-trivial probabilistic measure μ on the measurable space $(S, \mathscr{P}(S))$ that $\mu(\{a\}) = 0$ for any $a \in S$. ⌟

Def. (2.2.12.2) [Regular Cardinal]. A cardinal is called **regular** if it is not a sum of λ cardinals κ_i that $\lambda < \kappa$ and $\kappa_i < \kappa$. ⌟

Def. (2.2.12.3)[Strong Limit]. A cardinal κ is called a **strong limit** if $2^\lambda < \kappa$ for any $\lambda < \kappa$(2.2.12.3). ⌟

Def. (2.2.12.4)[Strongly Inaccessible Cardinal]. A cardinal κ is called **strongly inaccessible(SI)** if it is regular(2.2.12.2) and is a strongly limit. ⌟

Def. (2.2.12.5)[Weakly Inaccessible Cardinal]. A cardinal κ is called **weakly inaccessible** if it is regular and is a limit cardinal. ⌟

Prop. (2.2.12.6)[Measure and CH]. If there exists an abstract measure on $2^{\aleph_0}$, then the Continuum Hypothesis(2.2.7.8) fails. ⌟

Proof: Cf.[Jec03]P242. □

Prop. (2.2.12.7). If there is a measure on a set S, then some cardinal $\kappa \leq |S|$ is weakly inaccessible. ⌟

Proof: Cf.[Jec03]P243. □

Prop. (2.2.12.8). Let μ be a $\{0,1\}$-valued measure on S, then $U = \{X \subset S | \mu(X) = 1\}$ is a non-principal σ-complete ultrafilter of S ⌟

Prop. (2.2.12.9) [Stanislaw-Ulam Dichotomy]. If there exists a measure on some set, then either there exists a $\{0,1\}$-valued measure on some set, or there exists a measure on $2^{\aleph_0}$. ⌟

Proof: Cf.[Jec03]P245. □

Def. (2.2.12.10) [Measurable Cardinals]. A **measurable cardinal** is an uncountable cardinal κ on which there exists a non-principal κ-complete ultrafilter. ⌟

Prop. (2.2.12.11). A measurable cardinal is strongly inaccessible. ⌟

Proof: Cf.[Jec03]P247. □

13 Gödel Model

Thm. (2.2.13.1) [Gödel Incompleteness Theorem]. For any set of axioms for elementary number theory, there will always be statements which can be formulated in an elementary way, and which are decidable, but which can not be deduced using only elementary methods. ⌟

Proof: □

Remark (2.2.13.2). This theorem gives a reason why many theorems, for examples the Fermat's last theorem, must be proven using analytic methods or geometric methods. ⌟

14 Silver Machine

15 Forcing

Def. (2.2.15.1) [Dense Subset]. In a poset P, a subset $D \subset P$ is called **dense** if for any $p \in P$, there is a $q \in D$ that $q < p$. If $\mathcal{D}$ is a collection of dense subsets of P, a filter $G \subset P$ is called **$\mathcal{D}$-generic** if $D \cap G \neq \varnothing$ for all $D \subset \mathcal{D}$. ⌟

Prop. (2.2.15.2). If $\mathcal{D}$ is a countable collection of dense subsets of P, then there is a $\mathcal{D}$-generic filter G. ⌟

Proof: Let $\mathcal{D} = \{D_1, \ldots, D_n, \ldots\}$. Choose $p_0 \in P$, and consecutively choose $p_n \leq p_{n-1}$ that $p_n \in D_n$, and define $G = \{q | q \geq p_n \text{ for some } n\}$. □

Axiom (2.2.15.3) [Martin's Axiom]. If P is a partially ordered set satisfying the countable chain condition(2.2.3.7), and D is a collection of dense subsets of P with $|D| < 2^{\aleph_0}$, then there is a D-generic filter on P. ⌟

16 Determinacy

17 Stationary Set

2.3 Homotopy Type Theory

2.4 Model Theory

References are [Model Theory Marker]. The exercises of [Model Theory Marker] are important.

Notation (2.4.0.1).

- Use notations defined in Set Theory.
- All propositions from now are wffs in class theory(or with choice or large cardinal), so there are no metatheorems.

⌟

1 Set Models

Basics

Def. (2.4.1.1) [Structures]. Given a mathematical language $\mathcal{L}$(2.1.6.1), an **$\mathcal{L}$-structure** on a set M is an assignment for each constant symbol c an element $c^M \in M$, for each function symbol f of arity n a function $f^M : M^n \to M$, and for each relation symbol R of arity m a subset $R^M \subset M^m$. These c^M, f^M, R^M are called **interpretations** of $\mathcal{L}$.

And there is a natural definition of morphisms of $\mathcal{L}$-structures, and an injective morphism of $\mathcal{L}$-structures is called an embedding or a **structure extension**. ⌟

Def. (2.4.1.2) [Satisfaction]. Let φ be a formula with free variables $\overline{v} = (v_{i_1}, \ldots, v_{i_m})$, then we inductively define $\mathcal{M} \models \varphi(\overline{a})$ as follows:

- If φ is $t_1 = t_2$ where t_1, t_2 are terms, then $\mathcal{M} \models \varphi(\overline{a})$ if $\sqcup_1^{\mathcal{M}}(\overline{a}) = t_2^{\mathcal{M}}(\overline{a})$.
- If φ is $R(t_1, \ldots, t_n)$, then $\mathcal{M} \models \varphi(\overline{a})$ if $(t_1^{\mathcal{M}}(\overline{a}), \ldots, t_n^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{M}}$.
- If φ is $\neg\psi$, then $\mathcal{M} \models \varphi(\overline{a})$ if $\mathcal{M} \not\models \psi(\overline{a})$.
- If φ is $\psi \wedge \theta$, then $\mathcal{M} \models \varphi(\overline{a})$ if $\mathcal{M} \models \psi(\overline{a})$ and $\mathcal{M} \models \theta(\overline{a})$.
- If φ is $\exists v_j \psi(\overline{v}, v_j)$, then $\mathcal{M} \models \varphi(\overline{a})$ is there is a $b \in M$ that $\mathcal{M} \models \psi(\overline{a}, b)$.

and we say M **satisfies** $\varphi(\overline{a})$, or $\varphi(\overline{a})$ is true in M. Notice if there is no free variables, $\varphi(\overline{a})$ just writes φ. ⌟

Def. (2.4.1.3) [Mathematical $\mathcal{L}$-Theory]. Let $\mathcal{L}$ be a mathematical language, then a (mathematical)**$\mathcal{L}$-theory** is a formal system that is a consistent extension of $\mathscr{K}_{\mathcal{L}}$(2.1.5.2). ⌟

Def. (2.4.1.4) [Models]. If T is an $\mathcal{L}$-theory and $\mathcal{M}$ a set with $\mathcal{L}$-structure satisfying all theorems $\varphi \in T$, then $\mathcal{M}$ is called a **model** of T, and writes $M \models T$.

A theory T is called **satisfiable** iff there is a model $\mathcal{M}$ for T.

A set of $\mathcal{L}$-structures $\mathcal{K}$ is called an **elementary class** iff there is an $\mathcal{L}$-theory T that $\mathcal{K} = \{\mathcal{M} | \mathcal{M} \models T\}$.

Given a $\mathcal{L}$-structure on M, the **theory of** M is the set of all sentences true in M.

Two $\mathcal{L}$-structures $\mathcal{M}$ and $\mathcal{N}$ are called **elementary equivalent**, denoted by $\mathcal{M} \equiv \mathcal{N}$, if for all $\mathcal{L}$-sentences φ, $\mathcal{M} \models \varphi \iff \mathcal{N} \models \varphi$. ⌟

Prop. (2.4.1.5). If T is a mathematical $\mathcal{L}$-theory given by axioms, and every axiom of M is a set with $\mathcal{L}$-structure satisfying every axiom, then $\mathcal{M}$ is a model of T. ⌟

Proof: This follows from induction on the length of the proof of a theorem. □

Prop. (2.4.1.6). A mathematical $\mathcal{L}$-theory is consistent iff it has a model. ⌟

Proof: Cf.[Hamilton]P91+98.**?** □

Prop. (2.4.1.7) [Quantifier-Free Formulae]. Suppose $\mathcal{M}$ is a substructure of $\mathcal{N}$ and $\overline{a}$ is a tuple in $\mathcal{M}$. If $\varphi(\overline{v})$ is a quantifier-free formula, then $\mathcal{M} \models \varphi(\overline{a})$ iff $\mathcal{N} \models \varphi(\overline{a})$. ⌟

Proof: Cf.[Model Theory P11]. □

Prop. (2.4.1.8). If $\mathcal{L}$-structures $\mathcal{M} \cong \mathcal{N}$, then $\mathcal{M}$ is elementarily equivalent to $\mathcal{N}$. ⌟

Proof: This seemingly trivial proposition still needs proof, and the proof uses induction, just as that of(2.4.1.7). □

Def. (2.4.1.9) [Logical Consequence]. Let T be an $\mathcal{L}$-theory and φ an $\mathcal{L}$-sentence, then φ is called a **logical consequence** of $\mathcal{T}$, writes $T \models \varphi$, if for any $\mathcal{L}$-structure $\mathcal{M}$ that $\mathcal{M} \models T$, $\mathcal{M} \models \varphi$. ⌟

Definable Sets and Interpretability

Def. (2.4.1.10) [Definable Sets]. Let $\mathcal{M}$ be an $\mathcal{L}$-structure(2.4.1.1), a subset $X \subset \mathcal{M}^n$ is called a **definable set** iff there is an $\mathcal{L}$-formula $\varphi(v_1, \ldots, v_n, w_1, \ldots, w_m)$ and a tuple $\underline{b} \in \mathcal{M}^m$ that $X = \{\underline{a} \in M^n : \mathcal{M} \models \varphi(\underline{a}, \underline{b})\}$. Moreover if $A \subset \mathcal{M}$, $X \subset \mathcal{M}^n$ is called an A-**definable set** iff $y_i \in A$. ⌟

Prop. (2.4.1.11) [Examples of Definable Sets]. The definability of some sets are often nontrivial, using many number theories. For example, Cf.[Marker P20]. ⌟

Prop. (2.4.1.12). There is an inductive characterization of definable sets, Cf.[Marker P22]. ⌟

Prop. (2.4.1.13). If $\mathcal{M}$ is an $\mathcal{L}$-structure, If $X \subset \mathcal{M}^n$ is A-definable, then very $\mathcal{L}$-automorphism of $\mathcal{M}$ that fixes A pointwise will fixes X setwise. ⌟

Proof: For an automorphism τ of $\mathcal{M}$, $\mathcal{M} \models \varphi(\overline{b}, \overline{a})$ iff $\mathcal{M} \models \varphi(\tau(\overline{b}), \tau(\overline{a})) = \varphi(\tau(\overline{b}), \overline{a})$. □

Cor. (2.4.1.14). $\mathbb{R}$ is not definable in $\mathbb{C}$. ⌟

Proof: If $\mathbb{R}$ is definable, it is definable over a finite set $A \subset \mathbb{C}$, Let r, s be algebraically independent over $\mathbb{A}$ and $r \in \mathbb{R}, s \notin \mathbb{R}$. This can be done, otherwise $\mathbb{C}$ or $\mathbb{R}$ is finite transcendental over $\mathbb{Q}$, then $|\mathbb{C}| = |\mathbb{Q}|$(3.2.7.3), which is impossible by(2.2.3.24). Then there is an automorphism σ of $\mathbb{C}$ fixing A that $\sigma(r) = s$, so $\mathbb{R}$ is not definable by(2.4.1.13). □

Def. (2.4.1.15) [Definably Interpretability]. An $\mathcal{L}_0$-structure $\mathcal{N}$ is called **definably interpreted** in an $\mathcal{L}$-structure $\mathcal{M}$ if there is a definable set $X \subset \mathcal{M}^n$ that we can interpret the symbols of $\mathcal{L}_0$ as definable subsets and functions of X and the resulting $\mathcal{L}_0$-structure is isomorphic to $\mathcal{N}$.

The usual example is that the group structure of $GL_2(K)$ is definably interpreted in the ring structure of a field. ⌟

Def. (2.4.1.16) [Interpretability and Quotient Construction]. An $\mathcal{L}_0$-structure $\mathcal{N}$ is called **interpretable** in an $\mathcal{L}$-structure $\mathcal{M}$ iff there is a definable set $X \in \mathcal{M}^n$ and a definable equivalence relation E on X, that we can interpret the symbols of $\mathcal{L}_0$ as definable subsets and functions of X/E and the resulting $\mathcal{L}_0$-structure is isomorphic to $\mathcal{N}$.

The usual example is that the set structure of a projective space is interpretable in the ring structure of a field. ⌟

Prop. (2.4.1.17). Any structure for a countable language can be interpreted in a graph. ⌟

Proof:

□

2 Basic Techniques

Def. (2.4.2.1) [Definitions for Theories]. A theory T is said to have the **witness property** iff whenever $\varphi(v)$ is an $\mathcal{L}$-formula with one free variable v, there is a constant symbol c that $T \models (\exists v\varphi(v) \to \varphi(c))$.

A theory T is called **maximal** iff for any $\mathcal{L}$-sentence, either $\varphi \in T$ or $\neg\varphi \in T$.

A theory T is called **complete** iff for any $\mathcal{L}$-sentence, either $T \models \varphi$ or $T \models \neg\varphi$. ⌟

Def. (2.4.2.2) [Consistent Theory]. A theory T is called **inconsistent** if there is a sentence φ that $T \vdash \varphi \wedge \neg\varphi$, otherwise it is called **consistent**. ⌟

Def. (2.4.2.3) [Recursiveness and Decidablility]. A language $\mathcal{L}$ is called **recursive** iff there is an algorithm that decides whether a sequence of symbols is an $\mathcal{L}$-formula.

An $\mathcal{L}$-theory T is called **recursive** iff there is an algorithm that decides whether a given $\mathcal{L}$-sentence is in T.

An $\mathcal{L}$-theory T is called **decidable** iff there is an algorithm that decides whether a given φ satisfies $T \models \varphi$. ⌟

Prop. (2.4.2.4). If $\mathcal{L}$ is a recursive language and T is a recursive $\mathcal{L}$-structure, then $\{\varphi | T \vdash \varphi\}$ is recursively enumerable. ⌟

Proof: There is a computable listing $\sigma_1, \ldots, \sigma_n \ldots$ of all the finite sequences of $\mathcal{L}$-formulas, because $\mathcal{L}$ is recursive. Then we can check at each stage iff σ_i is a proof of φ. This involves checking if each formula is in T(checkable because T is recursive) or it is a simple consequences of formulae before it, and finally check the last formula is φ. If σ_i is a proof of φ, then halt, otherwise go on to check σ_{i+1}. □

Prop. (2.4.2.5). The halting computation set is not computable. ⌟

Proof: Cf.[Mathematical Logic Shoenfield]**?**. □

Cor. (2.4.2.6). The full theory $Th(\mathbb{N})$ of the ring structure of $\mathbb{N}$ is undecidable. ⌟

Proof: If such an algorithm exists, then we can use it to compute whether the sentence

$$\varphi(e,x) = \exists s T(\underbrace{1+\ldots+1}_{e-\text{times}}, \underbrace{1+\ldots+1}_{x-\text{times}}, s)$$

is computable. Then this will contradicts the fact that halting computation set is not computable(2.4.2.5). □

Prop. (2.4.2.7) [Gödel's Completeness Theorem]. Let T be an $\mathcal{L}$-theory and φ is an $\mathcal{L}$-sentence, then $T \models \varphi$ iff $T \vdash \varphi$. ⌟

Proof: **?** □

Cor. (2.4.2.8) [Consistent and Satisfiable]. A theory T is consistent iff it is satisfiable. ⌟

Proof: If T is satisfiable, then it is clearly consistent, and if T is not satisfiable, then there are no models for T, so $T \models \varphi \wedge \neg\varphi$ by definition, so $T \vdash \varphi \wedge \neg\varphi$ by Gödel's completeness theorem. □

Cor. (2.4.2.9) [Lemma on Constants]. Suppose $T \vdash \varphi(\overline{c})$ and $\overline{c}$ is a tuple of constants not appearing in T, then $T \vdash \forall x\varphi(x)$. ⌟

Proof: We use the Gödel's completeness theorem(2.4.2.7), and notice this theorem is obviously true for $\vdash$ replaced by $\models$. Notice we can add the constants to $\mathcal{L}$, thus $\varphi(\overline{c})$ has no free variables. □

Ultraproducts of Theories

Def. (2.4.2.10) [Ultraproducts of Theories]. If $M_i, i \in I$ is a collection of $\mathcal{L}$-structures and $\mathcal{F}$ is an ultrafilter on I, then the **ultraproduct** $\prod_I M_i/\mathcal{F}$ of M_i is a $\mathcal{L}$-structure defined as:

- The underlying set $M = \prod M_i/\sim$, where $(a_i) \sim (b_i)$ iff $\{i \in I | a_i = b_i\} \in \mathcal{F}$, which is an equivalent relation.
- If c is a constant symbol, then $c^M = (c^{M_i})$.
- If f is a function symbol, then $f^M([a_{i1}], \ldots, [a_{in}]) = [f^{M_i}(a_{i1}, \ldots, a_{in})]$.
- If R is a relation symbol, then $([a_{i1}], \ldots, [a_{in}]) \in R^M$ iff $\{i \in I | (a_{i1}, \ldots, a_{in}) \in R^{M_i}\} \in \mathcal{F}$.

⌟

Prop. (2.4.2.11) [Los Theorem]. Let $M_i, i \in I$ be $\mathcal{L}$-structures and $\mathcal{F}$ be an ultrafilter on I. Let $\varphi(\overline{x})$ be a first-order logic formula in the free variables $\overline{x}$, and let $\overline{[(a_i)]}$ be a tuple of elements from $\prod_I M_i/\mathcal{F}$, then

$$\prod_I M_i/\mathcal{F} \models \varphi(\overline{[(a_i)]}) \iff \{i \in I | M_i \models \varphi_i(\overline{a_i})\} \in \mathcal{F}.$$

⌟

Proof: The proof is by induction, which is routine, Cf.[Model Theory for Algebra and Algebraic Geometry, P22]. □

Cor. (2.4.2.12). An ultraproduct of models for a theory T is also a model for T. ⌟

Cor. (2.4.2.13) [Non-Standard Model for Th($\mathbb{R}$)]. Consider $\mathbb{R}$ in the language $\mathcal{L}_r$, where L_r is the language of rings, (i.e., the ring structure), let $\mathcal{F}$ be a non-principle ultrafilter on $\mathbb{N}$(2.2.10.9), and consider the ultraproduct $\mathcal{R} = \prod_{i\in\mathbb{N}} \mathbb{R}/\mathcal{F}$, which is called an **ultrapower** of $\mathbb{R}$.

Notice each factor satisfies $Th(\mathbb{R})$, so $\mathcal{R}$ also satisfies $Th(\mathbb{R})$. ⌟

Cor. (2.4.2.14). Using ultraproduct construction, we can find a field of characteristic 0 that has exactly one algebraic extension in each degree. ⌟

Proof: Just use the field model $\mathbb{F}_p$ for all p and construct their ultraproduct w.r.t. a non-principal ultrafilter. □

Prop. (2.4.2.15) [Keiler-Shelah Theorem]. Two $\mathcal{L}$-structures $\mathcal{M}$ and $\mathcal{N}$ are elementary equivalent iff there is an index set I and an ultrafilter $\mathcal{F}$ on I that $\prod_I M/\mathcal{F} \cong \prod_I N/\mathcal{F}$. ⌟

Proof: Cf.[C. C. Chang and H. J. Keisler, Model Theory 6.1.15]. □

Compactness Theorem and Henkin Construction

Lemma (2.4.2.16). Suppose T is a maximal and finitely satisfiable $\mathcal{L}$-theory with the witness property, then T is satisfiable. In fact, T has κ constant symbols, then there is a model $\mathcal{M} \models T$ that $|\mathcal{M}| \leq \kappa$. ⌟

Proof: Cf.[Marker, P35]. □

Lemma (2.4.2.17). Let $\mathcal{L}$ be a finitely satisfiable $\mathcal{L}$-theory, then there is a language $\mathcal{L} \subset \mathcal{L}^*$ and a $T \subset T^*$ a finitely satisfiable $\mathcal{L}^*$-theory that any $\mathcal{L}^*$-theory extending T^* has the witness property. And we can choose $|\mathcal{L}^*| = |\mathcal{L}| + \aleph_0$. ⌟

Proof: We first show there is a language $\mathcal{L} \subset \mathcal{L}_1$ and a finitely satisfiable $\mathcal{L}_1$-theory $T \subset T_1$ that witnesses all $\mathcal{L}$-formulae: We add a constant symbol c_φ for each $\mathcal{L}$-formula φ, and add sentences $(\exists v\varphi(v)) \to \varphi(c_\varphi)$ to T, then this T_1 is finitely satisfiable, because for any finite subset Δ of T_1, only f.m. constant symbols appear, and we have a model $\mathcal{M}$ for $\Delta \cap T$, thus we can interpret c_φ as the element a that $\mathcal{M} \models \varphi(a)$, if $\mathcal{M} \models \exists v\varphi(v)$. Now we can inductively define L_n, T_n, and consider their union, then this satisfies the desired conditions. And the cardinality is also clear. □

Lemma (2.4.2.18). If T is a finitely satisfiable $\mathcal{L}$-theory, then there is a maximal(2.4.2.1) finitely satisfiable $\mathcal{L}$-theory $\mathcal{L} \subset \mathcal{L}'$. ⌟

Proof: it is easy to construct a maximal satisfiable $\mathcal{L}$-theory, and it is truly maximal in sense of(2.4.2.1): for any sentence φ, if $T \cup \varphi$ is not finitely satisfiable, then there is a finite set $\Delta \subset T$ that $\Delta \models \neg\varphi$. Then we claim $T \cup \neg$ is finitely satisfiable: for another finite set Σ, because $\Delta \cup \Sigma$ is finitely satisfiable and $\Delta \models \neg\varphi$, $\Sigma \cup \neg\varphi$ is satisfiable. □

Prop. (2.4.2.19) [Strong Compactness Theorem]. If T is a finitely satisfiable $\mathcal{L}$-theory and κ is an infinite cardinal that $\kappa > |\mathcal{L}|$, then there is a model of T of cardinality at most κ. ⌟

Proof: By(2.4.2.17), we get a desired language $\mathcal{L}^*$ of cardinality$\leq \kappa$, and a theory $\mathcal{T}^*$, and by(2.4.2.18), we can assume T^* is maximal and finitely satisfiable, and it has the witness property. Then(2.4.2.16) says there is a model of cardinality$\leq \kappa$. □

Cor. (2.4.2.20) [Compactness Theorem]. A theory T is satisfiable iff every finite subset of T is satisfiable. ⌟

Remark (2.4.2.21). Notice the compactness theorem is also a consequence of the completeness theorem(2.4.2.7): if T is not satisfiable, then it is not consistent by(2.4.2.8). Let σ be a proof of a contradiction in T, then σ consists of f.m. sentences in T, which consists of a finite unsatisfiable subset T_0 of T.

It is clear provable using ultrafilters: If there is a family of structures $\{M_\Delta\}$ indexed by the collection of all finite subsets of T, with $M_\Delta \models \Delta$ for all $\Delta \in I$ where I is the set of all finite subsets of T.

Then we want to find an ultrafilter $\mathcal{F}$ on I that for all $\varphi \in T$, $\{\Delta | M_\Delta \models \varphi\} \in \mathcal{F}$, then we can use Leo's theorem(2.4.2.11) to show that $\prod_I M_\Delta/\mathcal{F}$ is a model for all $\varphi \in T$. Now in fact we make pick a ultrafilter over the filter generated by all the $A_\varphi = \{\Delta | \varphi \in \Delta\}$, because $M_\Delta \models \Delta$. In fact, this is the case because A_φ has the finite intersection property trivially. ⌟

Cor. (2.4.2.22). If $T \models \varphi$, then $\Delta \models \varphi$ for some finite $\Delta \subset T$. ⌟

Proof: If not, then $\Delta \cup \{\neg\varphi\}$ is satisfiable for all finite $\Delta \subset T$, so $T \cup \{\neg\varphi\}$ is finitely satisfiable, thus satisfiable by compactness theorem, but this cannot be true because $T \models \varphi$. □

Cor. (2.4.2.23) [Torsion Elements]. Let $\mathcal{L}$ be a language containing $\{\cdot, e\}$, the language of groups, and T is a theory extending the theory of groups, let $\varphi(v)$ be an $\mathcal{L}$-formula. If for any n there is a $G_n \models T$ and G_n has an element of finite order greater than n, then there is an $\mathcal{L}$-structure G that $G \models T$ and G has an element of infinite order.

In particular, there is no formula that defines the torsion elements in any models for T. ⌟

Proof: Consider a new language $\mathcal{L}^* = \mathcal{L} \cup \{c\}$, and T^* an $\mathcal{L}^*$-theory that

$$T^* = T \cup \{\varphi(c)\} \cup \{\neg(\underbrace{c \cdots c \ldots c}_{n-\text{times}} = e)\},$$

then the theory T^* is finitely satisfiable by hypothesis, so T^* is satisfiable by compactness theorem. □

Cor. (2.4.2.24) [Element Larger than All Natural Number]. Consider $\mathcal{L}$ the language of ordered rings, let $\mathrm{Th}(\mathbb{N})$ be the theory of $\mathbb{N}$, then there is an $\mathcal{L}$-structure $\mathcal{M}$ that $\mathcal{M} \models \mathrm{Th}(\mathbb{N})$ and $\mathcal{M}$ has an element that is larger than every natural number. ⌟

Proof: The same proof as that of(2.4.2.23), but use

$$T^* = \mathrm{Th}(\mathbb{N}) \cup \{\underbrace{1 + \ldots + 1}_{n-\text{times}} < c\}$$

□

Prop. (2.4.2.25) [Model of a Given Cardinality]. If T is an $\mathcal{L}$-theory with infinite models, then if κ is an infinite cardinal that $\kappa \geq |\mathcal{L}|$, then there is a model of T of cardinality κ. ⌟

Proof: Let $\mathcal{L}^* = \mathcal{L} \cup \{c_\alpha : \alpha < \kappa\}$, where c_α are pairwise different new constants, and T^* be the $\mathcal{L}^*$ theory $T \cup \{c_\alpha \neq c_\beta, \alpha < \beta < \kappa\}$, then any model for T^* must has cardinality$\geq \kappa$. But then we use strong compactness theore(2.4.2.19), it suffices to show T^* is finitely satisfiable: for any finite $\Delta \subset T^*$, there are only f.m. new constant symbols, thus we can use the infinite model $\mathcal{M}$ to interpret the constant symbols randomly, thus we are done. □

Complete Theories

Def. (2.4.2.26) [Categorial Theories]. Let κ be an infinite cardinal and T is a theory with models of size κ. T is called **κ-categorical** iff any two models of T of cardinality κ are isomorphic. ⌟

Prop. (2.4.2.27). The theory of torsion-free divisible Abelian groups is κ-categorical for all $\kappa > \aleph_0$. ⌟

Proof: A torsion-free Abelian group is just a vector space over $\mathbb{Q}$. Thus the conclusion is trivial, just notice for a cardinal $\kappa > \aleph_0$, a vector space of dimension κ has cardinality κ. □

Prop. (2.4.2.28) [Vaught's Test]. Let T be a satisfiable theory with no finite models, if L is κ-categorical for some $\kappa \geq |\mathcal{L}|$, then T is complete. ⌟

Proof: If there is a sentence φ that $T \not\models \varphi$ and $T \not\models \neg\varphi$, so $T_0 = T \cup \{\varphi\}$ and $T_1 = T \cup \{\neg\varphi\}$ is satisfiable. They both have infinite models by hypothesis, so by(2.4.2.25) there are models of cardinal κ for T_0 and T_1, but they cannot be isomorphic, contradiction. So T is complete. □

Prop. (2.4.2.29) [Recursive Complete Satisfiable is Decidable]. If T is a recursive complete satisfiable theory in a recursive language $\mathcal{L}$, then T is decidable. ⌟

Proof: Because T is satisfiable, The set of all φ that $\mathcal{M} \models \varphi$ and the set of all φ that $\mathcal{M} \models \neg\varphi$ are disjoint, and their sum is the set of all sentences by completeness. By Gödel's completeness theorem, this is equivalent to $\mathcal{M} \vdash \varphi$ or $\mathcal{M} \vdash \neg\varphi$. Then by(2.4.2.4), they are both enumerable, so it is decidable by definition. □

Up and Down(of Cardinality)

Def. (2.4.2.30) [Elementary Embedding]. An $\mathcal{L}$-structure embedding $i : \mathcal{M} \to \mathcal{N}$ is called an **elementary embedding**, denoted by $\mathcal{M} \prec \mathcal{N}$, if for any $\mathcal{L}$-formula φ,

$$\mathcal{M} \models \varphi(\overline{a}) \iff \mathcal{N} \models \varphi(i(\overline{a})).$$

Notice that one way implication is sufficient, because we can use negation.

Isomorphisms are elementary embeddings by(2.4.1.8). ⌟

Def. (2.4.2.31) [Diagrams]. Let $\mathcal{M}$ be an $\mathcal{L}$-structure, then we can add to $\mathcal{L}$ constant symbols for each element of M, and the class $Diag(M)$ of **atomic diagrams** of M is sentences of the form $\varphi(m_1, \ldots, m_n)$, where φ is an atomic $\mathcal{L}$-formula or the negation of an atomic $\mathcal{L}$-formula, and $\mathcal{M} \models \varphi(m_1, \ldots, m_n)$. And the class $Diag_{el}(M)$ of **elementary diagrams** of M is sentences of the form $\varphi(m_1, \ldots, m_n)$ where φ is an $\mathcal{L}$-formula that $\mathcal{M} \models \varphi(m_1, \ldots, m_n)$. ⌟

Prop. (2.4.2.32) [Diagrams and Embedding]. The diagram and elementary diagram is very important in constructing embeddings of theories: Let $\mathcal{N}$ be an $\mathcal{L}_M$-structure, then:

- If $\mathcal{N} \models Diag(M)$, there is an $\mathcal{L}$-embedding $\mathcal{M} \subset \mathcal{N}$.
- If $\mathcal{N} \models Diag_{el}(M)$, there is an elementary $\mathcal{L}$-embedding $\mathcal{M} \prec \mathcal{N}$.

⌟

Prop. (2.4.2.33) [Upward Löwenheim-Skolem Theorem]. Let $\mathcal{M}$ be an infinite $\mathcal{L}$-structure and κ be an infinite cardinal that $\kappa \geq |\mathcal{M}| + |\mathcal{L}|$, then there is an $\mathcal{L}$-structure $\mathcal{N}$ of cardinality κ that $\mathcal{M}$ embeds into $\mathcal{N}$. ⌟

Proof: $Diag_{el}(M)$ is clearly satisfiable, so by(2.4.2.25), there is an $\mathcal{L}^*$-model $\mathcal{N}$ of cardinality κ that $\mathcal{N} \models Diag_{el}(M)$. Then clearly $\mathcal{M} \prec \mathcal{N}$. □

Prop. (2.4.2.34) [Tarski-Vaught Test]. A substructure $\mathcal{M}$ of a structure $\mathcal{N}$ is an elementary substructure iff for any formula $\varphi(v, \overline{w})$ and $\overline{a} \in M$, if there is $b \in N$ that $\mathcal{N} \models \varphi(b, \overline{a})$, then there is a $c \in M$ that $\mathcal{N} \models \varphi(c, \overline{a})$. ⌟

Proof: Cf.[Marker P45].? □

Prop. (2.4.2.35) [(Downward)Löwenheim-Skolem Theorem]. Suppose $\mathcal{M}$ is an $\mathcal{L}$-structure and $X \subset \mathcal{M}$, then there is a elementary submodel $\mathcal{N}$ that $X \subset \mathcal{N}$ and $|\mathcal{N}| \leq |X| + |\mathcal{L}| + \aleph_0$. ⌟

Proof: Cf.[Marker P46]. □

Def. (2.4.2.36) [Universal Sentences]. A **universal sentence** is a sentence of the form $\forall v \varphi(v)$, where φ is quantifier-free.

For a theory T, denote by $T_\forall$ the set of all of the universal sentences φ that $T \models \varphi$.

A $\mathcal{L}$-theory T is said to have a **universal aximatization** iff there is a set of universal $\mathcal{L}$-sentences Γ that $\mathcal{M} \models T$ iff $\mathcal{M} \models \Gamma$. ⌟

Prop. (2.4.2.37) [Universal Axiomation]. An $\mathcal{L}$-theory T has a universal axiomatization iff for any $\mathcal{N} \subset \mathcal{M}$, if $\mathcal{M} \models T$, then $\mathcal{N} \models T$. ⌟

Proof: Cf.[Marker P47]. □

Prop. (2.4.2.38) [Universal Consequences]. If T is an $\mathcal{L}$-theory, then $\mathcal{A} \models T_\forall$ iff there is an $\mathcal{M} \models T$ that $\mathcal{A} \subset \mathcal{M}$. ⌟

Proof: If $\mathcal{A} \subset \mathcal{M}$, then $\mathcal{A} \models T_\forall$, by(2.4.2.37). Conversely, if $\mathcal{A} \models T_\forall$, then consider $Diag(\mathcal{A})$, then it suffices to show $Diag(\mathcal{A})$ is satisfiable. If it is not, then by compactness theorem(2.4.2.20) there is a finite set that is not satisfiable, and the part coming from diagrams of M can be expressed by a single formula $\chi(\overline{a})$, where χ is quantifier-free, $\overline{a} \in M$, $\mathcal{M} \models \chi(\overline{a})$, and we are saying that $T \cup \{\chi(\overline{a})\}$ is not satisfiable, then $T \models \neg\chi(\overline{a})$.

Now $T \models \forall\overline{x}\neg\varphi(\overline{x})$ as $\mathcal{L}$-theory because $\overline{a}$ can be designated arbitrarily, but this sentence is in $T_\forall$, thus $\mathcal{M} \models \forall\overline{x}\neg\varphi(\overline{x})$, in particular, $\mathcal{M} \models \neg\varphi(\overline{a})$, contradiction. □

Prop. (2.4.2.39) [Elementary Chain]. If $\mathcal{M}_i$ is a chain of $\mathcal{L}$-structures that $\mathcal{M}_i \prec \mathcal{M}_j$ for any $i < j$, then we can define there union $\mathcal{M} = \cup M_i$. Then $\mathcal{M}$ is an elementary extension of each $\mathcal{M}_i$. ⌟

Proof: Use induction on formulas to show that

$$\mathcal{M}_i \models \varphi(\overline{a_i}) \iff \mathcal{M} \models \varphi(\overline{a_i}),$$

for all $\mathcal{L}$-formulas φ. This is true for quantifier-free formula by(2.4.1.7), and if this is true for φ, ψ, then this is true for $\neg\varphi$ and $\varphi \wedge \psi$. For the sentence $\varphi = \exists v\psi(v, \overline{w})$, if $\mathcal{M}_i \models \psi(b, \overline{a})$ for some b, then so does $\mathcal{M}$. Conversely, if $\mathcal{M} \models \psi(b, \overline{a})$ for some b, then $b \in \mathcal{M}_j$ for some j, then $\mathcal{M}_j \models \varphi$, by the condition, $\mathcal{M}_i \models \varphi$ also. □

Back and Forth Argument

Cf.[Marker Chap2.4]. Some deep ideas are involved.

Prop. (2.4.2.40) [Cantor]. The theory DLO(2.1.6.3) is $\aleph_0$-categorical and complete. ⌟

Proof: It is $\aleph_0$-categorical by(2.2.3.12), and it is complete, by Vaught's test(2.4.2.28), as it has no finite models. □

3 Quantifier Elimination

Def. (2.4.3.1) [Quantifier Elimination]. A theory is said to have **quantifier elimination** if for each formula $\varphi(\overline{v})$, there is a quantifier free ψ that $T \models \forall\overline{v}(\varphi(\overline{v}) \leftrightarrow \psi(\overline{v}))$. ⌟

Lemma (2.4.3.2). Suppose $\mathcal{L}$ contains a constant symbol c, T is an $\mathcal{L}$-theory, and $\varphi(\overline{a})$ is an $\mathcal{L}$-formula, then the following are equivalent:

- There is a quantifier-free $\mathcal{L}$-formula $\psi(\overline{v})$ that $T \models \forall\overline{v}(\varphi(\overline{v}) \leftrightarrow \psi(\overline{v}))$.
- If $\mathcal{M}, \mathcal{N}$ are models of T, and $\mathcal{A}$ is an $\mathcal{L}$-structure that $\mathcal{A} \subset \mathcal{M} \cap \mathcal{N}$, then for all $\overline{a} \in \mathcal{A}$, $\mathcal{N} \models \varphi(\overline{a}) \iff \mathcal{M} \models \varphi(\overline{a})$.

⌟

Proof: $1 \to 2$ is clear, because a quantifier-free formula $\psi(\overline{a})$ is preserved under substructure by(2.4.1.7).

$2 \to 1$, Cf.[Marker, P74].**?** □

Lemma (2.4.3.3). Let T be an $\mathcal{L}$-theory that for any quantifier-free $\mathcal{L}$-formula $\theta(\overline{v}, w)$, there is a quantifier-free formula $\psi(\overline{v})$ that $T \models \forall\overline{v}(\exists w\theta(\overline{v}, w) \leftrightarrow \psi(\overline{v}))$, then T has quantifier elimination. ⌟

Proof: We want to show for each formula $\varphi(\overline{a})$, there is a quantifier-free formula $\psi(\overline{a})$ that $T \models \forall\overline{v}(\varphi(\overline{a}) \leftrightarrow \psi(\overline{v}))$, and we use induction on the complexity of φ.

If φ is quantifier-free, this is trivial. If $\varphi = \neg\theta_0$ or $\varphi = \theta_0 \wedge \theta_1$, then we are easily done. If $\psi(\overline{v}) = \exists w\theta(\overline{v}, w)$, and $T \models \forall\overline{v}(\theta(\overline{v}, w) \leftrightarrow \psi_0(\overline{v}, w))$, then $T \models \forall\overline{v}(\varphi(\overline{v}) \leftrightarrow \exists w\psi_0(\overline{v}, w))$. But the assumption shows there is a quantifier-free ψ that $T \models \forall\overline{v}(\exists w\psi_0(\overline{v}, w) \leftrightarrow \psi(\overline{v}))$, and then $T \models \forall\overline{v}(\varphi(\overline{v}) \leftrightarrow \psi(\overline{v}))$. □

Prop. (2.4.3.4) [Criterion for Quantifier Elimination]. Combining(2.4.3.2) and(2.4.3.3), we get: If T is an $\mathcal{L}$-theory that for all quantifier-free formula $\varphi(\overline{v}, w)$ and models $\mathcal{M}, \mathcal{N} \models T$, and $\mathcal{A} \subset M \cap N, \overline{a} \in A$, and if there is $b \in M$ that $\mathcal{M} \models \varphi(\overline{a}, b)$ will implie there is $c \in \mathcal{N}$ that $\mathcal{N} \models \varphi(\overline{a}, c)$, then T is quantifier-free. ⌟

Def. (2.4.3.5) [Algebraically Prime Models]. A theory T is said to have **algebraically prime models** if for any $\mathcal{A} \models T_\forall$(2.4.2.36), there is a $\mathcal{M} \models T$ and an embedding $i : \mathcal{A} \subset \mathcal{M}$ that for any other $\mathcal{N} \models T$, any embedding $j : \mathcal{A} \to \mathcal{N}$ factors through i. ⌟

Def. (2.4.3.6) [Simply Closed Model]. If $\mathcal{M}, \mathcal{N}$ are models of T, and $\mathcal{M} \subset \mathcal{N}$, then $\mathcal{M}$ is called **simply closed** in $\mathcal{N}$, denoted by $\mathcal{M} \prec_s \mathcal{N}$, iff for any quantifier-free formula $\varphi(\overline{a}, w)$ and $\overline{a} \in \mathcal{M}^n$, if $\mathcal{N} \models \exists w\varphi(\overline{a}, w)$, then so does $\mathcal{M}$. ⌟

Prop. (2.4.3.7) [Quantifier Elimination Test]. If T is an $\mathcal{L}$-theory that has algebraically prime models, and any inclusion of models for T is simply closed, then T has quantifier elimination. ⌟

Proof: This is an immediate consequence of(2.4.3.4). □

Def. (2.4.3.8) [Model-Complete]. An $\mathcal{L}$-theory T is called **model-complete** if for any two models $\mathcal{M}, \mathcal{N}$ for T, $\mathcal{M} \prec \mathcal{N}$(2.4.2.30) whenever $\mathcal{M} \subset \mathcal{N}$. A complete theoy is clearly model complete. ⌟

Prop. (2.4.3.9). let T be an $\mathcal{L}$-theory. If T has quantifier elimination, then T is model-complete. ⌟

Proof: If $\mathcal{M} \subset \mathcal{N}$, let $\varphi(\overline{a})$ be an $\mathcal{L}$-formula, and $\overline{a} \in \mathcal{M}$, then there is a quantifier-free formula $\psi(\overline{v})$ that $T \models \forall\overline{v}(\varphi(\overline{v}) \leftrightarrow \psi(\overline{v}))$. By(2.4.1.7), the formula $\psi(\overline{a})$ passes between $\mathcal{M}$ and $\mathcal{N}$, so

$$\mathcal{M} \models \varphi(\overline{a}) \iff \mathcal{M} \models \psi(\overline{a}) \iff \mathcal{N} \models \psi(\overline{a}) \iff \mathcal{N} \models \varphi(\overline{a}).$$

□

Prop. (2.4.3.10) [Minimal Model and Completeness]. If T is model-complete and there is a minimal model $\mathcal{M}_0$ that $\mathcal{M}_0$ embeds into every model of T, then T is complete. ⌟

Proof: Clearly any model is elementary equivalent to $\mathcal{M}_0$, thus clearly T is complete. □

Prop. (2.4.3.11) [Eliminating Algorithm]. Let T be a decidable theory with quantifier elimination, then there is an algorithm to find the elimination ψ of a given formula φ. ⌟

Proof: We just need to find a quantifier-free ψ that $T \models \forall\overline{v}(\varphi(\overline{v}) \leftrightarrow \psi(\overline{v}))$. This an effective search because T is decidable, and we can eventually find ψ because T has quantifier elimination. □

Examples of Quantifier Elimination

Prop. (2.4.3.12). The theory DLO(2.1.6.3) has quantifier elimination. ⌟

Proof: Cf.[Marker P72]. □

Lemma (2.4.3.13). DAG(2.1.6.3) has algebraically prime models. ⌟

Proof: This is just the alg.closure of the quotient field of an integral domain. □

Prop. (2.4.3.14). DAG has quantifier elimination. ⌟

Proof: We use(2.4.3.7) By(2.4.3.13), DAG has algebraically prime models, thus it suffices to show any inclusion of models for DAG(2.1.6.3) is simply closed: For any torsion-free divisible Abelian groups $H \subset G$, $\varphi(\overline{a}, w)$ quantifier-free, $\overline{a} \in H, b \in G$ that $G \models \varphi(\overline{a}, w)$. Then φ is a disjunction of conjunctions of atomic or negated atomic formulas, and we need to prove $H \models \varphi(\overline{a}, w)$.

So we may assume φ is conjunction of atomic formulas and negated atomic formuals:

$$\varphi(\overline{a}, w) \leftrightarrow \bigwedge(g_i + m_i w = 0) \wedge \bigwedge(h_i + m_i' w \neq 0).$$

If any $m_i \neq 0$, then $b \in H$. If all $m_i = 0$, then there are only f.m. constraints, and there is $b' \in H$ that $H \models \varphi(\overline{a}, b')$ because H is infinite. □

Cor. (2.4.3.15). The theory DAG is complete, by(2.4.3.10), as $(\mathbb{Q}, +, 0)$ embeds in every model of DAG, and(2.4.3.14)(2.4.3.9). ⌟

Prop. (2.4.3.16). The theory $ODAG$ is a complete theory with quantifier elimination. In particular, any ordered divisible Abelian group is elementarily equivalent to $(\mathbb{Q}, +, <)$, by completeness. ⌟

Proof: Cf.[Marker, P80]. □

Prop. (2.4.3.17) [Presburger Arithmetic]. Presburger arithmetic is a complete decidable theory with quantifier elimination in the language $\mathcal{L}^*$. ⌟

Proof: Cf.[Marker, P84]**?**. □

Minimal Structures and Minimal Theories

Def. (2.4.3.18) [Minimal Structures]. An $\mathcal{L}$-structure $\mathcal{M}$ is called a **minimal structure** if any definable set $X \subset M$ is either finite or cofinite. ⌟

Def. (2.4.3.19) [Quasi-Minimal Structures]. An $\mathcal{L}$-structure $\mathcal{M}$ is called a **quasi-minimal structure** if $\mathcal{M}$ is uncountable, and for any definable set $X \subset \mathcal{M}$ is either countable or uncountable. And it is called a **strongly quasi-minimal structure** if for any finite subset $A \subset \mathcal{M}$, each $\mathrm{Aut}_A(\mathcal{M})$-invariant subset of $\mathcal{M}$ is either countable or cocountable. ⌟

Def. (2.4.3.20) [Strongly-(Quasi-)Minimal Theories]. A **strongly-(quasi-)minimal theory** is a theory T s.t. any model $\mathcal{M} \models T$ is (quasi-)minimal. ⌟

Prop. (2.4.3.21). DAG(2.1.6.3) is a strongly-minimal theory. ⌟

Proof: Cf.[Marker P78]. □

4 Alg.Closed Fields

Lemma (2.4.4.1). ACF_p(2.1.6.3) is κ-categorical for all uncountable cardinal κ. ⌟

Proof: Because two alg.closed field of the same transcendental degree over the base field is isomorphic(3.2.7.4). The conclusion follows as an alg.closed field of transcendence degree κ has cardinality $\kappa + \aleph_0$. □

Prop. (2.4.4.2). The theory ACF_p is complete, by(2.4.4.1) and(2.4.2.28). ⌟

Cor. (2.4.4.3). ACF_p is decidable, in particular, Th($\mathbb{C}$), the first-order theory of the fields of complex numbers, is decidable. ⌟

Proof: ACF_p is complete by(2.4.4.1) and(2.4.2.28), it is clearly recursive, and it is clearly satisfiable, so use(2.4.2.29). □

Prop. (2.4.4.4) [First order Lefschetz Principle]. Let φ be a sentence in the language of rings, the following are equivalent:

1. φ is true in $\mathbb{C}$.
2. φ is true in every(some) alg.closed field of char 0.
3. For p large/there exists arbitrary large p, φ is true in any alg.closed field of char p.

⌟

Proof: $1, 2$ are equivalent because ACF_p is complete(2.4.4.2) and use Gödel's completeness theorem. If 2 is true, then $ACT_0 \models \varphi$, so by(2.4.2.22), then some $\Delta \models \varphi$. So for p sufficiently large, $ACF_p \models \Delta$, so $ACF_p \models \varphi$ for p large.

If $ACF_0 \not\models \varphi$, then $ACF_0 \models \neg\varphi$ by completeness(2.4.4.2), so by above argument, $ACF_p \models \neg\varphi$ for p large, contradiction. □

Cor. (2.4.4.5) [Ax]. Any injective polynomial map from $\mathbb{C}^n$ to $\mathbb{C}^n$ is surjective. ⌟

Proof: By Lefschetz principle(2.4.4.4), it suffices to show this for $(\mathbb{F}_p)^{alg}$ for p large. If this is not true, then choose the coefficients of the coordinate map of f, and the coordinates of an element that is not in the image, then the subfield k they generated is algebraic over $\mathbb{F}_p$, so it is finite, and clearly f is also surjective on k^n, contradiction. □

Cor. (2.4.4.6). Let $K \subset L$ be alg.closed fields, and V, W be varieties defined over K, and f is a polynomial isomorphism of V and W over L, then there is a polynomial isomorphism of V and W over K. ⌟

Proof: Let f have degree d. Then we can write a formula Ψ saying that there is an embedding of K into $\mathcal{M}$ and there is a polynomial bijection of V and W over $\mathcal{M}$, then $L \models \Psi$, and because ACF is complete(2.4.4.2), $K \models \Psi$, too. Thus there is also an isomorphism over K. □

Prop. (2.4.4.7). $ACF_\forall$ is the theory of integral domains. ⌟

Proof: Clearly a ring is a subring of an alg.closed field iff it is an integral domain, so the result follows from(2.4.2.38). □

Prop. (2.4.4.8). ACF has qualifier elimination. ⌟

Proof: Use(2.4.3.5), clearly it has algebraically prime models(2.4.4.7), and we need to check simply closedness.

For this, If $K \subset L$, notice that a quantifier-free formula φ is just a conjunction of some polynomial functions and negation of polynomial functions, with their coefficients in K. If there are some polynomial, then the solution b of φ in L is algebraic over K, thus in K because K is alg.closed. Now if it is just negations of polynomials, then clearly φ is true in K for some $c \in K$, because K is alg.closed thus infinite. □

Cor. (2.4.4.9). ACF is model-complete, by(2.4.3.9). ⌟

Lemma (2.4.4.10). Let K be a field, then the subsets of K^n defined by atomic formulas are exactly Zariski closed subsets. And a subset of K^n that is quantifier-definable iff it is a Boolean combination of Zariski closed subsets(constructible). (Clear). ⌟

Prop. (2.4.4.11). ACF is strongly minimal. ⌟

Proof: Because by quantifier elimination(2.4.4.8), every definable set is a finite Boolean combination of sets of the form $V(p) = 0$, where $p \in K[X]$, but $V(p)$ is either finite or all of K. □

Elimination of Imaginaries in Alg.Closed Fields

Def. (2.4.4.12) [Algebraicity]. Let $\mathcal{M}$ be an $\mathcal{L}$-structure and $A \subset M$, then for $b \in M$, $b \in acl(A)$ if there is a formula $\varphi(x, \overline{y})$ and $\overline{a} \in A$ that $\mathcal{M} \models \varphi(b, \overline{a})$, and $\{x \in M | \mathcal{M} \models \varphi(x, \overline{a})\}$ is finite. ⌟

Def. (2.4.4.13)[Algebraicity over Equivalence Class]. Let $\mathcal{M}$ be an $\mathcal{L}$-structure and E a definable equivalence relation on M^n, then we say a element $c \in M$ is algebraic over $\overline{a}/E, b_1, \ldots, b_m$ if there is a formula $\varphi(c, \overline{y}, \overline{z})$ that

- $\mathcal{M} \models \varphi(c, \overline{a}, \overline{b})$.
- If $\overline{a} E \overline{a}'$, then $\mathcal{M} \models \varphi(c, \overline{a}, \overline{b}) \leftrightarrow \varphi(c, \overline{a}', \overline{b})$.
- $\{x | \mathcal{M} \models \varphi(x, \overline{a}, \overline{b})\}$ is finite.

And a sequence $\overline{c}$ is called algebraic over $a/E, b_1, \ldots, b_m$ iff each coordinate is. ⌟

Lemma (2.4.4.14). Suppose $\overline{c}$ is algebraic over $\overline{a}/E, \overline{d}, \overline{b}$, and $\overline{b}$ is algebraic over $\overline{a}/E, \overline{d}$, then $\overline{c}$ is also algebraic over $\overline{a}/E, \overline{d}$. ⌟

Proof: Cf.[Marker, P92]. □

Lemma (2.4.4.15). Suppose K is an alg.closed field and E is a definable equivalence relation on K^n, and $\psi(\overline{x}, \overline{y}, \overline{d})$ defines E. If $\overline{a} \in K^n$, then there is a $\overline{c} \in K^n$ algebraic over $\overline{a}/E, \overline{d}$ s.t. $\overline{c} E \overline{a}$. ⌟

Proof: Cf.[Marker, P92].**?** □

Prop. (2.4.4.16) [Elimination of Imaginaries]. Let K be an alg.closed field, $A \subset K$, and E is an A-definable equivalence relation on K^n, then for some l there is an A-definable function $f : K^n \to K^l$ that $\overline{x} E \overline{y}$ iff $f(\overline{x}) = f(\overline{y})$. ⌟

Proof: Cf.[Marker, P92]. □

5 Real-Closed Fields

Prop. (2.4.5.1). The class of real-closed fields is an elementary class(2.4.1.4) of $\mathcal{L}_r$-structures. ⌟

Proof: The real-closed fields are axiomatized by:

- Axioms for fields.
- For each $n \geq 1$, the sentence $\forall x_1 \ldots \forall x_n(x_1^2 + \ldots + x_n^2 + 1 \neq 0)$.
- $\forall x \exists y(y^2 = x \vee y^2 + x = 0)$.
- For each $n \geq 0$, the sentence $\forall x_1 \ldots \forall x_n \exists y(y^{2n+1} + \sum_{i=0}^{2n} x_i y^i = 0)$.

These truly axiomatize real-closed fields, by(3.2.10.7). □

Prop. (2.4.5.2). Let F be a real-closed field, then the definable sets in F^n w.r.t the $\mathcal{L}_{or}$ is also definable w.r.t. $\mathcal{L}_r$. ⌟

Proof: Because we can replace all instances $t_i < t_j$ by $\exists v(v \neq 0 \wedge t_i + v^2 = t_j)$. □

Prop. (2.4.5.3). $RCF_\forall$ is the theory of ordered integral domains(easy). ⌟

Cor. (2.4.5.4). RCF has algebraically prime models. ⌟

Proof: Let D be an ordered domain, and let R be a real closure of the fraction field of D compatible with the ordering of D. Let F be another real-closed field extension of D, then let K be the algebraic closure of the fraction field of D in F, then K is a real-closed field by(3.2.10.7), then by(3.2.10.12) there is an isomorphism of $R \cong K$ extending $D \to K$, thus embeds R into F extending $D \to F$. □

Prop. (2.4.5.5). RCF has quantifier elimination (w.r.t. $\mathcal{L}_{or}$). ⌟

Proof: Use(2.4.3.5), it has algebraically prime models by(2.4.5.4), and we need to check simply closedness: Let $F \subset K$ be RCFs, $\varphi(v, \overline{w})$ be a quantifier-free formula and let $\overline{a} \in F, b \in K$ that $K \models \varphi(b, \overline{a})$. Then there are polynomials that

$$\varphi(v, \overline{a}) \leftrightarrow (\bigwedge p_i(v) = 0 \wedge \bigwedge q_i(v) > 0).$$

If any $p_i \neq 0$, then b is algebraic over F, but then $b \in F$ because F is real-closed. So we may assume $\varphi(v, \overline{a}) \leftrightarrow \wedge q_i(v) > 0$. Then because $q_i(b) > 0$ and q_i has f.m. zeros, by intermediate property(3.2.10.9), we can find a nbhd of b that is interval with endpoints in F that $q_i > 0$, and because F is dense(char0), there is an element b' that $F \models \varphi(b', \overline{a})$. □

Cor. (2.4.5.6). RCF is complete and decidable. Thus it is just the theory of $(\mathbb{R}, +, \cdot, <)$, and it is decidable. ⌟

Proof: It is model-complete by(2.4.3.9), and it has a minimal model that is the field $\mathbb{R}_{alg}$ of algebraic numbers in $\mathbb{R}$, then it is complete by(2.4.3.10). It is decidable by(2.4.2.29). □

Prop. (2.4.5.7) [RCF is o-Minimal]. The theory RCF(2.1.6.3) is o-minimal. ⌟

Proof: Because RCF has quantifier elimination, every definable set of a real-closed field R is semialgebraic, thus it is clearly a disjoint union of intervals and points. □

Semi-algebraic Sets

Def. (2.4.5.8) [Semi-algebraic Sets]. Let F be an ordered field, then $X \subset F^m$ is called **semi-algebraic** if there it is a Boolean combination of sets of the form $\{\underline{X} \in F^m | p(\underline{X}) > 0\}$, where $p(\underline{X}) \subset F[\underline{X}]$. ⌟

Thm. (2.4.5.9) [Tarski-Seidenberg]. If $F \in \texttt{Field}$ is real-closed, the semi-algebraic sets are closed under projection. ⌟

Proof: This is because quantifier elimination(2.4.5.5) implies semialgebraic sets are just definable sets, and the projection of a definable set is also definable. □

Cor. (2.4.5.10). The composite of two semialgebraic functions are semialgebraic. ⌟

Prop. (2.4.5.11) [Closure of Semialgerbaic Sets]. Let F be a real-closed field and $A \subset F^n$ be semialgebraic, then the closure of A in the Euclidean topology is also semialgebraic. ⌟

Proof: The closure of A is defined by

$$\{\overline{x} | \forall \varepsilon > 0, \exists \overline{y} \in A, d(\overline{x}, \overline{y}) < \varepsilon\}.$$

Thus it is definable, and thus semialgebraic by quantifier elimination(2.4.5.5). □

Prop. (2.4.5.12). Let F be a real-closed field and $X \subset F^n$ be closed and bounded, f be a continuous semialgebraic function, then $f(X)$ is closed and bounded. ⌟

Proof: If F is $\mathbb{R}$, then this follows from(4.4.5.2) that X is compact hence the image is also compact hence closed and bounded. As we can formulate a sentence asserting the conclusion. Thus the theorem follows as RCF is complete(2.4.5.6). □

Lemma (2.4.5.13). For R a real-closed field and $f : R \to R$ semialgebraic, then for any interval U there is an element x that f is continuous at x. ⌟

Proof: It suffices to prove for $R = \mathbb{R}$ by completeness of RCF. If there is an interval that f has finite range, then the inverse image of some point b is infinite, but also definable, so by o-minimality contains an interval that f is constant, hence continuous.

Otherwise, we inductively choose a chain of intervals: $V_0 = U$, and the image of V_n is definable thus contains an interval of length at most $1/n$, by o-minimality and our assumption. Now for the same reason the inverse image of this interval contains an interval, called V_{n+1}, s.t. $\overline{V_{n+1}} \subset V_n$, then $\cap V_n = \cap \overline{V}_n \neq \varphi$ because $\mathbb{R}$ is locally compact. For any $x \in V$, it is easy to see f is continuous at x. □

Prop. (2.4.5.14). For R a real-closed field and $f : R \to R$ semialgebraic, then f is discontinuous only at f.m. points. ⌟

Proof: The discontinuous points of f is definable by

$$D = \{x | F \models \exists \varepsilon > 0 \forall \delta > 0 \exists y |x - y| < \delta \wedge |f(x) - f(y)| > \varepsilon\},$$

thus it is a finite union of intervals and points, by o-minimality(2.4.5.7), but it must be f.m. points, by(2.4.5.13). □

Def. (2.4.5.15). We can naturally define the notion of **definably connected** and **definably arcwise connected** sets in R^n. ⌟

Def. (2.4.5.16) [Cells]. For an real-closed field F, we inductively define n-cells:

- $X \subset F^n$ is a 0-cell if it is a single point.
- If $X \subset F^m$ is an n-cell and $f : X \to F$ is a continuous definable function, then $Y = \{(\overline{x}, f(\overline{x}))|\overline{x} \in X\}$ is an n-cell.
- If $X \subset F^m$ is an n-cell and f, g are either continuous functions from X to F or constants $\pm\infty$, then $Y = \{(\overline{x}, y)|\overline{x} \in X \wedge f(\overline{x}) < y < g(\overline{x})\}$ is an $n+1$-cell.

⌟

Prop. (2.4.5.17) [Uniform Bounding]. Let $X \subset F^{m+1}$ be semialgebraic, then there is a natural number N that if $\overline{a} \in F^n$ and $X_{\overline{a}} = \{y|(\overline{a}, y) \in X\}$ is finite, then $|X_{\overline{a}}| < N$. ⌟

Proof: First notice $X_{\overline{a}}$ is definable, thus by o-minimality, $\{\overline{a}||X_{\overline{a}}| < \infty\}$ is definable, thus we may assume these are all of X.

Now let Γ be the theory

$$RCF + Diag(F) + \{\exists y_1, y_2, \ldots, y_m[\bigwedge_{i<j} y_i \neq y_j \wedge \bigwedge y_i \in X_{\overline{c}}]\}$$

where $m \in \mathbb{N}$, and $c_1, \ldots, c_n$ are new constants. (Notice $y_i \in X_{\overline{c}}$ is a sentence).

Then Γ is not satisfiable, because otherwise there is an embedding $F \subset K$, and by model completeness $F \prec K$, thus there is no $\overline{a}$ that $X_{\overline{a}}$ is infinite, because it is definable, contradiction.

Then by compactness theorem, there is some f.m. sentences of Γ that is unsatisfiable, thus the conclusion follows. □

Prop. (2.4.5.18) [Cell Decomposition]. Let F be a real-closed field, then any semialgebraic set $X \subset F^m$ is a finite disjoint union of cells. ⌟

Proof: Cf.[Marker, P103]. □

2.5 O-Minimal Structures

References are[O-Minimal Structures] and [Tame Topology and O-minimal Structures].

Notation (2.5.0.1).
- Use notations defined in Model Theory.

⌟

Def. (2.5.0.2) [O-Minimal Structure]. An ordered structure $\mathcal{M}$ is called ***o*-minimal** if any definable set is a finite union of intervals with endpoints in $M \cup \{\pm\infty\}$ and points, i.e. definable just by order relations. ⌟

Def. (2.5.0.3) [General O-Minimal Expansions]. A structure expanding the real-closed field R is a collection $\mathcal{S} = (\mathcal{S}^n)$, where $\mathcal{S}^n$ is a family of subsets of R^n, that
- Algebraic subsets are in $\mathcal{S}$.
- Each $\mathcal{S}^n$ is a Boolean subalgebra of the powerset of R^n.
- $\mathcal{S}$ is stable under Cartesian product and projection.

And $\mathcal{S}^n$ are called the **definable subsets** of R^n. And this structure is called ***o*-minimal** if moreover each subset in $\mathcal{S}^1$ is a finite unions of intervals and points. ⌟

1 Theory of Exponential Functions

References are [Zil05] and [Mar06].

Def. (2.5.1.1) [Exponential Maps]. For $R \in \mathcal{CR}\mathrm{ing}$, an **exponential map** on R is defined to be a non-trivial group homomorphism $\exp : R^+ \to R^\times$. A ring/field with an exponential map is called an **exponential ring/field**. ⌟

Prop. (2.5.1.2). An exponential field necessarily has characteristic 0. ⌟

Def. (2.5.1.3) [Exponential Polynomial Rings]. For any exponential ring $(A, \exp)$ and indeterminants $X_1, \ldots, X_n$, we can define the **exponential polynomial ring** $A[X_1, \ldots, X_n]_{\exp}$, and it satisfies an obvious universal property.**?** ⌟

Proof: □

Thm. (2.5.1.4) [van den Dries/Henson-Rubel]. The natural embedding $\mathbb{C}[X_1, \ldots, X_n]_{\exp} \to \mathcal{O}(\mathbb{C}^n)$ is injective. ⌟

Proof: Cf.[Exponential Rings, Exponential Polynomials and Exponential Functions]. □

Cor. (2.5.1.5). If $P \in \mathbb{C}[X, Y] \setminus (\mathbb{C}[X] \cup \mathbb{C}[Y])$ is irreducible, then $f(z) = P(z, e^z)$ has infinitely many zeros in $\mathbb{C}$. ⌟

Proof: If $f(z)$ has only f.m. zeros, then by Hadamard's factorization, $f(z) = e^{az}q(z)$ for some $q(X) \in \mathbb{C}[X]$. Then it follows from(2.5.1.4) that

$$P(z, e^z) = e^{az}q(z)$$

is a formal identity. Then $a \in \mathbb{N}$ and $P(X, Y) = Y^a q(X)$, which contradicts the hypothesis. □

Def. (2.5.1.6) [Exponential Algebraic Closures]. Let $(L, \exp)$ be an exponential field, and $A \subset L$. Suppose $K \subset L$ is the exponential subfield generated by A, then the **exponential algebraic closure** $\operatorname{expcl}(A)$ is defined to be the set of all $a \in L$ s.t. there exists $n \in \mathbb{Z}_+, f_1, \ldots, f_n \in K[X_1, \ldots, X_n]_{\exp}$, and $(b_1, \ldots, b_n) \in L^n$ s.t.

$$f_i(b_1, \ldots, b_n) = 0, \forall i, \quad \operatorname{Jac}(\frac{f_1, \ldots, f_n}{b_1, \ldots, b_n}) \neq 0, \quad b_1 = a.$$

⌟

Prop. (2.5.1.7). If $A \subset \mathbb{C}_{\exp}$ is a finite subset, then $\operatorname{expcl}(A)$ is countable. ⌟

Proof: □

Def. (2.5.1.8) [Ordered Exponential Fields]. Define $\mathbb{R}_{\exp} = (\mathbb{R}, +, \cdot, \exp, <, 0, 1)$, and $\mathbb{C}_{\exp} = (\mathbb{C}, +, \cdot, \exp, <, 0, 1)$ to be structures of ordered exponential fields. ⌟

Thm. (2.5.1.9) [Wilkie]. $\mathbb{R}_{\exp}$ is o-minimal. ⌟

Proof: ? □

Prop. (2.5.1.10). $\mathbb{Z}$ is definable in $\mathbb{C}_{\exp}$. ⌟

Proof: $\mathbb{Z} = \{x \in \mathbb{C} | \forall y(\exp(y) = 1 \to \exp(xy) = 1)\}$. □

Conj. (2.5.1.11). $\mathbb{C}_{\exp}$ is strongly quasi-minimal. ⌟

Proof: □

Conj.Cor. (2.5.1.12). $\mathbb{R}$ is not definable in $\mathbb{C}_{\exp}$. ⌟

Conj.Cor. (2.5.1.13). $\# \operatorname{Aut}(\mathbb{C}_{\exp}) = 2^{2^{\aleph_0}}$. ⌟

Proof: □

Conj. (2.5.1.14) [Schanuel's Conjecture over the Kernel]. Let $(K, \exp)$ be an exponential field, then the **Schanuel's conjecture over the kernel** says: For any $n \in \mathbb{Z}_+$ and $\alpha_1, \ldots, \alpha_n \in K$,

$$\operatorname{tr.deg}_{\mathbb{Q}(\ker \exp)} \mathbb{Q}(\alpha_1, \ldots, \alpha_n, \exp(\alpha_1), \ldots, \exp(\alpha_n), \ker \exp) \geq \dim_{\mathbb{Q}} \left((\ker \exp) \otimes \mathbb{Q} + \sum \mathbb{Q}\alpha_i\right) / (\ker \exp) \otimes \mathbb{Q}.$$

Notice the second term just equals $\operatorname{rank}(\exp(\alpha_1)^{\mathbb{Z}} \cdot \ldots \cdot \exp(\alpha_n)^{\mathbb{Z}})$. ⌟

Proof: □

Prop. (2.5.1.15). The Scaneul's conjecture is weak than the Schanuel's conjecture(14.7.1.2). But on $\mathbb{C}_{\exp}$, they are equivalent.? ⌟

Proof: □

Conj. (2.5.1.16) [Converse Schanuel's Conjecture]. Let $K \in \texttt{Field}$ is uncountable with an exponential function exp s.t. $\ker(\exp) \cong \mathbb{Z}$. Suppose that Schanuel's conjecture holds for K(14.7.1.2), then there exists an embedding $(K, +, \cdot, \exp, 0, 1) \hookrightarrow \mathbb{C}_{\exp}$. ⌟

Def. (2.5.1.17) [Strongly Exponentially-Closed Fields with Exponentials, Zilber]. Zilber showed that there is an $\mathcal{L}_{\omega_1,\omega}(Q)$-theory $C_{\exp}$ of **strongly exponentially-closed fields with exponentials**. ⌟

Proof: Cf.[Zil05]. □

Thm. (2.5.1.18) [Zilber]. $C_{\exp}$ is strongly quasi-minimal(2.4.3.20).

For any uncountable cardinal κ, there exists a unique model for $C_{\exp}$ of cardinality κ.

If $\mathcal{M} \models C_{\exp}$ and $A \subset \mathcal{M}$ is finite, then for any $a, b \in \mathrm{cl}(A)$, there exists an automorphism of $\mathcal{M}$ taking a to b. ⌟

Proof:

□

Conj. (2.5.1.19) [Zilber]. $\mathbb{C}_{\exp}$ is strongly exponentially-closed. ⌟

Proof: □

Prop. (2.5.1.20). Suppose Schanuel's conjecture is true(14.7.1.2), then for $P \in \mathbb{C}[X, Y] \setminus (\mathbb{C}[X] \cup \mathbb{C}[Y])$ is irreducible, $f(z) = P(z, e^z)$ has infinitely many alg.independent zeros in $\mathbb{C}$. ⌟

Proof: Cf.[Mar06]. □

2.6 Elementary Mathematics

1 Algebra

Prop. (2.6.1.1). If $(a_n)_{n\geq n_0, n\in\mathbb{N}}$ is a series of real numbers and $C\in\mathbb{R}$ s.t. $a_{m+n}\geq a_m+a_n+C$ for any $m,n\geq n_0\in\mathbb{N}$, then a_m/m converges to $\overline{\lim}\, a_n/n\in(-\infty,\infty]$.

Notice by taking $b_n=-a_n$, the $\leq$ case is also true. In particular, if $|a_{m+n}-a_m-a_n|\leq C$ for any $m,n\geq n_0\in\mathbb{N}$, then a_m/m converges in $\mathbb{R}$. ⌟

Proof: Let $\lambda=\overline{\lim}\, a_n/n$. By induction, for any $N\geq n_0\in\mathbb{N}$, $a_{2^kN}\geq 2^k a_N+(2^k-1)C$ for any $k\in\mathbb{N}$, so $a_{2^kN}/2^kN\geq a_N/N+\min\{C,0\}$, so $\lambda>-\infty$.

If $\lambda=+\infty$, then for any $M\in\mathbb{R}$, there exists $n>|C|/\varepsilon$ s.t. $a_n/n\geq M$. For any N large, $N=kn+m$ for some k,m and $n_0\leq m<n_0+n$, so $a_N\geq ka_n+a_m+(k+1)C$, so $\underline{\lim}\, a_N/N\geq a_n/n-\varepsilon\geq M-\varepsilon$ for N large, so $\underline{\lim}\, a_n/n=\overline{\lim}\, a_n/n$.

If $\lambda<\infty$, for any $\varepsilon>0$, there exists $n>|C|/\varepsilon$ s.t. $\lambda-a_n/n<\varepsilon$. For any N large, $N=kn+m$ for some k,m and $n_0\leq m<n_0+n$, so $a_N\geq ka_n+a_m+(k+1)C$, so $\underline{\lim}\, a_N/N\geq a_n/n\geq\lambda-2\varepsilon$ for N large, so $\underline{\lim}\, a_n/n=\overline{\lim}\, a_n/n$. □

2 Analysis

Lemma (2.6.2.1). If $P(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_0$ satisfies $a_n\geq 1, a_{n-1}\geq 0$, and $|a_i|\leq H$ for $i\leq n-2$, then for any root α of P, either $\mathrm{Re}\,\alpha\leq 0$, or $|\alpha|<\frac{1+\sqrt{1+4H}}{2}$. ⌟

Proof: □

3 Number Theory

Primes

Def. (2.6.3.1) [Prime Numbers]. $p\in\mathbb{Z}_+$ is called a (rational)**prime number** if for any $d\in\mathbb{Z}_+$, $d|p$ implies $d=1$ or $d=p$. The set of prime numbers is denoted by $\mathbf{P}$. ⌟

Lemma (2.6.3.2) [Infinitely Many Primes]. $\#\,\mathtt{Prime}=\infty$. ⌟

Proof: Suppose $\#\,\mathtt{Prime}<\infty$, let $N=\prod_{p\in\mathtt{Prime}}p$. Then $N+1$ has no prime factors, contradiction. □

Def. (2.6.3.3) [Mersenne Primes]. If $p\in\mathbf{P}$ and $M_p=2^p-1$ is also a prime, then M_p is called a **Mersenne prime**. ⌟

Def. (2.6.3.4) [Perfect Numbers]. A **perfect number** is a number $n\in\mathbb{Z}_+$ s.t.

$$\sigma(n)=2n(2.6.3.19).$$

Moreover, an **abundant number** is a number $n\in\mathbb{Z}_+$ s.t. $\sigma(n)>2n$, and a **deficient number** is a number $n\in\mathbb{Z}_+$ s.t. $\sigma(n)<2n$. ⌟

Thm. (2.6.3.5) [Even Perfect Numbers, Euclid-Euler]. $n\in\mathbb{Z}_+$ is an even perfect number iff there exists $p\in\mathbf{P}$ s.t. $n=2^{p-1}(2^p-1)$ and $2^p-1\in\mathbf{P}$. ⌟

Proof: If $p \in \mathbf{P}$ s.t. $n = 2^{p-1}(2^p - 1)$ and $2^p - 1 \in \mathbf{P}$, then it is clear that $n = 2^{p-1}(2^p - 1)$ is a perfect number. Conversely, suppose $n = 2^k x$ is even and perfect, where $2 \nmid x$. Then

$$2^{k+1}x = \sigma(2^k x) = (2^{k+1} - 1)\sigma(x).$$

Denote $y = x/(2^{k+1} - 1) \in \mathbb{Z}_+$, then

$$2^{k+1}y = \sigma(x) \geq x + y = 2^{k+1}y.$$

Thus x has only two divisors: x and y. So $y = 1$, and $x = 2^{k+1} - 1$ is a prime. This forces $k+1$ to be a prime, and x being a Mersenne prime. □

Conj. (2.6.3.6). There are no odd perfect numbers. ⌟

Proof: □

Thm& Conj.Cor. (2.6.3.7) [Dickson-Nielsen-Pollack]. For any $k \in \mathbb{Z}_+$,

1. If n is an odd perfect number, then $\nu(n) \geq 9$.
2. If n is an odd perfect number with $\nu(n) \leq k$, then $n < 2^{4^k}$.
3. For $X \in \mathbb{Z}_+$, the number of odd perfect numbers $n \leq X$ with $\nu(n) \leq k$ is bounded by $(\log x)^k$.
4. The number of odd perfect numbers N with $\nu(n) \leq k$ is bounded by 4^{k^2}.

⌟

Proof: 1: Cf.[Nielsen, Odd perfect numbers have at least nine distinct prime factors].

2: Cf.[Nielsen, An upper bound for odd perfect numbers].

3: Let N be an odd perfect number with $9 \leq \nu(N) \leq k$, let p_0 be the minimal prime divisor of N, and $p_0^{e_0}||N$. Denote $B = p_0^{e_0}$ and $N = BA$. Then

$$B < \sigma(B) = \frac{2A}{\sigma A}B \leq 2B,$$

with equality on the right iff $A = 1$. Suppose $A \neq 1$, then $\sigma(B) \nmid 2B$. So there is a least $p_1 \in \mathbf{P}$ s.t. $p_1|\sigma(B), p_1 \nmid 2B$. So $p_1|A$. Suppose $p_1^{e_1}||A$, and let $A' = A/p_1^{e_1}, B' = Bp_1^{e_1}$, then the same reasoning can apply to A' and B'. Finally, we get

$$A = p_1^{e_1}p_2^{e_2}\ldots p_l^{e_l},$$

and $8 \leq l = \nu(N) - 1 \leq k - 1$. Notice

$$\frac{1}{2} = \frac{N}{\sigma(N)} \geq \prod_{p|N}(1 - \frac{1}{p}) \geq 1 - \sum_{p|N}\frac{1}{p} \geq 1 - \frac{k}{p_0},$$

so $p_0 \leq 2k$. Thus there are$\leq k - 1$ possibilities of p_0. And there are$\leq \log x/\log 3$ possibilities of e_0. Notice that if B is given, then A is totally determined by the sequence $e_1, \ldots, e_n$. Thus there are at most

$$\frac{(k-1)(k-4)}{(\log 3)(\log 5)^{k-1}}(\log x)^k$$

possibilities of $N = AB$. This coefficient is deceasing for $k \geq 9$, and it is smaller than 1.

4 follows from item2 and item3. □

Thm& Conj.Cor. (2.6.3.8) [Euler]. If N is an odd perfect prime, then there exists $p \in \mathbf{P}$ s.t. $N = p^\gamma m^2$, where $p \equiv \gamma \equiv 1 \pmod 4$. ⌟

Proof: □

Thm. (2.6.3.9)[Power Lifting]. If $p \in \mathbf{P}, a, b \in \mathbb{Z}\backslash(p)$, and $v_p(a-b) = k \geq 1$, then $v_p(a^{p^n} - b^{p^n}) = k+n$ for $n \in \mathbb{Z}_+$, except for $p = 2$ and $k = 1$, in which case $v_p(a^{p^n} - b^{p^n}) = k+n+1$ for $n \in \mathbb{Z}_+$. ⌟

Proof: Use induction on n: If $a^{p^n} = b^{p^n} + p^{n+k}c$ for some c s.t. $p \nmid c$, then

$$a^{p^{n+1}} = b^{p^{n+1}} + p^{n+k+1} b^{p^n(p-1)} c \ldots + p^{(n+k)p} c^p,$$

and the assertion follows. □

Prop. (2.6.3.10). For $n \geq 2$, the multiplicative group of $(\mathbb{Z}/(2^n))^* \cong \mathbb{Z}/(2) \times Z/(2^{n-2})$. ⌟

Proof: it suffices to show $3^{2^{n-3}} \neq \pm 1 \mod 2^n$, and $3^{2^{n-2}} \equiv 1 \mod 2^n$. □

Prop. (2.6.3.11) [*b*-adic Decompositions and Irreducibility]. If $b > 2$ and p is a prime, consider the b-adic expansion $p = \sum a_n b^n$, then the polynomial

$$\sum a_n X^n$$

is irreducible over $\mathbb{Z}$. ⌟

Proof: If $p(x) = h(x)r(x)$, use the lemma(2.6.2.1) to show that $r(b)$ and $h(b)$ cannot be 1, thus $h(b)r(b) = p$ cannot happen. □

Thm. (2.6.3.12) [Zsigmondy]. If $a, n \in \mathbb{Z}_{>1}$, then there exists a prime divisor of $a^n - 1$ not dividing $a^j - 1$ for any $0 < j < n$, except in the following cases:

- $n = 2, a = 2^s - 1, s \geq 2$.
- $n = 6, a = 2$.

⌟

Proof: By(3.3.2.8), it suffices to find a prime ideal of $\Psi_n(a)$ not dividing n. If $n = 2$, then any prime divisor of $a+1$ not dividing $a-1$ suffices, as long as a is not of the form $2^s - 1$.

For $n \geq 3$, if all prime divisors of $\Psi_n(a)$ divides n, we prove that $\Psi_n(a) \in \mathbf{P}$: Take $p|\Psi_n(a)$, and let $k = \mathrm{ord}(a, \mathbb{F}_p^\times)|(p-1) < n$, then $p|\Psi_k(a)$, and $n/k = p^t$ for some $t \in \mathbb{Z}_+$. Then if $p \neq 2$, by power-lifting(2.6.3.9),

$$v_p(a^n - 1) = v_p(a^{n/p} - 1) + 1,$$

so $v_p(\Psi_n(a)) = 1$. And if $p = 2$, then clearly $k = 1$, and $n \in 2^{\mathbb{Z}_+}$, and $\Psi_n(a) = a^{n/2} + 1 \equiv 2 \pmod 4$ as $n \neq 2$, so it is still true that $v_2(\Psi_n(a)) = 1$.

And if $\ell \in \mathbf{P} \setminus \{p\}$ is another prime dividing $\Psi_n(a)$, then $n/p^t = k|(p-1), n/\ell^{t'} = k'|\ell - 1$, so $p \leq \ell - 1 < \ell \leq p - 1$, contradiction. So $\Psi_n(a) = p$ is a prime.

Then suppose $n = p^k r$ where $(r, p) = 1$, we prove that $p > (b^{p-2}(b-1))^{\varphi(r)}$ where $b = a^{q^{k-1}}$: By(3.3.2.5),

$$\Psi_n(a) = \Psi_r(b^p)/\Psi_r(b) \geq \Big(\frac{b^p - 1}{b+1}\Big)^{\varphi(r)} \geq \Big(\frac{b^{p-2}(b^2-1)}{b+1}\Big)^{\varphi(r)} = (b^{p-2}(b-1))^{\varphi(r)}.$$

If $p \geq 5$, then we have $b^{p-2} > p$, so only possible cases are $p = 2$ or 3. The case $p = 2$ is not possible, because then $a = 2$, and $2 = \Psi_n(2) \equiv 1 \pmod 2$. So $p = 3, a = 2, k = 1$ and $r = 1$ or 2. But $\Psi_n(2) \neq 3$, contradiction. □

Def. (2.6.3.13)[Numerical Polynomials]. A function $f:\mathbb{Z}\to\mathbb{Z}$ is called a **numerical polynomial** if it there exists $a_1,\ldots,a_r\in\mathbb{Z}$ that

$$f(n)=\sum_{i=0}^{r}a_i\binom{n}{i}.$$

for n sufficiently large. ⌟

Prop. (2.6.3.14). Suppose that $f:\mathbb{Z}\to\mathbb{Z}$ is defined for n sufficiently large and $g(n)=f(n)-f(n-1)$ is a numerical polynomial, then f is a numerical polynomial. ⌟

Proof: Suppose $f(n)-f(n-1)=\sum_{i=0}^{r}a_i\binom{n}{i}$ for all $n>0$. If we set $g(n)=f(n)-\sum_{i=0}^{r}a_i\binom{n+1}{i+1}$, then $g(n)-g(n-1)=0$ for n sufficiently large, so it is eventually constant, which is equal to a_{-1}. Then $f(n)=\sum_{i=0}^{r}a_i\binom{n+1}{i+1}+a_{-1}$ is a numerical polynomial. □

Cor. (2.6.3.15). Any polynomial function with coefficients in $\mathbb{Q}$ maps any integer sufficiently large into $\mathbb{Z}$ iff it is a numerical function. ⌟

Useful Functions

Def. (2.6.3.16)[Greatest Common Divisors]. For $S\subset\mathbb{Z}$, the **greatest common divisor** $\gcd(S)\in\mathbb{Z}_+\cup\{\infty\}$ denote the supremum of integers $m\in\mathbb{Z}+$ s.t. $m|s$ for each $s\in S$.

For $S\subset\mathbb{Z}^\times$, the **least common multiple** $\mathrm{lcm}(S)\in\mathbb{Z}_+\cup\{\infty\}$ denote the supremum of integers $m\in\mathbb{Z}+$ s.t. $s|m$ for each $s\in S$. ⌟

Prop. (2.6.3.17). For $n\in\mathbb{Z}_{\geq 7}$,

- For any $1\leq m\leq n$, $m\binom{n}{m}\Big|\,\mathrm{lcm}(\{1,2,\ldots,n\})$.
- $\mathrm{lcm}(\{1,2,\ldots,n\})\geq 2^n$.

⌟

Proof: 1: By**??** for any $p\in\mathbf{P}$, let $v_p(m)=k$, then $k+v_p(\binom{n}{m})\leq v_p(\mathrm{lcm}(\{1,2,\ldots,n\}))$. Thus the assertion follows.

2: By item1, $n\binom{2n}{n}|\,\mathrm{lcm}(\{1,2,\ldots,2n\})$, and $(2n+1)\binom{2n}{n}=(n+1)\binom{2n+1}{n+1}|\,\mathrm{lcm}(\{1,2,\ldots,2n+1\})$. So

$$n(2n+1)\binom{2n}{n}\Big|\,\mathrm{lcm}(\{1,2,\ldots,2n+1\}),$$

and $\mathrm{lcm}(\{1,2,\ldots,2n+1\})\geq n4^n$. So for $n\geq 2$, $\mathrm{lcm}(\{1,2,\ldots,2n+1\})$, and for $n\geq 4$, $\mathrm{lcm}(\{1,2,\ldots,2n+2\})\geq\mathrm{lcm}(\{1,2,\ldots,2n+1\})\geq 2^{2n+2}$. The case $n\in\{7,8\}$ can be verified directly. □

Def. (2.6.3.18)[ν-Function]. The **ν-function** is defined to be

$$\tau:\mathbb{Z}_+\to\mathbb{Z}_+:n\mapsto\#\{p\in\mathbf{P}:p|n\}.$$

⌟

Def. (2.6.3.19)[σ_s-Function]. For $s\in\mathbb{R}$, the function σ_s is defined to be

$$\sigma_s:\mathbb{Z}_+\to\mathbb{R}_+:n\mapsto\sum_{d\in\mathbb{Z}_+,d|n}d^s.$$

And also denote $\sigma(n)=\sigma_1(n)$.

And for $s=1$, denote $\tau(n)=\sigma_0(n)$, called the **ν-function**. ⌟

Def. (2.6.3.20) [Euler's φ-Function]. The **Euler's φ-function** is defined to be

$$\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+ : n \mapsto \#(\mathbb{Z}/(n))^*.$$

⌟

Def. (2.6.3.21) [Möbius Function]. The **Möbius function** is defined to be the multiplicative function

$$\mu : \mathbb{Z}_+ \to \{0, 1, -1\} : n \mapsto \begin{cases} (-1)^k & n = \prod_{i=1}^k p_i, p_i \neq p_j \in \mathbf{P} \\ 0 & \text{otherwise} \end{cases}.$$

⌟

Prop. (2.6.3.22) [Möbius Identities]. For $n \in \mathbb{Z}_+$,

- If $m \in \mathbb{Z}_+$ is prime to n, then $\mu(mn) = \mu(m)\mu(n)$.
- $$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}.$$
- If $p \in \mathbf{P}$,
$$\sum_{d|n, p\nmid d} \mu(d) = \begin{cases} 1 & n \in p^{\mathbb{Z}_+} \\ 0 & \text{otherwise} \end{cases}.$$

⌟

Proof: 1: This is clear.
2: By item1, it suffices to prove for $d = p^k$ for some $p \in \mathbf{P}$, then this is clear.
3: By item1, it suffices to prove for $d = p^k$ for some $p \in \mathbf{P}$, then this is clear. □

Cor. (2.6.3.23) [Möbius Inversion]. ⌟

Proof: □

Prop. (2.6.3.24) [Kronecker Symbol]. Define the **Kronecker symbol** as a function

$$\mathbb{Z} \times \mathbb{Z} \to \{0, -1, 1\} : (a, m) \to \left(\frac{a}{m}\right)$$

satisfying the following:

- $\left(\frac{a}{m}\right)$ is multiplicative in a and in m.
- $\left(\frac{a}{0}\right) = \begin{cases} 1 & a = \pm 1 \\ 0 & \text{otherwise} \end{cases}.$
- $\left(\frac{a}{-1}\right) = \begin{cases} -1 & a < 0 \\ 1 & a \geq 0 \end{cases}.$
- $\left(\frac{a}{2}\right) = \begin{cases} 0 & a \in 2\mathbb{Z} \\ (-1)^{\frac{a^2-1}{8}} & a \notin 2\mathbb{Z} \end{cases}.$
- For $p \in \mathbf{P}_{\geq 3}$, $\left(\frac{a}{p}\right) = \begin{cases} 0 & a \in p\mathbb{Z} \\ (-1)^{\frac{p-1}{2}} & a \notin p\mathbb{Z} \end{cases}.$

⌟

Lemma (2.6.3.25). $\sum_{x=0}^{p-1} x^k \equiv -1 \mod p$ iff $(p-1)|k$, and $\equiv 0 \mod p$ otherwise. ⌟

Proof: Choose a a that $a^k - 1$ is not divisible by p, this is doable iff k is not divisible by $p-1$, then it is clear. □

Prop. (2.6.3.26) [Quadratic Legendre Symbol Sum]. For add prime p,

$$\sum \left(\frac{x^2+1}{p}\right) = -1.$$

⌟

Proof: The sum is equivalent modulo p to $\sum_{x=0}^{p-1}(x^2+ax+b)^{\frac{p-1}{2}}$, which by the lemma(2.6.3.25) above equivalent to -1 modulo p. Now it can not be $p-1$, because otherwise there is a solution for $p|x^2+1$, and then it can be calculated directly. □

Def. (2.6.3.27) [Integral Part]. For any number $\alpha \in \mathbb{R}$, let $[\alpha]$ be the maximal integer n that $n \leq \alpha$, called the **integral part of** α and $\{\alpha\} = \alpha - [\alpha]$, called the **fractional part of** α. ⌟

Congruences of Binomial Coefficients

References are http://www.cecm.sfu.ca/organics/papers/granville/paper/binomial/html/binomial.html.

Prop. (2.6.3.28) [p-Power in Product]. $v_p(n!) = \frac{n-c(n)}{p-1}$, where $c(n)$ is the sum of the presentation of n in the p-adic base. ⌟

Cor. (2.6.3.29) [Kummer]. $v_p(\binom{a+b}{a})$ equals the number of carries when adding a and b in base p. ⌟

Prop. (2.6.3.30) [Wilson]. For $p \in \texttt{Prime}$, $(p-1)! \equiv -1 (\mod p)$. ⌟

Proof: Consider the two polynomials

$$g(X) = \prod_{k=1}^{p-1}(X-k), \quad h(X) = X^{p-1} - 1,$$

then

$$f(X) = g(X) - h(X)$$

are identically zero on $\mathbb{F}_q$ but has degree$\leq p-2$, so it must be identically 0. Thus the assertion follows. □

Cor. (2.6.3.31). For any $n \in \mathbb{Z}$,

$$\binom{np-1}{p-1} \equiv 1 (\mod p).$$

And

$$\binom{2p-1}{p-1} \equiv 1 (\mod p^r)$$

where $r = \min(3, p-1)$. ⌟

Proof: □

Prop. (2.6.3.32) [Lucas]. For $m, r \in \mathbb{Z}_+, n = m + r$, let n_i, m_i, r_i be their i-th term in base-p, then if $k = v_p(\binom{n}{m})$, then

$$\frac{(-1)^k}{p^k}\binom{n}{m} \equiv \prod_k \frac{n_k!}{m_k! r_k!} (\text{mod } p).$$

⌟

Proof: Denote $(n!)_p = \prod_{1\leq m\leq n, p\nmid m} m$, then by some argument, it suffices to prove that

$$(-1)^{\lfloor n/p \rfloor}(n!)_p \equiv n_0!(\text{mod } p).$$

And this follows easily from Wilson's theorem(2.6.3.30). □

Prop. (2.6.3.33) [Glaisher]. If $p \in \mathbf{P}, 1 \leq j, k \leq p-1$ and $n \in \mathbb{Z}$ s.t. $n \equiv k(\text{mod } p-1)$, then

$$\sum_{1\leq m\leq n, m\equiv j(\text{mod } p-1)} \binom{n}{m} \equiv \binom{k}{j} (\text{mod } p).$$

⌟

Proof: Notice if the i-th term of n, m in the base p are n_i, m_i, then $p \nmid \binom{n}{m}$ iff $m_i < n_i$ for each i. And then

$$\sum_{1\leq m\leq n-1, m\equiv j(\text{mod } p-1)} \binom{n}{m} = \sum_{(m_0,\ldots,m_d)} \binom{n_0}{m_0} \cdots \binom{n_d}{m_d}.$$

But the RHS equals the sum of coefficients of $X^j, X^{j+(p-1)}, X^{j+2(p-1)}, \ldots$ in $(X+1)^{n_0}(X+1)^{n_1} \cdot (X+1)^{n_d} = (X+1)^{\sum n_i}$, which is also equal to

$$\sum_{1\leq m\leq \sum n_i, m\equiv j(\text{mod } p-1)} \binom{\sum n_i}{m}$$

And also $n \equiv \sum n_i(\text{mod } p-1)$, so we can use induction on n, and notice that the assertion is trivial for $n \leq p-1$. □

Cor. (2.6.3.34) [Hermite]. If $n \in \mathbb{Z}_+, p \in \mathbf{P}$, then

$$\sum_{1\leq m\leq n-1, (p-1)|m} \binom{n}{m} \equiv 0(\text{mod } p)$$

⌟

Prop. (2.6.3.35) [Carlitz]. If $n \in \mathbb{Z}_+, p \in \mathbf{P}, r \in \mathbb{Z}_+$ and $p^{r-1}|n$, then

$$p + (p-1)\sum_{1\leq m\leq n-1, (p-1)|m} \binom{n}{m} \equiv 0(\text{mod } p^r).$$

⌟

Proof: □

Prop. (2.6.3.36) [Morley]. For $p \in \mathbf{P}$ and $p \geq 5$,

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{(p-1)/2} \equiv 4^{p-1}(\text{mod } p)^3.$$

⌟

Proof: □

Continued Fractions

Def. (2.6.3.37) [Continued Fractions]. A **finite continued fraction** $[a_1, \ldots, a_n]$ is an abbreviation of

$$\frac{1}{a_1 + \frac{1}{a_2 + \ldots \frac{1}{a_n}}}, \quad a_i \in \mathbb{Z}_+.$$

A **continued fraction** $[a_1, a_2, \ldots]$ is an abbreviation of

$$\frac{1}{a_1 + \frac{1}{a_2 + \ldots}}, \quad a_i \in \mathbb{Z}_+.$$

⌟

Def. (2.6.3.38) [Gauss Transformation]. The **Gauss transformation** is the function $\varphi : \mathbb{R} \to [0, 1]$:

$$\varphi(x) = \begin{cases} 1/x - [1/x] & x \neq 0 \\ 0 & x = 0 \end{cases}.$$

⌟

Prop. (2.6.3.39). For any sequence of positive numbers $\{a_1, \ldots, a_n, \ldots\}$, $[a_1, \ldots, a_n]$ converges. In particular, $\lim_{n\to\infty}[\varphi(x), \varphi^2(x), \ldots, \varphi^n(x)] = \{x\}$ for $x \in \mathbb{R}$. ⌟

Proof: We may assume the sequence is infinite. Then we notice for any $a \in \mathbb{Z}_+$ and t varying in an interval in $(0, 1]$ of length l, the value of $\frac{1}{a+t}$ is in an interval of length$l/a(a + l) \leq l/(l + 1)$. So clearly the length of possible values of $[a_1, \ldots, a_n, t]$ for t in an interval of length l is in an interval of length l_n that $\lim_{n\to\infty} l_n = 0$.

Then we conclude $[a_1, \ldots, a_n]$ is a Cauchy sequence for n, thus it converges. □

Prop. (2.6.3.40). $x \in \mathbb{R}$ is a rational number iff $\varphi^m(x) = 0$ for some $m > 0$. ⌟

Proof: If x is rational then this is Euclid division. If $\varphi^m(x) = 0$, then notice $x = [x] + [\varphi(x), \varphi^2(x), \ldots, \varphi^{m-1}(x)]$ is rational. □

Prop. (2.6.3.41). $x \in \mathbb{R}$ has eventually periodic continued fractions $[\varphi(x), \varphi^2(x), \ldots, \varphi^n(x), \ldots]$ iff $[\mathbb{Q}(x) : \mathbb{Q}] \leq 2$. ⌟

Proof: If the fraction is finite, then $\mathbb{Q}(x) = \mathbb{Q}$, by(2.6.3.40). If the fraction has periodic part $[a_1, \ldots, a_n]$, let $t = [a_1, \ldots, a_n, a_1, \ldots, a_n, \ldots, \ldots]$, then

$$\frac{at + b}{ct + d} = t$$

for some $a, b, c, d \in \mathbb{Z}$, so $[\mathbb{Q}[t] : \mathbb{Q}] = 2$, and hence $[\mathbb{Q}(x) : \mathbb{Q}] = 2$.

For the converse, **?**. □

4 Euclidean Geometry

Thm. (2.6.4.1) [Ptolemy]. Let A, B, C, D be points in $\mathbb{R}^2$, then

$$d(A,C) \cdot d(B,D) \le d(A,B) \cdot d(C,D) + d(A,D) \cdot d(B,C).$$

And the equality holds if A, B, C, D are consequence points on a circle. ⌟

Proof: Use complex numbers. there is an identity

$$(A-B)(C-D) + (A-D)(B-C) = (A-C)(B-D),$$

thus by triangle inequality,

$$||(A-C)(B-D)|| \le ||(A-B)(C-D)|| + ||(A-D)(B-C)||,$$

where the equality holds if A, B, C, D are consequence points on a circle. □

Thm. (2.6.4.2) [Euclid]. There are only five Platonic solids: tetrahedron, hexahedron, octahedron, dodecahedron and the icosahedron. ⌟

Proof: □

Higher Dimensions

Remark (2.6.4.3). Instead of using time to visualize higher dimensions, we can also use color to visualize higher dimensions. In fact, human eyes are even 3-color based, which means theoretically we can visualize $\mathbb{R}^3$ simply using colors. ⌟

2.7 Complexity Theory

References are [Computational Complexity, Padadimitriou], and [Logics for Mathematitians, Hamilton].

1 Problems and Algorithms

Def. (2.7.1.1) [Decision Problems]. For $I \in \mathcal{S}\mathrm{et}$, a **decision problem** on I is a subset $X \subset I$. The elements of X are called its **instances**. The goal is to determine the set X. ⌟

Def. (2.7.1.2) [Optimization Problems]. For $I \in \mathcal{S}\mathrm{et}$, a **optimization problem** is a subset $X \subset I$ and a cost function $f : I \to \mathbb{R}$. The goal is to seek the maximum of f on X. ⌟

Remark (2.7.1.3) [Cobham-Edmonds Thesis]. computational problems can be feasibly computed on some computational device only if they can be computed in polynomial time. ⌟

Examples of Problems

Example (2.7.1.4) [Graph Reachability]. The input is a directed graph $G = (V, E)$ and two nodes $s, t \in V$. The problem is to find if s is connected to t, and also find the shortest path from s to t.

This problem can be solved by maintaining a set $S \subset V$, where $S = \{s\}$ at first, and at each step, choose a vertex i in S that stayed the longest time, delete it, and add all vertices j s.t. $(i, j) \in E$. Proceed until $t \in S$, or S becomes empty. In the first case, s is connected to t, and we find a shortest path to t. While in the second case, s is disconnected to t.

Then this problem is in TIME($O(n^2)$). ⌟

Example (2.7.1.5) [Maximum Flow Problems]. The input is a directed graph $G = (V, E)$ with a source $s \in V$ with no incoming edges and a sink $t \in V$ with no out-coming edges, and each edge is labeled with a positive integer.

A **flow** in G from s to t, which means an assignment of non-negative integers $f(e)$ to each edge e s.t. for each vertex v except s and t, the sum of values of edges with source v equals the sum of values of edges with target v.

Then the problem is to find a flow with maximum sum of values at s.

This problem can be solved by at first finding a flow by finding the shortest path from s to t, then at each step, we draw the difference graph, and try to find a shortest path from s to t. This is called a augmentation flow.

If the edge on a path with the lest capacity is called a **bottleneck**, then it can be proved that there are at most $\#V^2$ iterations:

Lemma (2.7.1.6).

- The distance from s to any vertex doesn't decrease from one augmentation graph to the next graph.
- If an edge $e = (i, j)$ is a bottleneck in one augmentation, then the distance of i from s must increase by at least 2 before $-e$ becomes a bottleneck again.

⌟

Proof: 1: If the distance from s to some vertex decreases. Let v be a vertex s.t. the distance after augmentation is the shortest from s. Let $s - - > i - > v$ be a shortest path, then (v, i) must be in the shortest flow. Then the distance from s to i must also decreased, and that distance is smaller that the distance to v, contradiction.

2: This follows from 1, because the shortest path from s to j cannot decrease, the new path includes $-e = (j, i)$ instead of going to i directly, means that the distance from s to i must increased by at least 2. □

Then by(2.7.1.4), the problem is in TIME($O(n^4)$). ⌟

Example (2.7.1.7) [Bipartite Matching]. The input is a bipartite graph $G = (U, V, E)$ where $\#U = \#V = n$ and $E \subset U \times V$, the problem is to determine whether there is a matching between U and V via E.

By adding two points s, t with s pointing to each vertex in U and each vertex in V pointing to t, we can reduce the problem to finding a flow from s to t of capacity n. Thus this decision problem is in TIME($O(n^4)$), by(2.7.1.5). ⌟

Example (2.7.1.8) [Salesman Problem]. The salesman problem is clearly in $\mathtt{NP}$. ⌟

2 Turing Machines

Def. (2.7.2.1) [Turing Machines]. A **Turing machine** is a tuple

$$M = (K, \Sigma, \Delta, s, \amalg, \triangleright, h, y, n, \leftarrow, \rightarrow, -),$$

where

- $h, y, n, \leftarrow, \rightarrow, -$ are disjoint singletons, called the **halting state, accepting state, rejecting state, left curser, right curser, stay curser** resp.
- K is a finite set disjoint from $\{h, y, n, \leftarrow, \rightarrow, -\}$. elements of $K \cup \{h, y, n\}$ are called **states**.
- $s \in K$ is a state, called the **initial state**.
- Σ is a finite set disjoint from $K \cup \{h, y, n, \leftarrow, \rightarrow, -\}$, called the **alphabet of** M, and elements of Σ are called **symbols**.
- $\amalg, \triangleright \in \Sigma$ are two symbols, called the **blank symbol** and **first symbol** resp..
- $\Delta \subset K \times \Sigma \times (K \cup \{h, y, n\}) \times \Sigma \times \{\leftarrow, \rightarrow, -\}$, called the **transition relation of** M. δ must satisfy: for any states p, q, symbol σ and $m \in \{\leftarrow, \rightarrow, -\}$ s.t. $(p, \triangleright, q, \sigma, m) \in \Delta$, we have $\sigma = \triangleright$ and $m = \rightarrow$.

For normalization, we may assume that

$$\Sigma = \{1, 2, \ldots, \#\Sigma\}, \quad K = \{\#\Sigma + 1, \ldots, \#\Sigma + \#K\},$$

$$s = \#\Sigma + 1, \quad (h, y, n, \leftarrow, \rightarrow, -) = (\#\Sigma + \#K + 1, \ldots, \#\Sigma + \#K + 6).$$

where each integer is encoded by a binary string.

M is called a **deterministic Turing machine** if Δ is a function $\Delta : K \times \Sigma \to (K \cup \{h, y, n\}) \times \Sigma \times \{\leftarrow, \rightarrow, -\}$, and it is called a **non-deterministic Turing machine** otherwise.

Similarly, we can define **multi-string Turing machines**. ⌟

Prop. (2.7.2.2) [Computing with a non-deterministic Turing Machine]. Given a non-deterministic Turing machine and a finite string $x \in \mathrm{String}(\Sigma \setminus \amalg)$ called the **input of the Turing machine**, a **computation procedure** is the following:

- Write $\triangleright$ on the left of x.

- Put a cursor on $\triangleright$.
- set STATE $= s$.
- For $i \in \mathbb{Z}_+$, in the i-th step, if STATE $= p \in K$ and the cursor is pointing on ρ, choose $(q, \sigma, m) \in (K \cup \{h, y, n\}) \times \Sigma \times \{\leftarrow, \rightarrow, -\}$ s.t. $(p, \rho, q, \sigma, m) \in \Delta$, then replace the symbol pointed by the cursor by σ, replace STATE $= q$, and move the cursor according to m.
- If STATE $\in \{h, y, n\}$, stop.

Notice the cursor will never fall left to the leftmost $\triangleright$ we wrote. But it may go to the right of x, in which case we assume it reads $\amalg$. So the string may become longer.

The **output of the Turing machine** $M(x)$ is defined to be

- 'yes' if the machine stops with STATE $= y$, in which case we say this machine **accepts the input** in this procedure,
- 'no' if the machine stops with STATE $= n$, in which case we say this machine **rejects the input** in this procedure,
- the longest string following the leftmost $\triangleright$ and ending with a symbol in $\Sigma \setminus \amalg$, if the machine stops with STATE $= h$. In which case we say this machine **halted at the input** in this procedure.
- '$\nearrow$' if the machine never stops in this procedure.

$\lrcorner$

Def. (2.7.2.3) [Monte-Carlo Turing Machines]. $\lrcorner$

Def. (2.7.2.4) [Las-Vegas Turing Machines]. $\lrcorner$

<u>**Languages and Computation**</u>

Def. (2.7.2.5) [Languages]. Given a set of symbols Σ(containing $\amalg$), A **language on** Σ is a set of strings of symbols $\mathcal{L} \subset \text{String}(\Sigma \setminus \amalg)$. $\lrcorner$

Def. (2.7.2.6) [Recursive languages]. Given a set of symbols Σ containing $\amalg$ and a language on Σ, a deterministic Turing machine M with alphabet Σ is said to **decide the language** $\mathcal{L}$ if for any $x \in \text{String}(\Sigma \setminus \amalg)$, $M(x) = y$ if $x \in \mathcal{L}$ and $M(x) = n$ if $x \notin \mathcal{L}$.

$\mathcal{L}$ is called a **recursive**(or **computable/decidable**) language if it is decided by some deterministic Turing machine on Σ. $\lrcorner$

Def. (2.7.2.7) [Recursively Enumerable languages]. Given a set of symbols Σ containing $\amalg$ and a language on Σ, a deterministic Turing machine M with alphabet Σ is said to **accept the language** $\mathcal{L}$ if for any $x \in \text{String}(\Sigma \setminus \amalg)$, $M(x) = y$ if $x \in \mathcal{L}$ and $M(x) = \nearrow$ if $x \notin \mathcal{L}$.

$\mathcal{L}$ is called a **recursively enumerable**(or **computably enumerable/semidecidable/partially decidable/provable/Turing-recognizable**) language if it is accepted by some deterministic Turing machine on Σ.

The class of recursively enumerable languages is denoted by RE, and the class of complements of enumerable languages is denoted by co-RE. $\lrcorner$

Cor. (2.7.2.8). A recursive language is recursively denumerable. $\lrcorner$

Def. (2.7.2.9) [Recursive Functions]. Given a set of symbols Σ containing $\amalg$ and a function $f : \text{String}(\Sigma \setminus \amalg) \to \text{String}(\Sigma)$, a deterministic Turing machine M with alphabet Σ is said to **compute** f if for any $x \in \text{String}(\Sigma \setminus \amalg)$, $M(x) = f(x)$.

f is called a **recursively function** language if it is decided by some deterministic Turing machine on Σ. ⌟

Def. (2.7.2.10) [Non-deterministic Computations]. Given a set of symbols Σ containing $\amalg$ and a language on Σ, a non-deterministic Turing machine M with alphabet Σ is said to **decide the language** $\mathcal{L}$ if for any $x \in \text{String}(\Sigma \setminus \amalg)$, $M(x) = y$ iff $x \in \mathcal{L}$. ⌟

3 Computability

Remark (2.7.3.1) [Church-Turing Thesis]. Church proposed the assertion that every set of n-tuples of positive integers that is intuitively recursive is in fact Turing recursive.

"intuitively recursive" is not a mathematical statement, so this assertion has no mathematical proof or disproof. It is empirically right, and usually believed to be right.

The guiding role of this thesis played to mathematics should be compared to the role law of conservation of energy played to physics. Namely, once the the Turing undecidability of a set has been proved, one need not spend one's time seeking a universal method for recognizing the elements of that set. ⌟

Def. (2.7.3.2) [Universal Turing Machine]. There is a **universal Turing machine** U that with the input of a pair (M, x) where M is a Turing machine(2.7.2.1) and x is a input for M, the output of U is $U(M, x) = M(x)$. ⌟

Proof: Cf.[Computational Complexity, P57]. □

4 P and NP

<u>**Complexity Classes**</u>

Def. (2.7.4.1) [Complexity Classes]. Given a multi-string Turing machine model, a mode of computation, and a bound $f : \mathbb{N} \to \mathbb{N}$ on the resources, a **complexity class** is defined as the set of all languages(2.7.2.5) decided by some multi-string Turing machine M operating in this mode s.t. for any input x, each computation procedure of M expends at most $f(|x|)$ units of the specified resource. For example,

- $\text{TIME}(f)$: decided by a deterministic Turing machine in f times.
- $\text{SPACE}(f)$: decided by a deterministic Turing machine in f spaces.
- $\mathtt{P} = \cup_{j \in \mathbb{Z}_+} \text{TIME}(n^j)$: decided by a deterministic Turing machine in polynomial times.
- $PSPACE = \cup_{j \in \mathbb{Z}_+} \text{SPACE}(n^j)$: decided by a deterministic Turing machine in polynomial spaces.
- $\text{EXP} = \cup_{j \in \mathbb{Z}_+} \text{TIME}(2^{n^j})$: decided by a deterministic Turing machine in exponential times.
- $L = \text{SPACE}(\log n)$: decided by a deterministic Turing machine in log spaces.
- $\text{NTIME}(f)$: decided by a non-deterministic Turing machine in f times.
- $\mathtt{NP} = \cup_{j \in \mathbb{Z}_+} NTIME(n^j)$: decided by a non-deterministic Turing machine in polynomial time.
- co-$\mathtt{NP}$: The complement is in $\mathtt{NP}$.
- $NSPACE(f)$: decided by a non-deterministic Turing machine in f spaces.
- $NPSPACE = \cup_{j \in \mathbb{Z}_+} NSPACE(n^j)$: decided by a non-deterministic Turing machine in polynomial spaces.

- $NL = NSPACE(\log n)$: decided by a non-deterministic Turing machine in log spaces.
- $BP(f)$: decided by a two-sided Monte-Carlo Turing machine in f times.
- $BPP = \cup_{j\in\mathbb{Z}_+} BP(n^j)$: decided by a two-sided Monte-Carlo Turing machine in polynomial times.
- $R(f)$: decided by a one-sided Monte-Carlo Turing machine in f times.
- $RP = \cup_{j\in\mathbb{Z}_+} R(n^j)$: decided by a one-sided Monte-Carlo Turing machine in polynomial times.
- co-RP: The complements is in RP.
- $ZPP = RP \cap$ co-RP: decided by a Las-Vegas Turing machine in polynomial expected time.

⌟

Def. (2.7.4.2) [Proper Complexity Functions]. Cf.[Computational Complexity]P140. ⌟

Def. (2.7.4.3) [Hard and Complete Problems]. For a computational complexity class $\mathcal{C}$, a decision problem $X \subset I$ is called **$\mathcal{C}$-hard** if every problem in $\mathcal{C}$ can be reduced to it. And it is called **$\mathcal{C}$-complete** if it is $\mathcal{C}$-hard and it is in $\mathcal{C}$. ⌟

Prop. (2.7.4.4). Suppose a (deterministic or nondeterministic) Turing machine M decides a language $\mathcal{L}$ within time/space $f(n)$, where f is a proper complexity function(2.7.4.2), then there is a precise Turing machine M', which decides the same language in time/space $O(f(n))$. ⌟

Proof: Cf.[Computational Complexity]P141. □

Prop. (2.7.4.5) [Multi-String and Quadratic Time]. Given a multi-string deterministic Turing machine N and a language $\mathcal{L}$ decided by N in time $f(n)$, there is a single-string deterministic Turing machine M that determines $\mathcal{L}$ in time $O(f(n)^2)$. ⌟

Proof: Cf.[Computational Complexity]P30. □

Prop. (2.7.4.6) [Non-Deterministic Machines and Exponential Time]. Given a non-deterministic Turing machine N, there exists $C = C(N) \in \mathbb{R}_{>1}$ s.t. if a language $\mathcal{L}$ is decided by N in time $f(n)$, then it is decided by a 3-string deterministic Turing machine M in time $O(C^{f(n)})$. In particular,

$$\mathrm{NTIME}(f(n)) \subset \cup_{C\in\mathbb{R}_{>1}} \mathrm{TIME}(C^{f(n)}).$$

⌟

Proof: Cf.[Computational Complexity]P47. □

Prop. (2.7.4.7). $RP \subset \mathtt{NP} \subset PSPACE$. ⌟

Proof: □

Prop. (2.7.4.8). $\mathtt{P} \subset BPP$. ⌟

Proof: □

Conj. (2.7.4.9). What is the relation between BPP and $\mathtt{NP}$**?**. ⌟

Proof: □

Conj. (2.7.4.10) [Cook's Hypothesis]. $\mathtt{P} \neq \mathtt{NP}$. ⌟

Proof: □

5 Inside $\mathtt{P}$

6 Beyond $\mathtt{NP}$

7 Algebraic Complexity Theory

2.8 Computer Systems

References are [Computer Systems, a Programmer's Perspective].

1 Program Structure and Execution

2 Running Programs on a System

3 Interaction and Communication between Programs

4 Error Handling

2.9 Theoretical Computer Science

2.10 Computer Algebra

References are [Computer Algebra].

1 Euclid

Basic Algorithms

Euclidean Algorithms

Modular Algorithms

Resultants and gcd

2 Newton

Multiplications

Algo. (2.10.2.1) [Schönhage–Strassen Modular Exponentiation Algorithm]. There is an algorithm to calculate $x^r \mod n$ for l-bits numbers x, r, n in $O(l^2 \log l \log\log l)$ times. ⌟

Proof: □

Algo. (2.10.2.2) [Multiplication Algorithm, Harvey-van der Hoeven]. There is an algorithm that computes the product of two n-bit integers in $O(n \log n)$ times. ⌟

Proof: □

Fourier Transforms

Def. (2.10.2.3) [Discrete Fourier Transform]. The **inverse Fourier transform** is defined to be:

$$(x_0, \ldots, x_{n-1}) \mapsto (y_0, \ldots, y_{n-1}), \quad y_k = \frac{1}{N}\sum_{j=0}^{N-1} \omega_N^{jk} x_k.$$

This is in fact represented by a van der Waerden matrix of ω_N times $\frac{1}{N}$. ⌟

Prop. (2.10.2.4) [Fast Fourier Transform]. There is a **fast Fourier transform algorithm** that can calculate the Fourier transform in $O(N \log N)$ time. ⌟

Proof: □

Newton Iterations

Polynomial Evaluations and Interpolations

Linear Algebras

3 Gauss

Factorizing Polynomials over Finite Fields

Short Vectors in Lattices

4 Fermat

See also the section on computational number theory.

Primality Testing

Factorizing Integers

5 Hilbert

Gröbner Basis

Symbolic Integration

2.11 C++

References are [C++ Primer].

1 Data Structures

Def. (2.11.1.1) [Data]. What is a datum.

A **data structure** is a logical grouping of data and operations on that data. ⌟

2 Computer System Basics

Def. (2.11.2.1) [Buffer]. A **buffer** in a computer is a region of storage used to hold data. IO facilities often store input (or output) in a buffer and read or write the buffer independently from actions in the program. Output buffers can be explicitly flushed to force the buffer to be written. By default, reading tt cin flushes tt cout; tt cout is also flushed when the program ends normally. ⌟

Def. (2.11.2.2) [Console Windows]. ⌟

Def. (2.11.2.3) [Operands]. ⌟

Def. (2.11.2.4) [IO Devices]. ⌟

3 Basic Notions

Fact (2.11.3.1) [C++ Language]. C++ is a high-level, general-purpose programming language created by Danish computer scientist Bjarne Stroustrup.

Like other programing languages, C++ provides a common set of features, for examples

- Build-in types as integers types, characters, etc.(2.11.4.1),
- Variables(2.11.4.2), which let us give names to the objects we use.
- Expressions and statements(2.11.6.1) to manipulate values of these types.
- Control structures, such as if or while, that allow us to conditionally or repeatedly execute a set of actions.
- Functions(2.11.7.1) that let us define callable units of computation.

And it distinguishes from other programing languages in the feature of

- Classes(2.11.8.1), which let programmers define their own types that include operations as well as data, which are as easy to use as the built-in types.

⌟

Fact (2.11.3.2) [Philosophy of C++]. Throughout C++'s life, its development and evolution has been guided by a set of principles:

1. It must be driven by actual problems and its features should be immediately useful in real world programs.
2. Every feature should be implementable (with a reasonably obvious way to do so).
3. Programmers should be free to pick their own programming style, and that style should be fully supported by C++.
4. Allowing a useful feature is more important than preventing every possible misuse of C++.

5. It should provide facilities for organising programs into separate, well-defined parts, and provide facilities for combining separately developed parts.
6. No implicit violations of the type system (but allow explicit violations; that is, those explicitly requested by the programmer).
7. User-created types need to have the same support and performance as built-in types.
8. Unused features should not negatively impact created executables (e.g. in lower performance).
9. There should be no language beneath C++ (except assembly language).
10. C++ should work alongside other existing programming languages, rather than fostering its own separate and incompatible programming environment.
11. If the programmer's intent is unknown, allow the programmer to specify it by providing manual control.

⌟

Def. (2.11.3.3) [C++ Programs]. A **C++ program** is a combination of codes that can be used to solve real world problems. It is usually stored in computer files, referred to as the **source files**. ⌟

Fact (2.11.3.4) [How to Compile a C++ Program]. How to compile a program depends on the ongoing operating system and compiler. Many PC-based compilers are run from an integrated development environment (IDE) that bundles the compiler with build and analysis tools.?

On a command-line interface, a program is usually compiled in a console window(2.11.2.2).

```
$ CC prog1.cc
```

where tt $ is the system prompt. ⌟

Def. (2.11.3.5) [Headers]. A **header** in the C++ language is a mechanism whereby the definitions of a class or other names are made available to multiple programs. A program uses a header through a tt #include directive, cf.(2.11.9.1)(2.11.8.1). ⌟

Def. (2.11.3.6) [Comments]. A **comment** in a C++ program is a fragment of codes that helps whoever reads this code but ignored by the compiler. There are two kinds of comments: single-lined and multi-lined: comments start with a "//" symbol and ends with a newline:

```
// any comments you want to write.
```

and everything to the right of the slashes on the current line is ignored by the compiler, so it can contain anything but a newline.

Another kind of comments are multi-lined, which starts with a "/*" symbol and ends with a "*/" symbol:

```
/* any comments

that you want to write.
*/
```

and everything that falls between the "/*" and "*/" is ignored by the compiler, so it can contain anything but a "*/" symbol.

In particular, two fragment of comments cannot intersect each other. ⌟

4 Variables and Types

Def. (2.11.4.1) [Data Types]. A **type of a datum**(2.11.1.1) is an indication of the contents of this datum and also the operations that can be applied to this datum. Types are fundamental to any program: They tell us what our data mean and what operations we can perform on those data. ⌟

Def. (2.11.4.2) [Variables]. A **variable** in the C++ language is an object with name and types. A variable is defined by the following statement:

```
variable_type variable_name;
```

When defining a variable, we can **initialize** it at the same time, which means giving it a value at the same time that it is created. For example,

```
int v1=0;
```

⌟

5 Operators

Def. (2.11.5.1)[Operators]. An **operator** is a C++ language specifies an action and return an object. There are some common operators:

- The **dot operator** "tt .", which can be used to access a member function(2.11.8.1)(on the right-hand side) of an variable(2.11.4.2) of class type(2.11.8.1)(on the left-hand side), and return this member function. For example:

  ```
  variable_name.member_function
  ```

- The **call operator** "tt (", "tt)", which can be used to call a function(2.11.7.1)(on the left-hand side), and return this function. For example,

  ```
  main()
  ```

  or

  ```
  variable_name.member_function()
  ```

  A pair of parenthesis operator can enclose a (possibly empty) list of arguments(2.11.7.1) used to call this function.

- The scope operator "tt ::" is used to access names(on the right-hand side) in a namespace(on the left-hand side), and returns this name. For example,

  ```
  std::cout
  ```

⌟

6 Statements

Def. (2.11.6.1)[Statements]. A statement in a C++ program(2.11.3.3) that specifies an action to take place when the program is executed. Statements can contain other statements within themselves. ⌟

7 Functions

Def. (2.11.7.1) [Functions]. Every C++ program contains some **functions**, which is a unit of computation that can be called by the parenthesis operator(2.11.5.1) to be used, and generate a single output from several inputs. It consists of

- A **return type**, which is the type of the value returned by a function(2.11.4.1).
- A **function name**, which is the name by which a function is known, and the function can be called using the name.
- A **parameter list**, which is a list that specifies what **arguments**(i.e. values passed to this function) can be used to call the function.
- A **function body**, which is a sequence of zero or more statements(2.11.6.1) enclosed in curly braces, that defines the actions performed by a function.

Every function is displayed as follows:

```
return_type function_name(parameter_list){
    function_body
}
```

where the function body consists of a block of statements(2.11.6.1), each marked with a symbol ";". The block is delimited by a pair of curly braces "{" and "}". And the last statement must be a **return statement**, which determines the function, and also can be used to return a value to the function's caller. If it returns a value, the value must be compatible with the return type of this function. ⌟

Def. (2.11.7.2) [Main Function]. A **main function** in a C++ program(2.11.3.3) is a function(2.11.7.1) called by the operating system to execute this program. Each program must have one and only one function named main. The main function must have integer return type. The empty main function which return a value 0 to the system:

```
int main(){
    return 0;
}
```

The returning value 0 is usually an indication of a successes of running this function, and the returning value -1 is by default treated as a failure indicator. ⌟

8 Classes

Def. (2.11.8.1)[Classes]. A **class** in the C++ language is a facility for defining our own data structures together with associated operations, called its **member functions**. How these data are stored or computed is a question?.

A **class type** is a data type(2.11.4.1) defined by a class(2.11.8.1). A class determines all the operations that can be used on objects of this class type.

A class can be called by the directive tt #include:

```
#include "class_header";
```

Notice that we use the double quote """ symbols when the class is not defined by the standard library, cf.(2.11.9.1). ⌟

Copy Control

Overloaded Operations and Conversions

Object-Oriented Programming

Templates and Generic Programming

9 Standard Library

Def. (2.11.9.1) [Standard Library]. The **standard library** is a collection of types and functions that every C++ compiler must support. It has several sub-libraries, for example,

- The IO library.

Each library has a header(2.11.3.5), and they can be called by the directive tt #include:

```
#include <library_header>;
```

Notice this statement must be written in a single line, and outside any functions(2.11.7.1). Usually, these statements are placed at the begging of the program.

Each type defined in the standard library is called a **library type**. ⌟

Def. (2.11.9.2) [Namespaces]. A **namespace** is a mechanism for putting names defined by a library(2.11.9.1) into a single place. Namespaces help avoid inadvertent name clashes. Namespaces allow us to avoid inadvertent collisions between the names we define and uses of those same names inside a library. The names defined by the standard library are in the namespace tt std. ⌟

Input and Output

Def. (2.11.9.3)[Streams]. A **stream** in C++ language is a sequence of characters read from or written to an IO device(2.11.2.4). ⌟

Fact (2.11.9.4) [Iostream Library]. The **iostream** is a header that provides the library types(2.11.9.1) for stream-oriented(2.11.9.3) input and output. It contains two types, the **istream** providing stream-oriented input, and the **ostream** providing stream-oriented output. ⌟

Def. (2.11.9.5) [Standard Input/Output]. A **standard input/output** is an input/output stream(2.11.9.3) usually associated with the window in which the program executes.

A **standard error** is an output stream used for error reporting and warning. Ordinarily, the standard output and the standard error are tied to the window in which the program is executed. ⌟

Fact (2.11.9.6) [Some IO-Type Objects].

- tt cin is an object of type istream used to read from the standard input.
- tt cout is an object of type ostream used to write to the standard output.
- tt cerr is an object of type ostream tied to the standard error, which often writes to the same device as the standard output. By default, writes to tt cerr are not buffered(2.11.2.1). Usually used for error messages or other output that is not part of the normal logic of the program.
- tt clog is an object of type ostream tied to the standard error. By default, writes to clog are buffered(2.11.2.1). tt clog is usually used to report information about program execution to a log file.
- A **manipulator** is an object, such as tt std::endl, that when read or written “manipulates”the stream itself.

⌟

Def. (2.11.9.7) [Some IO Operators].

- The **output operator** " `<<`" writes the right-hand side operand to the output stream indicated by the left-hand operand, and returns the left-hand side. For example, `cout << "hi"` writes tt hi to the standard output(2.11.9.5). standard output.
- The input operator reads from the input stream specified by the left-hand side operand to the right-hand operand, and returns the left-hand side. For example, `cin >> i` reads the next value on the standard input(2.11.9.5) into `i`.

⌟

Sequential Containers

Generic Algorithms

Associative Containers

Dynamical Memory

Specialized Library Facilities

10 Tools for Large Programs

11 Specialized Tools and Techniques

3 Algebras

3.1 Group Theory

Main References are [Finite Groups, Issac], [?] and [代数学引论，丁石孙].

Notation (3.1.0.1).
- Use notations defined in Set Theory.

⌟

1 Magmas

Def. (3.1.1.1) [Binary Operators]. A **binary operator** on a set X is a map $\circ : X \times X \to X$. ⌟

Def. (3.1.1.2) [Unital Operator]. A **unital binary operator** on a set X is a map $\circ : X \times X \to X$ that has a left and right identity element $1_\circ$. ⌟

Prop. (3.1.1.3) [Associative Operators]. An **associative operator** on a set X is an operator $\circ : X \times X \to X$ s.t. $(x \circ y) \circ z = x \circ (y \circ z)$ for any $x, y, z \in X$. ⌟

Def. (3.1.1.4) [Magma]. A **magma** is a set X with a binary operator $\circ : X \times X \to X$. A **unital magma** is a magma that the operator is unital. It is called **Abelian** if $x \circ y = y \circ x$ for any $x, y \in X$. ⌟

Prop. (3.1.1.5) [Eckmann-Hilton argument]. If $\circ$ and $\otimes$ are two unital binary operators on a set that commute with each other: $(a \otimes b) \circ (c \otimes d) = (a \circ c) \otimes (b \circ d)$, then they are equal and in fact commutative and associative. ⌟

Proof: Firstly the units coincide, because

$$1_\circ = 1_\circ \circ 1_\circ = (1_\otimes \otimes 1_\circ) \circ (1_\circ \otimes 1_\otimes) = (1_\otimes \circ 1_\circ) \otimes (1_\circ \circ 1_\otimes) = 1_\otimes \otimes 1_\otimes = 1_\otimes.$$

Next

$$a \circ b = (1 \otimes a) \circ (b \otimes 1) = (1 \circ b) \otimes (a \circ 1) = b \otimes a = (b \circ 1) \otimes (1 \circ a) = (b \otimes 1) \circ (1 \otimes a) = b \circ a.$$

Thus $\circ$ and $\otimes$ coincide and are commutative. Finally for associativity:

$$(a \otimes b) \otimes c = (a \otimes b) \otimes (1 \otimes c) = (a \otimes 1) \otimes (b \otimes c) = a \otimes (b \otimes c).$$

□

Def. (3.1.1.6) [Monoid]. A **monoid** is an associative unital magma $(X, \circ)$. ⌟

2 Groups

Def. (3.1.2.1) [Groups, Cayley1854]. **?**, The category of Groups is denoted by $\mathcal{G}\mathrm{rp}$. ⌟

Def. (3.1.2.2) [Generators]. Let $G \in \mathcal{G}\mathrm{rp}$ and $S \subset G$, then S is said to be a **set of generator** for G if the only subgroup of G containing S is G. ⌟

Def. (3.1.2.3) [Normal Subgroups]. A **normal subgroup** of a group G is a subgroup N that if $x \in G$, then $x^{-1}Nx = N$. ⌟

Def. (3.1.2.4) [Simple Groups]. A **simple group** is a group that has no normal subgroups. ⌟

Def. (3.1.2.5) [Finitely Generated Group]. A group G is called finitely generated if there is a finite subset S that the only subgroup containing S is G itself. ⌟

Def. (3.1.2.6) [Product Subgroups]. Let G be a group and N, H be subgroups such that N is normal in G, then $NH = \{x \in G | x = nh, n \in N, h \in H\}$ is a subgroup of G, called the **product subgroup**. ⌟

Def. (3.1.2.7) [Coset]. Let G be a group and H a subgroup. Consider the equivalence relation on G s.t. $x \sim y$ iff $x = yh$ for some $h \in H$, then the equivalence classes is denoted by G/H, called the **right coset** of H in G. And G acts on this set by left translation.

Similarly we can define **left coset** $H\backslash G$ of H in G.

Moreover, if H is normal in G, then this set is a group with structure given by $\tau H \cdot \sigma H = \tau\sigma H$, called the **quotient group** structure. It satisfies the universal property that any group homomorphism $\varphi : G \to G'$ s.t. $\varphi(H) = e$ factors through G/H uniquely. ⌟

Prop. (3.1.2.8) [Fundamental Isomorphisms]. Let G be a group and N, H be subgroups such that N is normal in G, then

- there is a natural isomorphism $G/NH \cong (G/N)/(H/H \cap N)$ as sets, and if H is also normal, this is an isomorphism of groups.
- there is a natural isomorphism of groups: $H/N \cap H \cong NH/N$.

⌟

Proof: 1:

2: Consider the natural isomorphism $N \mapsto NH/H : n \mapsto nH$, then it is a group homomorphism, and the kernel is $N \cap H$, thus we are done. □

Cor. (3.1.2.9). if H_1, H_2 are subgroups of a group G that has finite indexes, then $H_1 \cap H_2$ also has finite index in G. ⌟

Proof: By fundamental isomorphism(3.1.2.8), $H_1/H_1 \cap H_2 \cong H_1H_2/H_2 \subset G/H_2$, so $H_1 \cap H_2$ has finite index in H_1, so by transitivity of indexes, $H_1 \cap H_2$ has finite index in G. □

Def. (3.1.2.10) [Index of Subgroup]. The **index of a subgroup** H in a group G is defined to be the number of the left coset G/H, if it is finite. Now if H has finite index in G, then $|G/H| = |H\backslash G|$. ⌟

Proof: Because for any system of representative a_i for the left coset G/H, a_i^{-1} is a representative for the right coset $H\backslash G$, and vise versa. □

Prop. (3.1.2.11). If a finite group G has an automorphism α that $\alpha^2 = \mathrm{id}$ and α has no fixed point other than e, then G is an Abelian group of odd order. ⌟

Proof: G is clearly of odd order. Consider the map $g \mapsto \alpha(g)g^{-1}$, then it is injective, hence it is also surjective, and consider $\alpha(\alpha(g)g^{-1}) = g\alpha(g)^{-1} = (\alpha(g)g^{-1})^{-1}$, thus $\alpha(h) = h^{-1}$ for all $h \in G$, thus clearly G is Abelian. □

Prop. (3.1.2.12). If H is a subgroup of a finite group G, then $G \neq \cup g^{-1}Hg$. ⌟

Proof: There are at most $|G/H|$ different summands in the right hand side, so it doesn't have enough elements. □

Prop. (3.1.2.13). If G is a f.g. group(3.1.2.5) and H is a group of finite index in G, then H is f.g. ⌟

Proof: Suppose G has generators g_i, we may add their inverses to it, and let $Ht_1, \ldots, Ht_m$ are all the right cosets with $t_1 = 1$, then there are h_{ij} that $t_i g_j = h_{ij} t_{k_{ij}}$, then we claim H is generated by h_{ij}.

For this, consider any $h = \prod g_{i_r}$, then $g_1 = h_{1i_r} t_{k_{1i_r}}$, and we can do this from left to right. Now $h = \prod h_{i_s j_s} t_o$, then t_o must by 1, and we are done. □

Prop. (3.1.2.14). Let $\varphi : G \to H$ be a map of sets between groups s.t. $\#\mathrm{Im}(\varphi) = \infty$, and for each $g \in G$, there is a set $S(g) \in H$ that $\varphi(h)\varphi(g) = \varphi(hg)$ for any h s.t. $\varphi(h) \notin S(g)$, then φ is a homomorphism. ⌟

Proof: For $g, h \in G$, take f s.t. $\varphi(f) \notin S(g) \cup \varphi(g)^{-1}S(h) \cup \{\varphi(gh)\}$. Then

$$\varphi(f)\varphi(g)\varphi(h) = \varphi(fg)\varphi(h) = \varphi(fgh) = \varphi(f)\varphi(gh),$$

thus $\varphi(g)\varphi(h) = \varphi(gh)$. □

3 Abelian Groups

Remark (3.1.3.1). An Abelian group is the same as a module over $\mathbb{Z}$. Thus the theory of commutative algebra applies in this case. The category of Abelian groups is denoted by $\mathcal{A}\mathrm{b}$. The category of finite Abelian groups are denoted by $\mathcal{A}\mathrm{b}^{\mathrm{fin}}$. ⌟

Prop. (3.1.3.2) [Abelianization]. There is a functor from the category of Abelian semi-groups to the category of Abelian groups that is left adjoint to the forgetful functor, called the **Abelianization**. ⌟

Proof: Define A' to be the quotient

$$\bigoplus_{(a,b)\in A^2} \mathbb{Z} \to \bigoplus_{x\in A} \mathbb{Z} \to A' \to 0,$$

where $1_{(a,b)}$ is mapped to $1_a + 1_b - 1_{a+b}$. Then it can be seen this satisfies the universal property and it is functorial in A. □

Prop. (3.1.3.3) [Classifying F.g. Abelian Groups]. Any finitely generated Abelian group is of the form

$$\mathbb{Z}^r \bigoplus_{p_i \text{ primes}} \oplus_{j\leq n_i} \mathbb{Z}/(p_i^{a_{i,j}})$$

⌟

Proof: As $\mathbb{Z}$ is PID, the classifying theorem follows immediately from(3.2.4.21): □

Prop. (3.1.3.4) [Baer-Specker Group]. The group $\prod^{\mathbb{N}} \mathbb{Z}$ is called the **Baer-Specker group**. Then the natural homomorphism

$$\mathrm{Hom}(\prod^{\mathbb{N}} \mathbb{Z}, \mathbb{Z}) \to \prod^{\mathbb{N}} \mathbb{Z}$$

is injective with image $\bigoplus^{\mathbb{N}} \mathbb{Z}$.. In particular, by countability argument, $\prod^{\mathbb{N}} \mathbb{Z}$ is not a free group(5.3.1.5). Moreover, any infinite direct product of $\mathbb{Z}$ is not free, because otherwise the subgroup $\prod^{\mathbb{N}} \mathbb{Z}$ would be free. ⌟

Proof: The natural homomorphism is the composite**?**

$$\mathrm{Hom}(\prod^{\mathbb{N}} \mathbb{Z}, Z) \xrightarrow{\varepsilon^*} \mathrm{Hom}(\#^{\mathbb{N}}\mathbb{Z}, \mathbb{Z}) \xrightarrow{\eta} \prod^{\mathbb{N}} \mathbb{Z}.$$

Thus the assertion follows from(3.1.5.6) and(3.1.5.5). □

Remark (3.1.3.5). This can be proven in other ways, like using condensed mathematics.**?**. ⌟

Forms on Abelian Groups

Def. (3.1.3.6) [Quadratic Forms]. For $A \in \mathcal{A}b$, a function $d : A \to \mathbb{R}$ is called a **quadratic form** if

- $d(\alpha) = d(-\alpha)$ for any $\alpha \in A$.
- The form $B_d : A \times A \to \mathbb{R}$: $(\alpha, \beta) \mapsto [d(\alpha + \beta) - d(\alpha) - d(\beta)]/2$ is bilinear.

It is called **positive semi-definite** if moreover $d(\alpha) \geq 0$. And **positive-definite** if moreover $d(\alpha) = 0 \iff \alpha = 0$. ⌟

Prop. (3.1.3.7) [Cauchy-Schwartz]. Let A be an Abelian group and d a positive semi-definite quadratic form over A, then

$$|d(\alpha - \beta) - d(\alpha) - d(\beta)| \leq 2\sqrt{d(\alpha)d(\beta)}.$$

⌟

Proof: Consider the bilinear form B_d, then

$$0 \leq d(m\alpha - n\beta) = m^2 d(\alpha) + n^2 d(\beta) - 2mnB_d(\alpha, \beta).$$

This is true for any $m, n \in \mathbb{Z}$, thus the discriminant $B_d(\alpha, \beta)^2 \leq d(\alpha)d(\beta)$. □

Prop. (3.1.3.8). If M, N are Abelian groups and d is a quadratic form on $M \times N$ s.t. $d(0 \times N) = d(M \times 0) = 0$, then d is bilinear in both M and N. ⌟

Proof: The bilinear form associated to d satisfies $B_d((a, 0), (0, b)) = d(a, b)$, thus it is clear d is bilinear in M and N. □

Def. (3.1.3.9) [Polarization]. Let Γ be an Abelian group and $h : \Gamma \to \mathbb{R}$ is a function, then the r-th **polarization function** $P_r(h) : \Gamma^r \to \mathbb{R}$ is defined to be

$$P_r(h)(x_1, \ldots, x_r) = \frac{1}{r!} \sum_{I \subset \{1, \ldots, r\}} (-1)^{r - \# I} (\sum_{i \in I} x_i).$$

⌟

Lemma (3.1.3.10).

- Let $\tau_a(h)(x) = h(a+x) - h(x)$, then $\tau_a\tau_b = \tau_{a+b} - \tau_a - \tau_b$.
- $P_r(h)(x_1,\dots,x_r) = \tau_{x_1}\tau_{x_2}\dots\tau_{x_r}(h)(0) = \tau_{x_2}\dots\tau_{x_r}(h)(x_1)$.
- If $A_r \in \operatorname{Sym}^r\Gamma^\vee$, let $\Delta A_r : \Gamma : \mathbb{R} : \Delta A_r(x) = \frac{1}{r!}A_r(x,\dots,x)$, then $\tau_a\Delta A_r(x) = \sum_{1\le s<r}\Delta A_s$, where $A_s \in \operatorname{Sym}^s\Gamma^\vee$, and $A_{r-1}(x_1,\dots,x_{r-1}) = A_r(x_1,\dots,x_{r-1},a)$.
- If $A_r \in \operatorname{Sym}^r\Gamma^\vee$, $P_r(\Delta A_r)(x_1,\dots,x_n) = A_r(x_1,\dots,x_r)$ and $P_s(\Delta A_r) = 0$ for $s > r$.

⌟

Prop. (3.1.3.11). There is a natural isomorphism of additive groups

$$\bigoplus_{j=0}^{r-1}\operatorname{Sym}^j\Gamma^\vee \cong \{h:\Gamma\to\mathbb{R}|P_r(h)=0\} : (A_0,\dots,A_{r-1}) \mapsto \sum_{i=0}^{r-1}\Delta A_i.$$

⌟

Proof: This is an injective map by(3.1.3.10), and for any h that $P_r(h) = 0$, By(3.1.3.10) item1, this means $A_{r-1} = P_{r-1}(h) \in \operatorname{Sym}^{r-1}\Gamma^r$. Let $h' = h - \Delta A_{r-1}$, then(3.1.3.10) item4 shows $P_{r-1}(h') = 0$, thus we can use induction to show $h' = \sum_{i=1}^{r-2}\Delta A_i$, thus $h = \sum_{i=1}^{r-1}\Delta A_i$. □

Prop. (3.1.3.12). Let Γ be an Abelian group, for functions $h_1, h_2 : \Gamma \to \mathbb{R}$, let $h_1 = h_2 + O(1)$ denote the fact that $|h_1 - h_2|$ is bounded on Γ. Then there is a natural isomorphism of additive groups:

$$\bigoplus_{j=0}^{r-1}\operatorname{Sym}^j\Gamma^\vee \cong \{h:\Gamma\to\mathbb{R}|P_r(h)=O(1)\}/O(1) : (A_0,\dots,A_{r-1}) \mapsto h(x) = A_0+A_1(x)+\dots A_{r-1}(x,\dots,x).$$

⌟

Proof: The map is injective by(3.1.3.11). To show surjectivity:

By hypothesis and(3.1.3.10), there exists $C>0$ s.t.

$$|P_{r-1}h(x_0+x_1,x_2,\dots,x_{r-1}) - P_{r-1}h(x_0,x_2,\dots,x_{r-1}) - P_{r-1}h(x_1,x_2,\dots,x_{r-1})| \le C.$$

So

$$|P_{r-1}h(2^N x_1,x_2,\dots,x_{r-1}) - 2P_{r-1}h(2^{N-1}x_1,x_2,\dots,x_{r-1})| \le C$$

for any N, and by iterating,

$$|P_{r-1}h(2^N x_1,2^N x_2,\dots,x_{r-1}) - 2^{r-1}P_{r-1}h(2^{N-1}x_1,2^{N-1}x_2,\dots,2^{N-1}x_{r-1})| \le (2^{r-1}-1)C.$$

$$\left|\frac{P_{r-1}h(2^N x_1,2^N x_2,\dots,x_{r-1})}{2^{N(r-1)}} - \frac{P_{r-1}h(2^{N-1}x_1,2^{N-1}x_2,\dots,2^{N-1}x_{r-1})}{2^{(N-1)(r-1)}}\right| \le \frac{2^{r-1}-1}{2^{N(r-1)}}C.$$

Thus

$$A_{r-1}(x_1,\dots,x_{r-1}) = \lim_{N\to\infty}\frac{P_{r-1}h(2^N x_1,2^N x_2,\dots,x_{r-1})}{2^{N(r-1)}}$$

exists, and it is clear that $A_{r-1} \in \operatorname{Sym}^{r-1}\Gamma^\vee$ and $A_{r-1}(x_1,\dots,x_{r-1}) - P_{r-1}h(x_1,\dots,x_{r-1}) \le 2^{r-1}C$. Let $h' = h - \Delta A_{r-1}$, then $P_{r-1}h' = P_{r-1}h - A_{r-1} = O(1)$, thus we can use induction to show $h' = \sum_{i=1}^{r-2}\Delta A_i + O(1)$, thus $h = \sum_{i=1}^{r-1}\Delta A_i + O(1)$. □

Cor. (3.1.3.13). Let Γ be an Abelian group and $h:\Gamma\to\mathbb{R}$ be a function on an Abelian group Γ that

$$h(\sum_{i=1}^{3}x_i)=\sum_{1\leq i<j\leq 3}h(x_i+x_j)-\sum_{i=1}^{3}h(x_i)+O(1),$$

then there exists a unique symmetric bilinear pairing b on Γ and l a homomorphism $\Gamma\to\mathbb{R}$, that

$$h(x)=\frac{1}{2}b(x,x)+l(x)+O(1).$$

⌟

Prop. (3.1.3.14). Let M be an Abelian group and $b:M\times M\to\mathbb{R}$ is a bilinear form on M that $\mathrm{rad}(B)=0$, so b defines a bilinear form on $B_{\overline{R}}:M\otimes_{\mathbb{Z}}\mathbb{R}$. Then $b_{\mathbb{R}}$ is positive-definite iff for any f.g. subgroup M' of M and $C>0$, $\{x\in M'|B(x,x)\leq C\}$ is finite. ⌟

Proof: We may assume M is f.g.. As M/M_{tor} is torsion-free, it is a lattice in $M_{\mathbb{R}}$(14.2.3.34). Assume $b_{\mathbb{R}}$ is positive-definite, then it defines a topology on $M_{\mathbb{R}}$, then $\{x\in M'|b_{\mathbb{R}}(x,x)\leq C\}$ is finite because it is a compact discrete set.

Conversely, if $\{x\in M'|b(x,x)\leq C\}$ is finite and $b_{\mathbb{R}}$ is not positive-definite, then it is at least semi-positive definite. If $b_{\mathbb{R}}(y,y)=0$, then by Cauchy-Schwartz inequality(3.1.3.7), y is in the radical of $b_{\mathbb{R}}$. By hypothesis $y\notin M_{\mathbb{Q}}$.

Now choose a basis $e_1,\ldots,e_n$ of M, for any $n>1$, there is a $y_n\in M$ s.t. $y_n-ny\in S=\{\sum\alpha_ie_i|0\leq\alpha\leq 1\}$, and

$$b_{\mathbb{R}}(y_n,y_n)=b_{\mathbb{R}}(y_n-ny,y_n-ny)$$

is bounded by the maximal value of $b_{\mathbb{R}}$ on S. These y_n are all different because $y\notin M_{\mathbb{Q}}$, thus contradicting the hypothesis. □

Prop. (3.1.3.15). Let $M\in\mathcal{A}b$ s.t. $\#M/nM<\infty$ for some $n\geq 2$ and there is a positive semi-definite symmetric bilinear form B on M s.t. $\{x\in M|B(x,x)\leq C\}$ is finite for any $C>0$, then M is f.g.. ⌟

Proof: Choose a set of generators $\{x_i\}$ for M/nM. Now there is a constant C that whenever $(x,x)\geq C$,

$$(x-x_i,x-x_i)<2(x,x),\forall i,$$

because by Cauchy-Schwartz inequality(3.1.3.7), $(x-x_i,x-x_i)$ is similar to (x,x) when (x,x) is large.

Now let $\Gamma=\{x_1,\ldots,x_s\}\cup\{x\in\Gamma|(x,x)<C\}$. Then Γ is finite by hypothesis. We prove Γ generates M: Consider the infimum C_0 of (x,x) that x is not generated by M, then there is a x that $C_0\leq(x,x)<2C_0$. Obviously $C_0\geq C$. Let $x=x_i+ny$ for some $x_i\in\Gamma,y\in M$, then

$$(y,y)=\frac{1}{n^2}(x-x_i,x-x_i)<\frac{2}{n^2}(x,x)\leq\frac{1}{2}(x,x)<C_0.$$

Thus by minimality of C_0, $y\in\Gamma$, thus $x\in\Gamma$. □

Prop. (3.1.3.16)[Lagrangian Decomposition]. Let A be a f.g. Abelian group and $\Gamma:A\times A\to\mathbb{Q}/\mathbb{Z}$ is a bilinear alternating non-degenerate pairing, then a **Lagrangian decomposition** of A is an Abelian subgroup $B\subset A$ s.t. $\Gamma|_B=0$, called an **isotropic subgroup** of A, such that $A\cong B\oplus B^\vee$, and Γ is given by

$$\Gamma((x,\chi),(y,\psi))=\chi(y)\psi(x)^{-1}.$$

Then A admits a Lagrangian decomposition. In particular, if $\#A<\infty$, then $\#A\in(\mathbb{Z}_+)^2$. ⌟

Proof: Because A is f.g., take x, y in A s.t. $\Gamma(x,y)$ has the maximal denominator, then it is easy to see that for any $z \in A$, $z - ax - by \in \mathrm{span}(x,y)^{\perp}$ for some $a, b \in \mathbb{Z}$, so $A = \mathrm{span}(a,b) \oplus \mathrm{span}(a,b)^{\perp}$, and we can use induction. □

Finite Abelian Groups

Prop. (3.1.3.17)[Characterizing Finite Cyclic Groups]. Let $G \in \mathcal{A}\mathrm{b}^{\mathrm{fin}}$ that $\#\{x \in G | x^d = 1\} \leq d$ for any $d \geq 1$, then G is cyclic. ⌟

Proof: Consider the subset G_d of elements of order d, if it is non-empty, choose $y \in G_d$, then $\#\langle y \rangle = d$, thus $\langle y \rangle = \{x \in G | x^d = 1\}$, which means $\#G_d \leq \varphi(d)$. Then $|G| = \sum_{d|n} \#G_d \leq \sum_{d|n} \varphi(d) = n$. Thus $G_n \neq \varnothing$, which means G is cyclic. □

Cor. (3.1.3.18). For $k \in$ `Field`, any finite subgroup of $k^{\times}$ is cyclic. ⌟

Cor. (3.1.3.19) [Primitive roots modulo q]. For $p \in \mathbf{P}$ and $q \in p^{\mathbb{Z}_+}$, $\mathbb{F}_q^{\times}$ is cyclic, i.e. $\mathbb{F}_q^{\times} \cong \langle \sigma \rangle$. Any such generator σ is called a **primitive root modulo** p. ⌟

4 Automorphism Groups

Def. (3.1.4.1) [Automorphisms Groups]. Let $G \in \mathcal{G}\mathrm{rp}$, the set of automorphism of G is a group, denoted by $\mathrm{Aut}(G)$.

Then for any $g \in G$, there is an automorphism $C_g \in \mathrm{Aut}(G) = \mathrm{Hom}(G,G) : x \mapsto gxg^{-1}$. And the mapping $G \to \mathrm{Aut}(G) : g \mapsto C_g$ is a group homomorphism. All automorphisms of G of the form are called **inner automorphisms** of G. The group of inner automorphisms of G is denoted by $\mathrm{Inn}(G)$. Automorphisms that are not inner are called **outer automorphisms**. ⌟

Prop. (3.1.4.2). Any group of order> 2 have at least 2 automorphisms. ⌟

Proof: Assume the contrary, consider its inner automorphism, then it is Abelian, and then multiplying by p for p large prime is not identity, Then $\#G|(p-1)$ for such G. Now it is clear $|G| = 2$, because otherwise we can choose $p \equiv 2 (\mathrm{mod}\ \#G)$. □

Def. (3.1.4.3) [Automorphic Complete Groups]. An **automorphic-complete group** is a group whose automorphisms are all inner. ⌟

Prop. (3.1.4.4). S_n is the automorphism group of A_n for $n = 5$ or $n \geq 7$. ⌟

Proof: □

Prop. (3.1.4.5). If G is a non-Abelian simple group, then $\mathrm{Aut}(G)$ is a complete group. ⌟

Prop. (3.1.4.6). S_n are complete groups except for S_6. ⌟

Proof: S_n is the automorphism group of A_n for $n = 5$ or $n \geq 7$ by(3.1.4.4), thus it is complete by(3.1.4.5). □

Prop. (3.1.4.7) [Wielandt]. If G is a finite group with trivial center, then the sequence

$$G < \mathrm{Aut}(G) < \mathrm{Aut}(\mathrm{Aut}(G)) < \dots$$

must terminate in finite steps. ⌟

Proof: □

5 Free Groups and Presentations

Def. (3.1.5.1) [Free Groups]. There is a **free group** functor $\mathrm{F} : \mathcal{S}\mathrm{et} \to \mathcal{G}\mathrm{rp}$ that is left adjoint to the forgetful functor.

The image of the set $[n-1]$ is denoted by F_n. ⌟

Proof: For the existence of F, Cf.[?]P66.**?** □

Prop. (3.1.5.2) [Nielsen-Schreier]. A subgroup H of a free group G is a free group. Moreover, a subgroup H of finite index m in F_n is isomorphic to $\mathrm{F}_{1+m(n-1)}$. ⌟

Proof: A free group is the fundamental group of a graph X which is a wedge sum of circles, and there is a covering $X_H \to X$ the $\pi_1(X_H) = H$ by(4.15.1.28). And if H is of index m in a free group G, $X_H \to X$ has degree m by(25.2.1.25). Now (25.2.1.25) shows $H = \pi_1(X_H)$ is a free group, and the final assertion follows by comparing two ways of counting Euler number χ. □

Prop. (3.1.5.3). Use the same method as in(3.1.5.2), we can determine all the subgroups of index 2 in F_2. ⌟

Proof: **?** □

Def. (3.1.5.4) [Earring Group]. For any $n \in \mathbb{Z}_+$, there are group homomorphisms $\mathrm{F}_n \to \mathrm{F}_{n-1}$ corresponding to the map of sets

$$[n-1] \to \mathrm{F}_{n-1} : i \mapsto \begin{cases} [i] & , i \le n-2 \\ 1 & , i = n-1 \end{cases}.$$

The **Earring group** $\#^{\mathbb{N}}\mathbb{Z}$ is defined to be the subgroup of

$$\varprojlim_{n\in\mathbb{N}} \mathrm{F}_n$$

consisting of elements $(w_0, w_1, \ldots, w_n, \ldots)$ s.t. if each w_n is a reduced word, then for any $k \in \mathbb{Z}_+$, the number of $[k]^{\pm}$ appearing in w_n stablizes. ⌟

Prop. (3.1.5.5). The natural homomorphism

$$\eta : \mathrm{Hom}(\#^{\mathbb{N}}\mathbb{Z}, \mathbb{Z}) \to \prod^{\mathbb{N}} \mathbb{Z}$$

is injective with image $\oplus^{\mathbb{N}}\mathbb{Z}$. ⌟

Proof: Cf.https://wildtopology.com/2014/05/09/the-hawaiian-earring-group-is-not-free-part-i/. □

Prop. (3.1.5.6). There is a natural group homomorphism $\varepsilon : \#^{\mathbb{N}}\mathbb{Z} \to \prod^{\mathbb{N}} \mathbb{Z}$ that is surjective. ⌟

Proof: The k-th coordinate of this map is given by omitting all the elements that is not $[k]$. It is clearly surjective. □

Prop. (3.1.5.7) [Smith]. $\#^{\mathbb{N}}\mathbb{Z}$ is not a free group. ⌟

Proof: Cf.https://wildtopology.com/2014/05/09/the-hawaiian-earring-group-is-not-free-part-i/. □

<u>**List of Presentations of Important Groups**</u>

Prop. (3.1.5.8). Let F be a field, then $SL(2,F)$ has a representation as:

$$\langle t(y), n(z), w_1\rangle, \quad y\in F^*, z\in F$$

quotient the relations:

$$t(y_1)t(y_2)=t(y_1y_2), \quad n(z_1)n(z_2)=n(z_1+z_2), \quad t(y)n(z)t(y)^{-1}=n(y^2z), \quad w_1t(y)w_1=t(-y^{-1}).$$

$$w_1n(z)w_1=t(-z^{-1})n(-z)w_1n(-z^{-1}), z\in F^*,$$

And the isomorphism is given by Φ:

$$t(y)\mapsto\begin{bmatrix} y & \\ & y^{-1}\end{bmatrix}, \quad n(z)\mapsto\begin{bmatrix} 1 & z\\ & 1\end{bmatrix}, \quad w_1\mapsto\begin{bmatrix} & 1\\ -1 & \end{bmatrix}.$$

⌟

Proof: The map vanishes on the relations is direct calculation. An inverse of Φ is constructed by

$$\Psi(\begin{bmatrix} a & b\\ c & d\end{bmatrix})=\begin{cases} n(a/c)t(-c^{-1})w_1n(d/c) & c\neq 0\\ t(a)n(b/a) & c=0\end{cases}$$

The verification of the inverse is verified by direct calculation. □

Prop. (3.1.5.9). Let F be a field, then $SL(2,F)$ is generated by $N(F)$ and any element in $SL(F)\backslash N(F)$. ⌟

Proof: Take this element in $G(F)\backslash B(F)$, left and right multiplying by elements in $N(F)$, we see it contains some $\begin{bmatrix} & -a^{-1}\\ a & \end{bmatrix}$, then it contains $\begin{bmatrix} & -a^{-1}\\ a & \end{bmatrix}^{-1}N(F)\begin{bmatrix} & -a^{-1}\\ a & \end{bmatrix}=\begin{bmatrix} 1 & \\ * & 1\end{bmatrix}$. Then it contains $N(F)\begin{bmatrix} & -a^{-1}\\ a & \end{bmatrix}=\begin{bmatrix} * & -a^{-1}\\ a & \end{bmatrix}$. Left multiplying by $\begin{bmatrix} 1 & \\ * & 1\end{bmatrix}$ and right multiplying by $N(F)$, we see it contains all diagonal matrices in $SL(2,F)$. So it contains $\begin{bmatrix} & -1\\ 1 & \end{bmatrix}$, thus contains $SL(2,F)$, by Bruhat decomposition. □

Prop. (3.1.5.10) [Metaplectic Modular Group]. In the metaplectic modular group $\mathrm{Mp}(2,\mathbb{Z})$(12.12.4.1), define

$$\widetilde{S}=(\begin{bmatrix} & 1\\ -1 & \end{bmatrix}, -\mathrm{i}\sqrt{\tau}), \quad \widetilde{T}=(\begin{bmatrix} 1 & 1\\ & 1\end{bmatrix}, \mathbb{1}), \quad \widetilde{R}=\widetilde{S}^2=(-I,-\mathrm{i}).$$

Then $\mathrm{Mp}(2,\mathbb{Z})$ is generated by $\widetilde{S},\widetilde{T}$ with relations

$$\widetilde{S}^8=(\widetilde{S}\widetilde{T})^3=1.$$

And the center $C(\mathrm{Mp}(2,\mathbb{Z}))=\langle\widetilde{S}^2\rangle\cong\mathbb{Z}/(4)$, with $\mathrm{Mp}(2,\mathbb{Z})/\{1,\widetilde{S}^4\}=\mathrm{SL}(2,\mathbb{Z})$. ⌟

Proof: ? □

Cor. (3.1.5.11). $\mathrm{SL}(2,\mathbb{Z})$ is generated by $S = \begin{bmatrix} & -1 \\ 1 & \end{bmatrix}, T = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$ with relations

$$S^4 = 1, \quad (ST)^3 = S^2$$

. ⌟

Proof: [Serre, Trees, P81]. □

Cor. (3.1.5.12) [Modular Group]. $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/\{\pm 1\}$ is generated by $S = \begin{bmatrix} & -1 \\ 1 & \end{bmatrix}, T = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$ with relations

$$S^2 = 1, \quad (ST)^3 = 1.$$

⌟

6 Sylow Theory

Prop. (3.1.6.1) [Class Equation]. For a finite group G, if $G_x = C((x))$, then

$$|G| = |C(G)| + \sum |G|/|G_x|$$

where the summation is over non-trivial conjugate classes of G. ⌟

Proof: Consider the left action of G on itself, and calculate elements. □

Cor. (3.1.6.2) [p-Groups are Solvable]. if G is a p-group, then G has a non-trivial center. In particular, any p-group is solvable. ⌟

Cor. (3.1.6.3). If $p||G|$, then G has an element of order p. ⌟

Proof: Follows from Sylow theory and any p-group has a non-trivial center. □

Lemma (3.1.6.4). For any p-group G acting on a finite set X, $|X| \equiv X^G \mod p$.(trivial). ⌟

Prop. (3.1.6.5) [Sylow Theorem, Sylow1872]. For a finite group of order $|G| = p^k m$.

- There is a Sylow p-group.
- For a Sylow p-subgroup, any p-subgroup is contained in a conjugate of P. In particular, any two Sylow p-subgroups are conjugate.
- the number of Sylow p-groups n_p satisfies: $n_p|m, n_p \equiv 1 \mod p$.

⌟

Proof: 1: Use induction, let $Z = C(G)$, if $p||Z|$, then Z contains a cyclic group of order p. Choose a p-Sylow subgroup of G/C, then its inverse image in G is a p-Sylow subgroup. If Z is prime to p, consider the conjugate action of G on $G - Z$, then some conjugacy class has order prime to p, by(3.1.6.4), then the stablizer H of this class satisfies $[G : H]$ is prime to p. Thus H contains a p-Sylow subgroup by induction.

2: If Q is a p-subgroup, then Q acts on G/P by left translation, so it has a fixed element by(3.1.6.4), $QxP = xP$ for some x, thus $Q \subset xPx^{-1}$.

3: $n_p|m$ by considering the conjugate action of P on the set of conjugates of P, then as in the proof of item2, P is the only fixed element, so $n_p \equiv 1 \mod p$ by(3.1.6.4). □

Lemma (3.1.6.6). If G has a sylow subgroup H that $|G/H|!$ is not divisible by $|G|$, then G is not simple. ⌟

Proof: Consider the conjugate action of G on the conjugacy classes of H, then it is a group homomorphism of G into a subgroup of $S_{|G/H|}$, but the hypothesis shows that it is not injective, thus the kernel is non-trivial normal. □

Prop. (3.1.6.7) [Frattini Argument]. If G is a finite subgroup, N is normal in G and P is a Sylow subgroup of N, then $NN_G(P) = G$. ⌟

Proof: For any element $g \in G$, consider $g^{-1}Pg \subset N$ is a Sylow subgroup of N, thus by Sylow theorem(3.1.6.5), there is a $n \in N$ that $g^{-1}Pg = n^{-1}Pn$, thus $gn^{-1} \in N_G(P)$, thus $g \in NN_G(P)$. □

7 Split Extension

Prop. (3.1.7.1) [Cyclic Central Extension Split]. If there is an exact sequence $0 \to Z \to G \to C \to 0$ where $Z \subset C(G)$ and C is cyclic, then G is Abelian. ⌟

Proof: This is because we can choose an inverse image of a generator of C. □

Prop. (3.1.7.2) [Schur-Zassenhaus]. An exact sequence of finite groups $0 \to A \to E \to G \to 0$ must split when $|A|$ and $|G|$ are relatively prime. ⌟

Proof: □

Prop. (3.1.7.3). Let $\alpha, \beta : G \to \mathrm{Aut}(H)$ be two actions of G on H, then theirs semiproduct sequences

$$1 \to H \to G \ltimes H \to G \to 1$$

are isomorphic iff α, β are equivalent modulo $\mathrm{Inn}(H)$. ⌟

8 Subnormality

Def. (3.1.8.1) [Normal Series]. A **subnormal series** of a group G is a descending chain of groups:

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{e\}$$

that G_{k+1} is normal in G_k. It is called a **composite series** iff each G_k/G_{k+1} is simple. ⌟

Lemma (3.1.8.2) [Butterfly Lemma]. Let H_1, H_2 be subgroups of a group G, N_1, N_2 are normal subgroups of H_1 and H_2, then there is a canonical isomorphism of groups:

$$N_1(H_1 \cap H_2)/N_1(H_1 \cap N_2) \cong N_2(H_2 \cap H_1)/N_2(H_2 \cap N_1).$$

⌟

Proof: Cf.[**?**]P20. □

Prop. (3.1.8.3) [Schreier]. Any two subnormal series of a group G have a common refinement. ⌟

Proof: □

Cor. (3.1.8.4) [Jordan-Hölder]. For any two composition series $G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = \{e\}$, $G = G'_0 \rhd G'_1 \rhd \ldots \rhd G'_{r'} = \{e\}$, there $r = r'$, and there exists a permutation $\sigma \in S_{r-1}$ s.t. $G_i/G_{i+1} \cong G'_{\sigma(i)}/G'_{\sigma(i)+1}$. ⌟

Def. (3.1.8.5) [Central Series]. A **central series** of a group G is an ascending chain of groups:

$$\{e\} = Z_0 < G_1 < \ldots < G_r = G$$

that Z_{k+1}/Z_k is in the center of G/Z_k. ⌟

Prop. (3.1.8.6). A group is

- solvable iff it has a normal series that G_i/G_{i+1} is Abelian.
- nilpotent iff it has an upper central series.

⌟

Proof: □

Def. (3.1.8.7) [Supersolvable Groups]. A group G is called a **supersolvable group** iff it has a normal series that G_i/G_{i+1} is cyclic.

If G is finite, this notion is equivalent to solvable. ⌟

Lemma (3.1.8.8) [p-Group is Nilpotent]. Any p-group is nilpotent. ⌟

Proof: Using induction by(3.1.6.2), we see it has a central series, thus nilpotent(3.1.8.6). □

Prop. (3.1.8.9) [Nilpotent Finite Groups]. If G is a finite group, then the following are equivalent:

- G is nilpotent.
- $N_G(H) > H$ for every proper subgroup $H < G$.
- Every maximal subgroup of G is normal.
- Every Sylow subgroup of G is normal.
- G is a direct product of its non-trivial Sylow subgroups.

⌟

Proof: $1 \to 2$: Choose a central series Z_n, let $Z_n \subset H$ and $Z_{n+1} \not\subset H$, then $[Z_{n+1}, H] \subset [Z_{n+1}, G] \subset Z_n \subset H$, thus $Z_{n+1} \subset N_G(H)$.

$2 \to 3, 4 \to 5$: trivial.

$3 \to 4$ For any p-Sylow subgroup G, if $N_G(P)$ is proper subgroup, then it is contained in some maximal subgroup M, and M is normal, thus by Frattini argument(3.1.6.7), $G = N_G(P)M = M$, contradiction.

$5 \to 1$: By lemma(3.1.8.8). □

Prop. (3.1.8.10) [Jordan-Horder]. For a finite group G, any two of its composite series has the same length, then the quotient groups G_k/G_{k+1} are in bijection with each other as sets. ⌟

Proof: Cf.[代数学引论 P89]. □

Prop. (3.1.8.11) [Minimal Normal Subgroup]. The minimal normal subgroup N of a finite group G is a direct product of simple groups L^n. ⌟

Proof: Let N_1 be a maximal normal subgroup of N, then N/N_1 is simple, and let N_i be the conjugates of N_1 in G, then they are all maximal normal subgroup of N. the simple groups N/N_i are mutually isomorphic, and $\cap N_i = 1$ by the minimality of N.

Now we use induction to prove $N/N_1 \cap \ldots \cap N_i$ is isomorphic to a product of N/N_1, which will finish the proof.

Now assume $N_1 \cap \ldots \cap N_{i-1} \not\subseteq N_i$, then $(N_1 \cap \ldots \cap N_{i-1})N_i = N$, and notice

$$N/N_1 \cap \ldots \cap N_i \cong N_1 \cap \ldots \cap N_{i-1}/N_1 \cap \ldots \cap N_i \times N_i/N_1 \cap \ldots \cap N_i \cong N/N_i \times N/N_1 \cap \ldots \cap N_{i-1}.$$

□

Prop. (3.1.8.12). If a finite group $|G| = \prod p_i$, where p_i are different primes that $\prod p_i$ and $\prod(p_i - 1)$ are coprime, then G is cyclic. ⌟

Proof: We prove all the Sylow groups are normal. Choose the maximal Sylow group A_n, then it is normal by Sylow theorem, and other Sylow groups act by conjugation is trivial(consider the center(3.1.6.2), then the center of the quotient, and so on), hence A_n is in the center. Now consider the quotient, by induction it is cyclic, hence this is a central extension of a cyclic group, hence G is Abelian(3.1.7.1), so cyclic. □

Prop. (3.1.8.13). If G is a finite group and p is the minimal prime number of $|G|$, then all subgroups N of G of index p is normal. ⌟

Proof: Consider the left action of G on G/H, then the kernel is $\cap a^{-1}Ha$, which is the maximal normal subgroup contained in H. Now this is group homomorphism of G into S_p, thus it has kernel at lest $|G|/p$, so the kernel equals H, showing H is normal. □

Prop. (3.1.8.14) [Burnside's Theorem]. If p, q are primes, then any finite groups of order $p^a q^b$ is solvable. ⌟

Proof: Cf.[Serre Linear representations of finite groups, P65]. □

Prop. (3.1.8.15) [Thompson]. A finite group is not solvable iff there exist non-trivial elements x, y, z of coprime orders a, b, c that $xy = z$. ⌟

Prop. (3.1.8.16) [Feit-Thompson]. All finite groups that has odd order is solvable. ⌟

Proof: □

9 Commutators

Def. (3.1.9.1) [Notation].
- $[a, b] = a^{-1}b^{-1}ab$.
- $x^y = y^{-1}xy$.

⌟

Prop. (3.1.9.2) [Commutator relations]. . ⌟

Def. (3.1.9.3) [Metabelian Groups]. A **metabelian** group is a group G that G' is Abelian. ⌟

Prop. (3.1.9.4). If $G = AB$ where A, B are Abelian, then $[G, G] = [A, B]$ and G is metabelian. ⌟

Proof: The first one is easy to verify, the second because if we let $b^{a_1} = a_2b_2$, $a^{b_1} = b_3a_3$, then

$$[a, b]^{a_1b_1} = [a, b^{a_1}]^{b_1} = [a, b_2]^{b_1} = [a^{b_1}, b_2] = [a_3, b_2]$$

and similarly, $[a, b]^{b_1a_1} = [a_3, b_2]$, so we have $[a, b]$ commutes with $[b_1^{-1}, a_1^{-1}]$, which shows $[A, B]$ is Abelian. □

Prop. (3.1.9.5). If G is a metabelian finite group, then the transfer of $Ver : G \to G'$ is trivial map. ⌟

10 Transfer

11 Permutation Groups

Lemma (3.1.11.1). If $n \geq 3$, then any proper normal subgroup of A_n has index divisible by 3. ⌟

Proof: Otherwise consider $n = |G/H|$, then every p-power is in H. But then an element c of order 3 is in H, because $c = c^{3k+1} = (c^{-1})^{3k+2}$ for any k. But A_n is generated by 3-Cycles. □

Lemma (3.1.11.2). A_5 is simple. ⌟

Proof: By(3.1.11.1), any proper normal subgroup H has order dividing 20. H cannot contain a 5-cycle, because a 5-cycle has □

Prop. (3.1.11.3). A_n is simple for $n \geq 5$. ⌟

Proof: Cf.[代数学引论 P66]. □

12 Classification of Finite Groups

Thm. (3.1.12.1) [Classification of Finite Simple Groups]. Every finite simple group is one of the following:

- $\mathbb{Z}/(p)$.
- A_n.
- 16 infinite family of finite groups of Lie type.
- 26 exceptional groups, called **sporadic simple groups**.

⌟

Proof: A full list is inhttps://brauer.maths.qmul.ac.uk/Atlas/v3/**?** □

Prop. (3.1.12.2) [Monster Group]. The largest sporadic simple group is called the **Monster group** $\mathbb{M}$.

$$\#\mathbb{M} = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

⌟

Proof: □

Prop. (3.1.12.3) [Happy Family]. There are 20 sporadic groups appearing as a subquotient of $\mathbb{M}$, and they form a set called the **happy family**. The remaining 6 groups are known as the **pariah groups**, including the **Lyons group**, **Janko groups** J_1, J_3, J_4, **Rudvalis group** and the **O'Nan group** $\mathbb{O}\mathbb{N}$. ⌟

Prop. (3.1.12.4) [Baby Monster Group]. The second largest sporadic simple group is called the **baby Monster group** $\mathbb{B}$. ⌟

Def. (3.1.12.5) [O'Nan Group]. ⌟

Prop. (3.1.12.6). The O'Nan group has size

$$\#\mathbb{O}\mathbb{N} = 2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31.$$

⌟

Prop. (3.1.12.7) [Classification of Small Groups].

1. A group G of prime order p or order p^2 is Abelian.
2. A group G of order $p^a q^b$ that it has q^b p-Sylow subgroups, then its q-Sylow subgroup is normal thus it is not simple.
3. A non-Abelian group G of order 6 is isomorphic to S_3.
4. Any non-Abelian group of order 8 is isomorphic to D_4 or quadratic numbers Q.
5. A group of order smaller than 60 is solvable.
6. Any simple group G of order 60 is isomorphic to A_5.
7. A group of order 148 is not simple, by(3.1.6.6) applied to the 37-Sylow subgroup.
8. A group of order 150 is not simple, by(3.1.6.6) applied to the 5-Sylow subgroup.

⌟

Proof:

1. Because G has non-trivial center Z by(3.1.6.2), if $Z = G$, then it is Abelian, otherwise the $|Z| = p$, and the quotient G/Z is cyclic, thus G is Abelian by(3.1.7.1).
2. Calculating elements.
3. Consider its normal 3-Sylow group, then the quotient is cyclic thus G is semi-product which must by S_3 when non-Abelian.
4.
5.
6. Consider G has 6 5-Sylow groups, thus there are 24 elements of order 5.
   G has 4 or 10 3-Sylow subgroups, if it have 4 3-Sylow subgroups, then the normalizer contains a 5-Sylow subgroup, so we have a subgroup of order 15, which must by $\mathbb{Z}/15$, so it contains a normal 5-Sylow subgroup, which shows there are at most $60/15 = 4$ 5-Sylow subgroups, contradiction.
   So we have 10 3-Sylow subgroups, which shows there are at most 15 elements of order 2 or 4. So we have 3 or 5 2-Sylow subgroups. If it is 3, then we can do the same as that for 3-Sylow to construct a 20-order group and reach contradiction.
   So now it have 5 2-Sylow subgroups, and then we consider the conjugate action on Sylow subgroups, which is transitive, so it has trivial kernel, and $G \hookrightarrow S_5$. Now $G = [G, G] \subset [S_5, S_5] = A_5$.

□

Prop. (3.1.12.8). There is a group that is group that $a^3 = 1$ for any $a \in G$, but is not Abelian. It is the uni-upper-triangular matrices in $M_3(\mathbb{F}_3)$. ⌟

13 Profinite Groups

Basic references are [Neukirch Cohomology of Number Fields], [Serre Galois Cohomology] [Profinite Groups Zalesskii] and [Shatz Profinite Groups, Arithmetic and Geometry].

Def. (3.1.13.1) [Profinite Groups]. A **profinite group** is a topological group that is an inverse limit of finite discrete groups. ⌟

Lemma (3.1.13.2). For a compact totally disconnected group G, any nbhd U of e contains a normal open subgroup. ⌟

Proof: U contains a precompact nbhd of e, then by(4.12.1.24), U contains an open subgroup V, so by(4.12.1.6), there is a nbhd V' of e that $xV'x^{-1}\subset V$ for all $x\in G$, this says $\cap x^{-1}Vx$ is open, so it is an open normal subgroup. □

Prop. (3.1.13.3) [Profinite Compact and Totally Disconnected]. A profinite group is the same thing as a totally disconnected, compact Hausdorff topological group. In particular, $G\cong\varprojlim G/U$ where U runs over all open normal subgroups of G. ⌟

Proof: One way is because $\lim G_i$ is a closed subgroup of $\prod G_i$ which by Tychonoff's theorem is compact.

Conversely, by(3.1.13.2), G has a basis of e consisting of normal open subgroups, and by(4.12.1.23), the intersection of open normal subgroups is $\{e\}$. For any open normal subgroup N of G, G/N is compact discrete hence finite, the map $G\to\varprojlim G/N$ is continuous and has dense image, but G is compact and the right is Hausdorff, so the image is closed, hence it is surjective. It is injective because $\cap N=\{e\}$. Hence $G\cong\varprojlim G/N$. □

Cor. (3.1.13.4). A closed subgroup of a profinite group is profinite, and a quotient group is profinite.

A direct product of profinite groups are profinite, and so the inverse limit profinite groups are profinite, as it is a closed subgroup of a direct product. ⌟

Proof: The closed subgroup is totally disconnected by(4.4.1.27).

To show the quotient group is totally disconnected, by(4.12.1.23), it suffice to prove H is intersection of compact open nbhds in G/H. If $x\notin H$, then there is an open subgroup U disjoint from xH by(4.12.1.7), so it is closed hence compact. So UH is a compact nbhd of H in G/H that doesn't contains xH, hence the result. □

Cor. (3.1.13.5). A closed subgroup of a profinite group is a intersection of open normal subgroups of G containing it, as G/H is profinite and as in the proof of(3.1.13.3), H is the intersection of open normal subgroups of G/H. ⌟

Prop. (3.1.13.6). For $G\in\mathcal{P}\mathrm{rof}$, if U_α is the system of open normal subgroups of G, and H is a closed subgroup of G, then there is a natural isomorphism of topological groups

$$H\cong\varprojlim H/H\cap U_\alpha,$$

and if H is normal, then there is a natural isomorphism of topological groups

$$G/H\cong\varprojlim G/HU_\alpha.$$

⌟

Proof: Cf.[Central Simple Algebras]P113.? □

Prop. (3.1.13.7). Any infinite profinite groups is uncountable. ⌟

Proof: [Profinite Groups Zalesskii]Prop2.3.1. □

Prop. (3.1.13.8). The category of profinite Abelian groups is Pontryagin dual to the category of torsion abelian group. (not that hard to verify). ⌟

Proof: □

Pro-p-Groups

Def. (3.1.13.9) [Surnatural Number]. To consider indexes of closed subgroups of a profinite group, the notion of surnatural numbers are needed. A **surnatural number** is a formal product $\prod_p p^{n_p}$, $n_p \in \mathbb{N} \cup \{0, \infty\}$.

For a closed subgroup H of a profinite group G, $[G : H]$ is defined to be the least common multiple of $[G/U : H/H \cap U]$ where U goes over all open normal subgroups of G. This also equals the least common multiple of $[G : V]$ for V open containing H(because for any such V, there is an open normal subgroup U that $HU \subset V$(4.12.1.6)). ⌟

Prop. (3.1.13.10). The index is compatible with composition and quotient: $[G : K] = [G : H][H : K]$ and $[G : H] = [G/K : H/K]$ for K closed normal in G.

$[G : H]$ is finite iff H is open. For a decreasing family of closed subgroups H_i of G, $[G : \cap H_i]$ equals the least common multiple of $[G : H_i]$. ⌟

Proof: $[G/U : K/K \cap U] = [G/U : H/H \cap U][H/H \cap U : K/K \cap U] | [G : H][H : K]$, giving one way of inequality. For the converse, Cf.[Etale Cohomology Fulei P150]. The quotient case is trivial.

If $[G : H]$ is finite, then For the final assertion, notice for a open subgroup V, $G - V$ is compact, so $\cap H_i \subset V$ iff $\cap H_i \subset V$ for some i. □

Def. (3.1.13.11) [Pro-p-Group]. A profinite group G is called a **pro-p-group** iff $[G : 1]$ is a power of p.

Given a profinite group, a closed subgroup H is called **Sylow pro-p-subgroup** of G if H is pro-p and $[G : H]$ is prime to p. ⌟

Proof: □

Prop. (3.1.13.12). A profinite group G is a pro-p-group iff it is an inverse limit of finite p-groups. In particular, any finite quotient of a pro-p-group is a p-group. ⌟

Proof: □

Prop. (3.1.13.13) [Sylow Pro-p-Group Exists]. ⌟

Proof:

□

Prop. (3.1.13.14). Any pro-p subgroup H of G is contained in a Sylow p-subgroup of G, and any two Sylow p-subgroups are conjugate. And a surjective morphism of profinite groups maps a pro-p group to a pro-p group. ⌟

Proof: For any open normal subgroup U of G, let I_U be the sets of all Sylow groups of G/U containing $H/H\cap U$, then the map $G/V\to G/U$ maps I_V to I_U, and I_U is finite nonempty by Sylow theory. So the inverse limit of I_U is nonempty, and let (P_U) be such an element, and $P=\varprojlim_U P_U$, then P is a pro-p subgroup of G, and $[G:P]$ equals the least common multiple of $[G/U:P_U]$, which is prime to p, so it is a Sylow p-group. Similarly, for two Sylow-p subgroup, we consider A_U the set of all $x\in G/U$ that $x^{-1}(PU/U)x=P'U/U$, then there is a inverse element x, and $x^{-1}Px=P'$.

If $G'=G/N$, then $[G/N:PN/N]=[G:PN]|[G:P]$ is prime to p, and $[PN/N:1]=[P:P\cap N]|[P:1]$ is a power of p, so PN/N is Sylow-p in G'. □

Prop. (3.1.13.15). For a pro-p group G, any nonzero simple p-torsion G-module is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ with trivial G-action. ⌟

Proof: The action of G on A factors through a finite quotient group which is a p-group, by(18.1.3.6), $A^G\neq 0$, so $A=A^G$, then A must be $\mathbb{Z}/p\mathbb{Z}$. □

3.2 Abstract Algebra

References are [?], [Rom07] and [Finite Groups Issac].

This section differs from sections on Commutative Algebras because it contains more basic, but maybe non-commutative properties. This section differs from sections on Group Theory because it concerns objects with more structure than a group.

Notation (3.2.0.1).

- Use notations defined in Group Theory.

⌟

1 Rings

Basics

Def. (3.2.1.1) [Rings]. A **ring** is an Abelian group $(R, +)$ together with a multiplication map

$$\times : R \times R \to R$$

s.t.

- $(R, \times)$ is a monoid.
- For any $x, y, z \in R$,
$$x(y+z) = xy + xz, \quad z(x+y) = zx + zy$$

A **commutative ring** is a ring that the multiplication is commutative.

- The category of rings is denoted by $\mathcal{A}\mathrm{lg}$.
- The category of unital rings is denoted by $\mathcal{R}\mathrm{ing}$.
- The category of commutative rings is denoted by $\mathcal{C}\mathcal{A}\mathrm{lg}$.
- The category of commutative unital rings is denoted by $\mathcal{C}\mathcal{R}\mathrm{ing}$.

⌟

Def. (3.2.1.2). $R \in \mathcal{R}\mathrm{ing}$ is called

- a **simple ring** iff it has no non-trivial two-sided ideals.
- a **prime ring** iff for any two ideals $A, B \in \mathcal{R}\mathrm{ing}$, $AB = 0$ implies $A = 0$ or $B = 0$.
- a **domain** or **integral ring** if for any $a, b \in \mathbb{R}$, $ab = 0$ implies $a = 0$ or $b = 0$.
- a **reduced ring** iff it has no non-zero nilpotent element.
- a **Dedekind-finite ring** iff for any $a, b \in R$, $ab = 1 \Rightarrow ba = 1$.

⌟

Def. (3.2.1.3) [Fields]. A **field** is a commutative ring that every non-zero element has an inverse. The category of fields is denoted by `Field`. ⌟

Prop. (3.2.1.4) [Characteristic]. For $R \neq 0 \in \mathcal{R}\mathrm{ing}$, there exists at most one $p \in \mathbf{P}$ s.t. $p \cdot 1 = 0 \in k$. If such a p exists, denote $\operatorname{char} k = p$, otherwise denote $\operatorname{char} k = 0$. ⌟

Prop. (3.2.1.5). If $1-ab$ is left(resp. right) invertible in a unital ring R, then so is $1-ba$, and

$$(1-ba)^{-1} = 1 + b(1-ab)^{-1}a.$$

⌟

Proof: Direct Calculation. □

Prop. (3.2.1.6) [Kaplansky]. If a has a right inverse by no left inverse in a ring, then a has infinitely many right inverses. ⌟

Proof: If $ab=1$, then in fact $b+(1-ba)a^n$ are right inverses for a for any $n\geq 0$, and they are distinct, because if $b+(1-ba)a^n = b+(1-ba)a^m$, then $(1-ba)a^n = (1-ba)a^m$. And by multiplying b on the right, we get $(1-ba)a^{n-m} = 1-ba$, so $((1-ba)a^{n-m-1}+b)a = 1$. □

Division Rings

Def. (3.2.1.7) [Division Rings]. A **skew field**(or **division ring**) is a unital ring that every non-zero element is invertible (but may not be commutative). ⌟

Prop. (3.2.1.8) [Wedderburn]. A finite division ring D is a field. ⌟

Proof: Use the class equation for the invertible elements of D, if it is not isomorphic, consider the center $Z(D)$ of D, let $|Z(D)|=z$, then it is a field, and any other centralizer can be seen as a vector space over $Z(D)$, let it of dimension k, then $z^n-1 = z-1+\sum\frac{z^n-1}{z^{k_i}-1}$. But then let Ψ_n be the cyclotomic polynomial of degree n, then $\Psi_n(z)$ divides $z-1$. But this is not true, as it is bigger. □

Prop. (3.2.1.9). If D is a f.d. division algebra over $\mathbb{R}$, then it is isomorphic to $\mathbb{R},\mathbb{C}$ or $\mathbb{H}$. ⌟

Proof: Cf.[Advanced Linear Algebra P466]. □

Prop. (3.2.1.10). Let $k\in \texttt{Field}, k=\overline{k}$, then any division ring A over k with dimension$<\#k$ is isomorphic to k.

In particular, a division ring A of at most countable dimension over $\mathbb{C}$ is isomorphic to $\mathbb{C}$. ⌟

Proof: Notice it suffices to find an eigenvalue of $\varphi\cdot: A\to A$ for each $\varphi\in A$. But $\{(\varphi-a)^{-1}\}$ is a uncountable set of elements of A, so some $\sum a_i(\varphi-c_i)^{-1}=0$, spanning the expression, we see $\prod_k(\varphi-\mu_k)=0$, so some $\varphi-\mu_k=0$, contradiction. □

Prop. (3.2.1.11) [Hua Equation]. In a division ring D, if $a,b\neq 0$ and $ab\neq 1$, then

$$a-(a^{-1}+(b^{-1}-a)^{-1})^{-1} = aba$$

⌟

Proof: suffices to show

$$1 = (1-ab)a(a^{-1}+(b^{-1}-a)^{-1}) = (1-ab)(1+a(b^{-1}-a)^{-1}).$$

But this is equal to

$$(1-ab)(1-(b^{-1}-a)(b^{-1}-a)^{-1}+b^{-1}(b^{-1}-a)^{-1}) = (1-ab)(1-ab)^{-1} = 1.$$

□

Prop. (3.2.1.12) [Cartan-Brauer-Hua]. Let $K\subset D$ be division rings s.t. $x^{-1}Kx\in K$ for any $x\in D^\times$, then either $K\subset Z(D)$ or $K=D$. ⌟

Proof: Cf.[Lam, P211]. □

Remark (3.2.1.13). For more about division rings, see Finite Semisimple k-Algebras and Brauer-Grothendieck Groups. ⌟

Others

Prop. (3.2.1.14). If $R \in \mathcal{R}\text{ing}$, $\#R = p^2$, then R is commutative. ⌟

Proof: Consider the center of R, it is non-trivial because**?**. □

Prop. (3.2.1.15). Let A, A' be k-algebras and B, B' subalgebras of A, A' with centralizers C, C', then the centralizer of $B \otimes_k B' \subset A \otimes_k A'$ is $C \otimes_k C'$. ⌟

Proof: It suffices to show that $C \otimes_k A' \cap A \otimes_k C' = C \otimes_k C'$, which is clear because they are flat over k. □

2 Gröbner Basis

Cf.[Algebraic Aspects of Cryptography]P70.

3 Commutative Rings

Bézout Domain

Def. (3.2.3.1) [Bézout Domains]. A **Bézout domain** is an integral domain that any sum of two principal domains is also principal. ⌟

Prop. (3.2.3.2). The localization of a Bézout domain is Bézout. A local ring is Bézout iff it is a valuation ring by(11.2.2.8). ⌟

UFDs

Def. (3.2.3.3) [UFDs]. A non-zero element x in a domain R is called **irreducible** iff for any $y, z \in R$ that $x = yz$, either y or z is a unit.

A non-zero element x in a domain R is called a **prime** iff (x) is a prime ideal. Every prime is irreducible.

A domain R is called a **UFD** iff every non-zero element $x \in R$ has a factorization into irreducibles, unique up to units. ⌟

Def. (3.2.3.4) [Relatively Prime Elements]. A set of elements $(x_1, \ldots, x_n)$ in a domain R is called **relatively prime** if there are no irreducible elements that divides each one of them. ⌟

Prop. (3.2.3.5). if R is Noetherian domain, then each element has a decomposition into irreducible. ⌟

Proof: Trace the decomposition inductively, if it doesn't stop, then it contradicts with Noetherian hypothesis. □

Prop. (3.2.3.6). An integral domain R is a UFD iff each element x factors into irreducibles, and every irreducible element is a prime. Also this is equivalent to every non-zero element factors into prime elements. ⌟

Proof: If R is a UFD, then if x is irreducible, if $ab \in (x)$, $ab = xc$, then x is one irreducible in the decomposition of a and b, by UFD, so $a \in (x)$ or $b \in (x)$, and (x) is a prime ideal.

Conversely, if there are two decompositions $\prod a_i = \prod b_j$, then some $b_j \in (a_i)$ by primeness of (a_i), so $b_j = a_i u$, so u must by units, so by induction, this two decompositions are the same.

If every element factors into prime elements, then an irreducible element is a prime because it factors as a product of primes, and notice every prime is irreducible(3.2.3.3). □

Prop. (3.2.3.7) [Kaplansky]. An integral domain R is UFD iff every non-zero prime ideal contains a non-zero principle prime ideal. In particular, any prime of height1 is principal. ⌟

Proof: If R is a UFD, let $\mathfrak{p}$ be a non-zero prime ideal, choose $a \neq 0 \in \mathfrak{p}$, and write $a = \pi_1 \ldots \pi_n$ as a product of irreducibles. Then $\pi_i \in \mathfrak{p}$ for some i, so $\mathfrak{p}$ contains the prime ideal (π_i)(3.2.3.6).

Conversely, let S be the set of all finite products of prime ideals of R, then S is a multiplicative set of R. For any non-zero element $a \in R$, if $(a) \cap S = \varnothing$, then there is a prime ideal P containing (a) and is maximal among those avoiding elements of S. Then P contains a non-zero prime π, contradiction. So $(a) \cap S \neq \varnothing$. Let $b \in R$ that $ab = \pi_1 \ldots \pi_n$, then we show $a \in S$ by induction on n.

If $n = 1$, then a is a unit or a prime, so we are done. For general n, if $\pi_k | b$ for some k, then $b = \pi_k c$, and $ac = \pi_1 \ldots \pi_{k-1}\pi_{k+1} \ldots \pi_n$, then $a \in S$ by induction hypothesis. Otherwise $\pi_k | a$ for all k, thus $a = \pi_1 \ldots \pi_n c$ and $1 = bc$, thus c is a unit and $a \in S$.

Thus we proved that every non-zero element is a product of prime elements, so R is a UFD by(3.2.3.6). □

Prop. (3.2.3.8). A polynomial ring over a UFD is a UFD. ⌟

Proof: □

Prop. (3.2.3.9). Let k be a field, then the ring of power series $k[[X_1, \ldots, X_n]]$ is a UFD. ⌟

Proof: Cf.[Algebra Lang P209]. □

Remark (3.2.3.10). WARNING: if A is a UFD, $A[[X]]$ may not be a UFD. Cf.[Matsumura, Commutative Ring Theory, P165]. ⌟

Prop. (3.2.3.11) [Gauss Lemma]. ⌟

Prop. (3.2.3.12) [Nagata]. If A is a Noetherian domain and $x \in A$ is a prime element s.t. $A[\frac{1}{x}]$ is a UFD, then A is a UFD. ⌟

Proof: $A[\frac{1}{x}]$ is normal by(5.3.5.2), and A is also normal: If $a \in \mathrm{Frac}(A)$ is integral over A, then $a = r/x^m$ for some $m \in \mathbb{Z}, r \in A \backslash (x)$. If $a \notin A$, then $r \in x$, contradiction.

Then we can use(8.1.2.25) to show that $\mathrm{Cl}(\mathrm{Spec}\, A) = 0$, and then A is a UFD by(8.1.5.6). □

Prop. (3.2.3.13). For a field k of characteristic$\neq 2$ and $n \geq m \geq 5$, $A = k[x_1, \ldots, x_n]/(-x_1^2 + x_2^2 + \ldots + x_m^2)$ is a UFD. ⌟

Proof: $A \cong k[x_1, \ldots, x_n]/(x_1x_2 + x_3^2 + \ldots + x_m^2)$, and (x_2) is a prime ideal of A s.t. $A[\frac{1}{x}]$ is a UFD by(3.2.3.8), so A is a UFD by Nagata'e lemma(3.2.3.12). □

Prop. (3.2.3.14)[Quadratic Extension of UFDs]. If $A \in \mathcal{CA}\mathrm{lg}$ is an integral domain and $Z^2 - gZ + f$ doesn't have a root in $\mathrm{Frac}(A)$, then $A[Z]/(Z^2 - gZ - f)$ is integral and normal. ⌟

Proof: If $(a + bZ)(c + dZ) = 0$, then by hypothesis $ad + bc + bdg = 0, ac + fbd = 0$. Then $b(fd^2 - c^2 - cdg) = 0$, so $b = 0$ or $c = d$ by hypothesis. If $(c, d) \neq (0, 0)$, then $ac = ad = 0$, so $a = b = 0$. □

PID

Def. (3.2.3.15) [Euclidean Domain]. ⌟

Prop. (3.2.3.16) [Euclidean Domains are PID]. Euclidean domains(3.2.3.15) are PIDs. ⌟

Proof: □

Example (3.2.3.17).

- $\mathbb{Z}$ is a PID.
- For $k \in \texttt{Field}$, $k[X]$ is a PID.

⌟

Thm. (3.2.3.18) [Chinese Remainder Theorem, S. Tzu300-400]. ⌟

Proof: □

Prop. (3.2.3.19) [PID Structures]. In a PID,

- An element t is irreducible iff (t) is maximal.
- A PID is UFD hence Noetherian.
- An element t is irreducible iff it is a prime.
-

⌟

Proof: 1:
2: By(3.2.3.7).
3: By item2 and(3.2.3.5).
□

4 Modules

Def. (3.2.4.1) [Modules]. For $R \in \text{Mon}$, a (left)R-modules is defined to be **?**. The category of R-modules is denoted by $\mathcal{M}\text{od}_R$.

Left modules are preferred. there are several proposition that is written in favor of right modules, they should be rectified. ⌟

Def. (3.2.4.2) [Finite Modules]. For $R \in \text{Mon}$, a **finite R-module** is an R-module M that there is a surjection $R^n \to M$ for some $n \geq 0$. ⌟

Prop. (3.2.4.3). Let $R \in \mathcal{CR}\text{ing}$ and M be an R-module generated by $n-1$ elements, then any R-module map $R^n \to M$ has a nonzero kernel. ⌟

Proof: Choose a surjection $R^{n-1} \to M$, then the map $R^n \to M$ can be extended to a map $R^n \to R^{n-1}$. It suffices to assume $M = R^{n-1}$. This map is represented by a matrix. If some entry $a_{ij} = a$ is not nilpotent, then we can localize R to R_a that a is a unit. We can assume $a_{11} = a$, and apply elementary row and column transformation to make $A = \text{diag}(1, B)$, then we finish by induction. Now if all a_{ij} are nilpotent, then $I = (a_{ij})$ is nilpotent, and if m is the maximal integer that $I^m \neq 0$, then $(I^m)^{\oplus n}$ is contained in the kernel of this morphism. □

Cor. (3.2.4.4) [Rank of Free Modules]. If M is a free module over a nonzero commutative ring R, then any basis of M is of the same cardinality, called the **rank** of M, and any spanning subset of M has greater cardinalities. In particular, $R^m \neq R^n$ as R-modules. ⌟

Prop. (3.2.4.5) [Fitting Lemma]. For an endomorphism T of a R module M, if we denote p the minimal integer that $R(T^p) = R(T^{p+1})$ and q the minimal integer that $N(T^q) = N(T^{q+1})$. Then the morphisms are stable afterward. Then if there is a m, n that $R(T^m) \oplus N(T^n) = X$ for a R-module endomorphism $T \in \mathrm{End}(M)$, then $p, q < \infty$ and they are equal. Moreover, if we know $p, q < \infty$, then we have $R(T^p) \oplus N(T^q) = M$. ⌟

Proof: We notice that

$$T^i : N(T^{i+j})/N(T^i) \to R(T^i) \cap N(T^j), \quad T^i : M/(R(T^j) + N(T^i)) \to R(T^i)/R(T^{i+j})$$

are isomorphisms. Thus $R(T^m) \oplus N(T^n) = X$ shows $q \leq m$ and $p \leq n$, thus we have $R(T^p) \oplus N(T^q) = M$, which implies $p \geq q$ and $q \geq p$. thus the result. The rest also follows easily from these isomorphisms. □

Prop. (3.2.4.6) [Nakayama]. If M is a finite A-module, and $I \subset A$ is an ideal that $IM = M$, then there is a $a \in 1 + I$ that $aM = 0$.

In particular, if $I \subset \mathrm{rad}(A)$, then a is a unit(5.2.6.2), so $M = 0$. ⌟

Proof: Because $M = IM$, choose a set of generators $\{x_i\}$ of M, then $x_i = \sum a_{ij} x_j$, where $a_{ij} \in I$. Then if the matrix $M = (\delta_{ij} - a_{ij})$, then $Mx_i = 0$. So taking the adjoint matrix, then $\det(M)x_i = 0$. Notice $\det(M)$ is a morphism. But the determinant must be element like $1 + k, k \in I$, so we are done. □

Cor. (3.2.4.7). If M is a finite A-module, N a submodule and $M = \mathrm{rad}(A)M + N$, then $M = N$. ⌟

Cor. (3.2.4.8). If a finite R-module M satisfies $M \otimes_R k(p) = 0$, then there is a $f \notin p$ that $M_f = 0$. ⌟

Proof: Because $M_p = 0$, and the support of M is closed(finiteness used). □

Cor. (3.2.4.9). If an endomorphism φ of a finite module M over R is surjective, then it is injective. ⌟

Proof: This endomorphism makes M a finite module over $R[X]$ by letting X acts by φ. So the hypothesis shows $IM = M$ where $I = (x) \subset R[x]$. Then Nakayama(3.2.4.6) shows there are some $(1 + f(X)X)M = 0$. Thus for any $m \in M$ that $X(m) = 0$, $m = 0$, so φ is injective. □

Prop. (3.2.4.10). If $A \in \mathfrak{Ring}/\mathbb{C}$ and $\alpha \in A$ is not nilpotent, then there exists a simple A-module M that $a|_M \neq 0$. ⌟

Proof: First we claim that there is some $\lambda \neq 0 \in \mathbb{C}$ that $a - \lambda$ is not invertible in A, this is nearly the same as the proof of(3.2.1.10), noticing that a is not nilpotent. Now we can take $M = A/(a-\lambda)A$, then $a1 = \lambda \neq 0$. □

Prop. (3.2.4.11) [Jordan-Horder]. Cf.(3.1.8.10). ⌟

Tensor Module and Hom Module

Def. (3.2.4.12) [Hom Module]. If B is an R-S-bimodule and C is a T-S-bimodule, then $\mathrm{Hom}_S(B,C)$ is naturally a $T-R$-module given by the action $(tfr)(b) = tf(rb)$.

Dually, if B is an $S-R$-bimodule and C is a $S-T$-bimodule, then $\mathrm{Hom}_S(B,C)$ is naturally an $R-T$-bimodule given by the action $(rft)(b) = f(br)t$. ⌟

Def. (3.2.4.13) [Tensor Product]. Given a ring R, a T-R-bimodule A and an R-S-bimodule B, their **tensor product** is a T-S-bimodule defined by universal properties: $A \times B \to A \otimes_R B$ is a T-S-bimodule map, and any T-S-bimodule map $A \times B \to C$ to a T-S-bimodule C factors uniquely through $A \otimes_R B \to C$.

The tensor product can be constructed as:

There is an adjoint:

$$- \otimes_R B : {}_T\mathcal{M}\mathrm{od}_R \leftrightarrows {}_T\mathcal{M}\mathrm{od}_S : \mathrm{Hom}_S(B,-) \ .$$

In particular, tensoring commutes with colimits.

Similarly, there is an adjoint:

$$A \otimes_R - : {}_R\mathcal{M}\mathrm{od}_S \leftrightarrows {}_T\mathcal{M}\mathrm{od}_R : \mathrm{Hom}_T(A,-) \ .$$

⌟

Proof: We need to give an isomorphism

$$\tau : \mathrm{Hom}_S(A \otimes_R B, C) \cong \mathrm{Hom}_R(A, \mathrm{Hom}_S(B,C)).$$

Given $f \in \mathrm{Hom}_S(A \otimes_R B, C)$, we define

$$\tau(f) : A \to \mathrm{Hom}_S(B,C) : (\tau(f)a)(b) = f(a \otimes b).$$

and conversely, for $g \in \mathrm{Hom}_R(A, \mathrm{Hom}_S(B,C))$,

$$\tau^{-1}(g)(a \otimes b) = (g(a))(b).$$

The verifications is routine and the isomorphism for left modules is dual. □

Prop. (3.2.4.14) [(Co)Induced Modules]. Given a ring homomorphism $S \to R$, then R is a $S-R$-bimodule as well as a R-S-bimodule, then we define:

- $f^* : {}_R\mathcal{M}\mathrm{od} \to {}_S\mathcal{M}\mathrm{od} : f^*M = {}_SM = \mathrm{Hom}_R(R,M) = R \otimes_R M$(3.2.4.12)(3.2.4.13), the **restriction**.
- $f_! : {}_S\mathcal{M}\mathrm{od} \to {}_R\mathcal{M}\mathrm{od} : f_!M = R \otimes_S M$ is the **induced module**, it is left adjoint to restriction, by(3.2.4.13).
- $f_* : {}_S\mathcal{M}\mathrm{od} \to {}_R\mathcal{M}\mathrm{od} : f_*M = \mathrm{Hom}_S(R,M)$ is the **coinduced module**, it is right adjoint to restriction, by(3.2.4.13).

Dually for left modules, we define:

- $f^* : \mathcal{M}\mathrm{od}_R \to \mathcal{M}\mathrm{od}_S : f^*M = M_S = \mathrm{Hom}_R(R,M) = M \otimes_R R$(3.2.4.12)(3.2.4.13), the **restriction**.

- $f_!: \mathcal{M}\mathrm{od}_S \to \mathcal{M}\mathrm{od}_R : f_! M = M \otimes_S R$ is the **induced module**, it is left adjoint to restriction, by(3.2.4.13).
- $f_*: \mathcal{M}\mathrm{od}_S \to \mathcal{M}\mathrm{od}_R : f_* M = \mathrm{Hom}_S(R, M)$ is the **coinduced module**, it is right adjoint to restriction, by(3.2.4.13).

⌟

Def. (3.2.4.15) [Algebras]. For $R \in \mathcal{CR}\mathrm{ing}$, a(n) (commutative/unital/associative)**algebra** over R is a (commutative/unital/associative)magma object in the monoidal category $(\mathcal{M}\mathrm{od}_R, \otimes)$.

The category of R-algebras is denoted by $\mathcal{A}\mathrm{lg}_R$. The category of commutative R-algebras is denoted by $\mathcal{CA}\mathrm{lg}_R$, the category of commutative unital associative algebra over R is denoted by $\mathcal{CR}\mathrm{ing}_R$. Notice $\mathcal{CR}\mathrm{ing}_R \cong \mathcal{CR}\mathrm{ing}/R$. ⌟

Torsion-Free Modules

Def. (3.2.4.16) [Torsion-Free Modules]. Let R be a ring, an R-module M is called **torsion-free** iff there are no non-zero divisor $x \in R, 0 \neq f \in M$ that $xf = 0$. ⌟

Prop. (3.2.4.17). If $0 \to M_1 \to M_2 \to M_3$ and M_1, M_3 are torsion-free, then M_2 is torsion-free. Torsion-free is a stalk-wise property(5.1.4.2). ⌟

Proof: Trivial. □

Prop. (3.2.4.18). Let M be a finite R-module, then M is torsion-free if it is a submodule of a finite free module. ⌟

Proof: One direction is trivial, for the other, if M is torsion-free, then $M \subset M \otimes_R K$, and $M \otimes_R K$ is a finite K-vector space, with basis e_i. Now let x_i be a basis of M, let $x_i = \sum a_{ij}/b_{ij} e_j$, then let $e = \prod_{ij} b_{ij}$, then $M \subset Re_1/b \oplus \ldots \oplus Re_n/b$. □

Prop. (3.2.4.19). If M, N are R-modules that M is torsion-free, then $\mathrm{Hom}(N, M)$ is torsion free. ⌟

Proof: Choose a surjection $\bigoplus_I R \to N \to 0$, then $\mathrm{Hom}(N, M) \hookrightarrow \prod_I M$ is torsion free. □

Modules over PIDs or Bézout Domains

Prop. (3.2.4.20) [Modules over a Bézout domain]. Let R be a Bézout domain, then

- any finite submodule of a free module over is finite free.
- any f.p. R-module M is a summand of a free R-module and M_{tor}, where $M_{\mathrm{tor}} = \oplus R/(f_i)$ where $f_i \in R^*$.

⌟

Proof: Cf.[Sta]0ASU.**?** □

Prop. (3.2.4.21) [Classification of Modules over PID].

1. Every submodule of a free module over a PID is free of smaller rank. Thus a projective module over a PID is free
2. Every finite torsion-free module over a PID is free.
3. Every finite module over a PID has a primary decomposition $M = \bigoplus_i R/(q_i)$,where (q_i) is primary ideals.

So projective $\iff$ free $\iff$ torsion-free(when f.g.). ⌟

Proof: 1: Choose a well ordering on the basis of F, let F_i is the submodule generated by $e_j, j \le i$. Then $\mathrm{pr}_i(P \cap F_i) \subset R$ is an ideal of the form (a_i), thus choose $u_i \in P$ that $\mathrm{pr}_i(u_i) = a_i$. Then u_i is a basis for P: they are linearly independent, because for any finite linear combination that are 0, the maximal coordinate are 0. It also spans P, because we can choose an element in $P - \{u_i\}$ whose maximal nonzero coordinate α is minimal among them, by well-orderedness. But we can subtract a multiple of u_α, thus producing a smaller element, contradiction.

2: If it is finite torsion-free, then it is a submodule of a finite free module(3.2.4.18), so it is free by item1.

3: Follows immediately from(5.2.5.34) and(3.2.3.19). □

Prop. (3.2.4.22) [Primary Cyclic Decomposition]. There is a primary cyclic decomposition theorem for a torsion module M over a PID R. Thus the multisets of elementary divisors of M is a complete set of invariants for M. ⌟

Proof: Cf.[Advanced Linear Algebra P153]. □

Cor. (3.2.4.23) [Invariant Factor Decomposition]. By reordering the cyclic decomposition, we can get the **invariant factor decomposition** of M, there are scalars $d_m|d_{m-1}|\ldots|d_1$ that are called the **invariant factors** of M. ⌟

Proof: Cf.[Advanced Linear Algebra P157]. □

Cor. (3.2.4.24) [Elementary Factor Theorem]. Let F be a free module over a PID R, and let M be a f.g. submodule$\neq 0$, then there exists a basis $\mathcal{B}$ of F, elements $e_1, \ldots, e_m$ in this basis, and non-zero elements $a_1, \ldots, a_m \in R$ that

- the elements $a_1e_1, \ldots, a_me_m$ forms a basis of M.
- $a_i|a_{i+1}$.

And these a_i are uniquely determined up to units. ⌟

Transfinite Direct Sum Dévissage of Modules

Def. (3.2.4.25) [Direct Sum Dévissage of Modules]. Let M be a module over a ring R, then a **direct sum dévissage** is a family of submodules M_α indexed by an ordinal S such that

- $M_0 = 0$.
- if $\alpha + 1 \in S$, then M_α is a direct sum of $M_{\alpha+1}$.
- if α is a limit ordinal, then $M_\alpha = \cup_{\beta<\alpha} M_\beta$.
- $\cup_{\alpha \in S} M_\alpha = M$.

If moreover, for any $\alpha \in S, \alpha + 1 \in S$, $M_{\alpha+1}/M_\alpha$ is countably generated , then M_α is called a **Kaplansky dévissage** of M. ⌟

Prop. (3.2.4.26). Let M_α be a direct sum dévissage of M, then $M \cong \bigoplus_{\alpha\in S, \alpha+1\in S} M_{\alpha+1}/M_\alpha$. ⌟

Proof: Cf. [Sta]058V. □

Cor. (3.2.4.27). M is a direct sum of countably generated modules iff M admits a Kaplansky dévissage. ⌟

Prop. (3.2.4.28). Suppose M is a direct sum of countably generated modules and P is a direct sum of M, then P is also a direct sum of countably generated modules. ⌟

Proof: Cf.[Sta]058X. □

Prop. (3.2.4.29)[Direct Summand Criterion of Free Modules]. Let M be a countably generated R-module that for any direct summand N of M and an element $x \in N$, x is contained in a free direct summand of N, then M is free. ⌟

Proof: Let $x_1, x_2, \ldots$ be a countable set of generators for M, then we can use inductions to find free submodules $F_1, F_2, \ldots$ of M s.t. $\oplus_{i=1}^n F_i$ are direct summands of M and contains $x_1, \ldots, x_n$ for any n, thus $M = \oplus F_i$ is free. □

5 Fields

Finite Fields

6 Field Extensions

Prop. (3.2.6.1)[Artin]. If G is a monoid and K is a field, any distinct characters of G in K are linearly independent over K. ⌟

Proof: Consider the minimal length of linear combination that is 0, then we multiply a suitable z in it, then we can can cancel a character, contradicting the minimality. □

Cor. (3.2.6.2). If α_i are different elements in K and there are element a_i that $\sum a_i \alpha_i^v = 0$ for every $v \geq 0$, then $a_i = 0$ for all n. (Seen as characters from $\mathbb{Z}_{\geq 0} \to K$). ⌟

Def. (3.2.6.3) [Composition of Fields Extensions]. ⌟

Field Extensions

Def. (3.2.6.4) [Distinguished Class of Extensions]. A family $\mathscr{L}$ of extensions are called a **distinguished class** iff

- It is closed under base change.
- $E/F/K \in \mathscr{L}$ iff $F/K \in \mathscr{L}$ and $E/F \in \mathscr{L}$.

⌟

Def. (3.2.6.5) [Algebraic Extensions]. An **algebraic extension** is a field extension L/K s.t. for any element $\alpha \in L$, there exists a nonzero polynomial $f(X) \in K[X]$ s.t. $f(\alpha) = 0$. ⌟

Prop. (3.2.6.6). The family of finite extensions form a distinguished class.
The family of algebraic extensions form a distinguished class.
The family of f.g. extensions form a distinguished class. ⌟

Proof: Finite case is trivial. For the alg. extensions, for $k \subset F \subset E$, for any $\alpha \in E$, α satisfies an polynomial function with f.m coefficients in F, the coefficients form a subfield F_0 of F which is finite over k, so $k \subset F_0 \subset F_0(\alpha)$ is a finite tower, so it is finite, hence algebraic. The base change is easy to check.

For f.g. extensions, it suffice to check composition:**?** □

Prop. (3.2.6.7). For an alg.extension $k \subset E$, any injective field map $E \to E$ over k is an automorphism. (This is because it induce a permutation of any α with its conjugates in E, so it is surjective). ⌟

Lemma (3.2.6.8). Let $f \in k[X]$ be a polynomial of degree≥ 1, then there is a field K that f has a root in K. Hence for any finite set of polynomials, there is a field K that all of them have roots in K. ⌟

Proof: Cf.[Algebra Lang P231]. □

Lemma (3.2.6.9). For any $k \in \mathtt{Field}$, there exists $K \in \mathtt{Field}$ s.t. $k \subset K, \overline{K} = K$. ⌟

Proof: Firstly, we construct a field that every polynomial in $k[X]$ of degree≥ 1 has a root. Consider the polynomial ring $k[X_f]$, where there is a indeterminant X_f for each $f \in k[X]$ of deg≥ 1. Then the ideal generated by $f(X_f)$ is not a unit ideal, which can be seen by constructing a finite field extension that f_i all have a root in it(3.2.6.8).

So if $\mathfrak{m}$ is a maximal ideal containing all $f(X_f)$, then the quotient field is a field that all f have a root(X_f).

So now if we construct inductively like this, and consider their union, then it is clearly a field and any polynomial of degree≥ 1 have a root in it. □

Prop. (3.2.6.10) [Algebraic Closure]. Assume the axiom of choice, for any $K \in \mathtt{Field}$, there exists uniquely an algebraic field extension K/k s.t. K is alg.closed, up to isomorphism over k. Any such field K is called an **algebraic closure** of k, denoted by $\overline{k}$. ⌟

Proof: Let E be a field that is alg.closed and contains k by(3.2.6.9). Let k^a be the union of subextensions that are algebraic over k. k^a is a field, by(3.2.6.6), and k^a is alg.closed, because if $f(X)$ is a polynomial of degree≥ 1 in $k^a[X]$, then it has a root $\alpha \in E$, and α is algebraic over k^a, so $\alpha \in k^a$. □

Prop. (3.2.6.11) [Finite Algebraic Extensions]. Let L/K be a field extension and F/L be a finite extension, then there is a finite extension F'/K s.t. $F = LF'$. ⌟

Proof: Take a generator x_i of F/L, then x_i are algebraic over L, thus there are polynomials $f_i \in L[X]$ s.t. $f_i(x_i) = 0$. Let F' be the fields over K generated by all the coefficients of f_is, then $F = LF'$. □

Prop. (3.2.6.12). If E/F is an algebraic field extension, then for any R that $E \subset R \subset F$, R is a field. ⌟

Proof: If $\alpha \in R$, then α is algebraic over E, so there is a relation $\alpha^n + \ldots + a_0 = 0$, so $\alpha^{-1} = -a_0^{-1}(a_1 + \ldots \alpha^{n-1}) \in R$. □

Normal & Separable Extensions

Def. (3.2.6.13) [Normal Extensions]. A field extension K/k in $\overline{k}$ is called **normal extension** iff it satisfied the following equivalent conditions:

- Any embedding of K into $\overline{k}$ induce an automorphism on K.
- K is the splitting field of a family of polynomials in $k[X]$.
- Every irreducible polynomial in $k[X]$ that has a root in K splits in K.

⌟

Proof: Cf.[Algebra Lang P237]. □

Prop. (3.2.6.14). Normal extension are stable under base change and composition, by the first definition of(3.2.6.13). ⌟

Def. (3.2.6.15) [Normal Closure]. For any field extension F/K, there is a field extension E/F that E/K is normal, called the **normal closure** of F/K. It is the composite of conjugates of F/K. ⌟

Def. (3.2.6.16) [Separable Degree]. Define the **separable degree** $[E:k]_s$ of an extension E/k as the cardinality of embedding of E into $\overline{k}$. Separable degree commutes with composition, and when E/k is finite, $[E:k]_s \leq [E:k]$. ⌟

Def. (3.2.6.17) [Separable Polynomials]. A finite extension is called a **separable extension** iff $[E:k]_s = [E:k]$, an algebraic number α over k is called **separable over** K iff $k(\alpha)/k$ is separable. A polynomial $f \in k[X]$ is called a **separable polynomial** iff it has no multiple roots in $\overline{k}$. ⌟

Def. (3.2.6.18) [Separable Extensions]. An algebraic extension E/k is called a **separable extension** iff it satisfies the following equivalent conditions:

- every f.g. subfield is separable over k,(this is compatible because subfield of a finite separable extension is separable, by the compatibility of separable degree).
- Every element of E is separable.
- It is generated by a family of separable elements.

⌟

Proof: If E/k is separable and $k \subset k(\alpha) \subset E$, then by(3.2.6.17), $k(\alpha)$ is separable. And if it is generated by a family of separable elements $\{\alpha_i\}$, then any f.g. subfield can are f.g. by elements $\{\alpha_i\}$. Now it is a tower of separable extensions, hence separable by the compatibility of separable degree. □

Prop. (3.2.6.19). Separable extensions form a distinguished class. ⌟

Proof: Cf.[Algebra Lang P241]. □

Prop. (3.2.6.20) [Primitive element Theorem]. A finite extension E/k is primitive iff there are only f.m. middle fields. And if E/k is separable, this is satisfied. ⌟

Proof: If k is finite, this is simple. Assume k infinite, for any two elements α, β, consider $k(\alpha + c_i\beta)$, if there is only finitely many middle fields, there exists two that is equal, so $k(\alpha, \beta) = k(\gamma)$. Proceeding inductively, E is primitive.

Conversely, if $k(\alpha) = E$, every middle field corresponds to a divisor of the irreducible polynomial of α. This map is injective, because for any g_F, degree of α over F is the same over the degree over the coefficient field of g_F, so it must be equal to F.

If E/k is separable, Let

$$P(X) = \prod_{i \neq j} (\sigma_i\alpha + X\sigma_i\beta - \sigma_j\alpha - X\sigma_j\beta)$$

for different embedding σ_i, σ_j of $E(\alpha, \beta)$ into $\overline{k}$. Then it is not identically zero, thus there exists c that $\sigma_i(\alpha + c\beta)$ is all distinct, thus generate $K(\alpha, \beta)$. □

Inseparable Extensions

Prop. (3.2.6.21). Any irreducible polynomial of fields of characteristic 0 is separable and if char= p, then all roots have the same multiplicity and thus $[k(\alpha):k]=p^n[k(\alpha):k]$ for some n. ⌟

Proof: All roots have the same multiplicity because there are Galois actions. If the multiplicity is not 1, the derivative f' is zero, otherwise f is not irreducible. Then $f(X)=g(X^p)$. We can choose $f(X)=h(X^{p^n})$ with h separable, then $[k(\alpha):k(\alpha^{p^n})]=p^n$, thus the result. □

Def. (3.2.6.22). The **inseparable degree** $[E:k]_i$ is defined as the quotient $[E:k]/[E:k]_s$. An algebraic element α is called **purely inseparable** over k iff there is a n that $\alpha^{p^n}\in k$. ⌟

Def. (3.2.6.23) [Purely Inseparable Extensions]. An extension is called **purely inseparable** if it satisfies the following equivalent conditions:

- $[E:k]_s=1$.
- Every element α of E is purely inseparable over k.
- For every $\alpha\in E$, the irreducible equation of α over k is of type $X^{p^n}-a$.
- It is generated by a family of purely inseparable elements.

⌟

Proof: Cf.[Algebra Lang P249]. □

Cor. (3.2.6.24). A field over $\mathbb{F}_p$ is perfect iff there are no purely inseparable extensions of it. ⌟

Cor. (3.2.6.25) [Perfect Closure]. For any field k of char p, there is a unique purely inseparable field extension k^{perf}/k that k^{perf} is perfect, called the **perfect closure** of k. It is generated by adding all the p^n-th roots to k. ⌟

Prop. (3.2.6.26). Purely inseparably extensions form a distinguished class. ⌟

Proof: Cf.[Algebra Lang P250]. □

Prop. (3.2.6.27). If E/k is algebraic and E_0 be the maximal separable extension contained in E, then E/E_0 is purely inseparable. And if E/k is normal, then E_0/k is normal, too. ⌟

Proof: By the proof of(3.2.6.21), any α has a p^n that α^{p^n} that α^{p^n} is separable, hence it is purely inseparable over E_0 by(3.2.6.23). E_0/k is normal because any σ maps E to itself, and E_0 to $\sigma(E_0)\in E$ separable, hence $\sigma(E_0)\subset E_0$. □

Trace and Norm

Prop. (3.2.6.28) [Trace and Norm]. Let L/K be a finite field extension and Σ be the set of embeddings $\sigma:L\to\overline{K}$, then define the **trace map** $\mathrm{tr}_{L/K}:L\to K:x\mapsto[L:K]_i\sum_{\sigma\in\Sigma}\sigma(x)$ and the **norm map** $N_{L/K}:L\to K:x\mapsto(\prod_{\sigma\in\Sigma}\sigma(x))^{[L:K]_i}$. ⌟

Prop. (3.2.6.29). Let L/K be a field extension,

- The norm induces a multiplicative homomorphism $L^\times\to K^\times$, and the trace induces an additive homomorphism $L\to K$.
- If $E/F/K$ are field extensions, then $N_{E/K}=N_{F/K}\circ N_{E/F}$, and $\mathrm{tr}_{E/K}=\mathrm{tr}_{F/K}\circ\mathrm{tr}_{E/F}$.

- If $L=K(\alpha)$ and $F=\mathrm{Irr}(\alpha,k;X)=X^n-a_{n-1}X^{n-1}+\ldots+(-1)^n a_0$, then

$$N_{L/K}(\alpha)=a_0,\quad \mathrm{tr}_{L/K}(\alpha)=a_{n-1}.$$

⌟

Proof: Cf.[?]P285. □

Prop. (3.2.6.30)[Calculating Dual Basis]. Let $L=K(\alpha)$ be a finite separable extension, let $f(X)=\mathrm{Irr}(\alpha,K;X)$, and

$$\frac{f(X)}{(X-\alpha)}=\beta_0+\beta_1X+\ldots+\beta_{n-1}X^{n-1},$$

then the dual basis of $(1,\alpha,\ldots,\alpha^{n-1})$ w.r.t. the trace form(3.2.6.32) is

$$\frac{\beta_0}{f'(\alpha)},\ldots,\frac{\beta_{n-1}}{f'(\alpha)}.$$

⌟

Proof: Denote the roots of f be α_i, then they are pairwise different, and

$$\sum_i\frac{f(X)}{X-\alpha_i}\frac{\alpha_i^r}{f'(\alpha_i)}=X^r$$

for all r by Lagrange interpolation(3.3.1.2). But this is equivalent to

$$\mathrm{tr}(\frac{\alpha^r\beta_j}{f'(\alpha)})=\delta_{ij}$$

□

Prop. (3.2.6.31). Let L/K be a field extension, then $x\in L$ acts on L via multiplication T_x. Then

$$\det(T_x)=N_{L/K}(x),\quad \mathrm{tr}(T_x)=\mathrm{tr}_{L/K}(x).$$

⌟

Proof: Let $F=K(x)\subset L$, and $p(X)$ be the minimal monic polynomial of x, then $\mathrm{char}(T_x|;X)=\mathrm{char}(T_x|_K;X)^{[L:K(x)]}$, thus we are done by(3.2.6.29). □

Prop. (3.2.6.32)[Trace Form]. For $L\subset_{\mathrm{fin}}K\in\texttt{Field}$, consider the pairing

$$\mathrm{Tr}_{L/K}:L\times L\to K:(x,y)\mapsto\mathrm{tr}(xy),$$

called the **trace form**. Then the following are equivalent:

1. L/K is separable.
2. $\mathrm{tr}_{L/K}\neq 0$.
3. $\mathrm{Tr}_{L/K}$ is non-degenerate.

⌟

Proof: $2, 3$ are equivalent by a minute's thought. For $1 \iff 2$:

If L/K is inseparable, then by(3.2.6.29), if we consider $L/K'/K$ that L/K' is purely inseparable of degree p, then it is generated by some equation $x^p - a$, and the root is α. Then $L = K'(\alpha)$ and the minimal polynomial of $\alpha^i, 0 \le i \le p-1$ is $x^p - a^i$, so $\mathrm{tr}(\alpha^i) = 0$, and $\mathrm{tr}_{L/K} = 0$.

If L/K is separable, $\mathrm{tr}_{L/K} \neq 0$ by the linear independence of characters(3.2.8.3). □

Def. (3.2.6.33) [Discriminant of a Basis]. Let α_i be a basis of a separable extension L/K, then the **discriminant of the basis** $d(\alpha_1, \ldots, \alpha_n)$ is defined to be $(\det(\sigma_i(\alpha_j))_{i,j})^2$. Clearly, $d(\alpha_1, \ldots, \alpha_n)$ is invariant under the Galois action of L/K, thus it is an element of K. ⌟

Prop. (3.2.6.34). Notice $\mathrm{tr}_{L/K}(\alpha_i\alpha_j) = \sum_k \sigma_k(\alpha_i)\sigma_i(\alpha_j)$, thus $(\mathrm{tr}_{L/K}(\alpha_i\alpha_j))$ is the product of the matrices $(\sigma_k\alpha_i)^t$ and $(\sigma_k\alpha_j)$, thus

$$d(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{tr}_{L/K}(\alpha_i\alpha_j)).$$

So the discriminant of $\{\alpha_1, \ldots, \alpha_n\}$ is the Gram matrix of the trace norm w.r.t. this basis(3.5.10.15). In particular, by(3.2.6.32),

$$d(\alpha_1, \ldots, \alpha_n) \neq 0.$$

⌟

Prop. (3.2.6.35). If $L = K(\theta)$ is a separable field extension of degree d, and $\theta_1 = \theta, \ldots, \theta_n$ are the conjugates of θ, then

$$d(1, \theta, \ldots, \theta^{d-1}) = (\det \mathrm{Van}(\theta_1, \ldots, \theta_d))^2 = \prod_{i<j}(\theta_i - \theta_j)^2.$$

⌟

7 Transcendental Extensions

Def. (3.2.7.1) [Transcendental Basis]. Let K be an extension of a field k, a **transcendental base** is an algebraically independent set that any element is algebraic over it.

Given any algebraically independent set $S \subset T$ a set over which K is algebraic, S can be extended to a transcendental base contained in T, by Zorn's lemma. In particular, a transcendental basis exists. ⌟

Prop. (3.2.7.2). Any two transcendental basis have the same cardinality, called the **transcendental degree** of K/k, denoted by $\mathrm{tr}\deg_k(K)$. ⌟

Proof: If K/k has a finite transcendental basis, then let $X = \{x_1, \ldots, x_m\}$ transcendental base of minimal number, $S = \{w_1, \ldots, w_n\}$ an algebraically independent set. If $n > m$, we proceed by changing one element in X a time using induction and prove that K is algebraic over $\{w_1, \ldots, w_r, x_{r+1}, \ldots, x_m\}$, contradiction.

Because w_{r+1} is algebraic over $\{w_1, \ldots, w_r, x_{r+1}, \ldots, x_n\}$, we have a minimal polynomial

$$f = \sum g_j(w_{r+1}, w_1, \ldots, w_r, x_{r+2}, \ldots, x_m)x_{r+1}^j$$

s.t. $f(w_{r+1}, w_1, \ldots, x_m) = 0$ (after possibly renumbering x_i, this x must exists because S is itself algebraically independent). So x_r is algebraic over $\{w_1, \ldots, w_{r+1}, x_{r+2}, \ldots, x_m\}$, hence K is independent over it, too.

If K/k has an infinite basis B, let B' be another basis, then for any $\alpha \in B^*$, there is a finite set $B_\alpha \subset B$ that α is algebraic over $k(B_\alpha)$, because algebraic equation involves f.m. generators. Then we define $B^* = \cup_{\alpha \in B'}$, then it has cardinality smaller than B'. But $B^* = B$, because for any $\beta \in B$, β is algebraic over B' which is algebraic over $k(B^*)$, thus β is algebraic over $k(B^*)$, thus $\beta \in B^*$. □

Prop. (3.2.7.3). If K is of finite transcendental degree over k, then $\#K = \#k$. ⌟

Proof: We find a purely transcendental L/k that K/L is algebraic, then the element of L are all polynomials of finite indeterminants of elements of k, so $|L| = |k|$ by(2.2.8.4), and similarly $|K| = |L|$. □

Prop. (3.2.7.4). For $k \in \texttt{Field}$, any two alg.closed field extension $K_1/k, K_2/k$ of the same transcendental degree over k are isomorphic. ⌟

Proof: We define a bijection of the transcendental basis, and then extend it to an isomorphism of fields, by(3.2.6.10). □

Cor. (3.2.7.5). Any two alg.closed field of the same characteristic and cardinality are isomorphic. ⌟

Proof: It suffices to show that their transcendental basis over the base field are of the same cardinality**?** □

Prop. (3.2.7.6) [Lüroth]. The automorphism group of $K(T)$ is $PGL(2;K)$. ⌟

Proof: Consider $\theta = \sigma(x) = \frac{f(x)}{g(x)}$, then x is algebraic over $K(\theta) : \theta g(x) - f(x) = 0$. Now x is transcendental over K, thus θ is transcendental over K as well. Now the minimal polynomial of x over $K(\theta)$ is just $\theta g(x) - f(x)$, because it is irreducible, as it is linear over θ. But $K(x) = K(\theta)$, thus the polynomial must have degree 1, so $f(x), g(x)$ is of degree 1. Now the rest is clear. □

Prop. (3.2.7.7) [Lüroth]. Any subfield $K \subsetneq L \subset K(T)$ is of the form $K(u)$ where $u \in K(X)$ is transcendental over K. ⌟

Proof: It is clearly transcendental over K, so this follows from(6.12.1.17) and Riemann-Hurewitz(6.12.1.32), notice that the field extension is separable by(5.3.9.4): The non-singular complete curve corresponding to L has genus0, and it has a rational point, so isomorphic to $\mathbb{P}^1_k$(6.12.8.2). □

8 Galois Theory

Def. (3.2.8.1) [Galois Extension]. A **Galois field extension** is a field extension that is both normal and separable. ⌟

Def. (3.2.8.2) [Galois Closures]. Let F/K be a separable extension, then the normal closure E/K is also separable, called the **Galois closure** of F/K.

In particular, the maximal separable extension k^{sep}/k, called the **separable closure** of k, is Galois over k, and $\text{Gal}(k^{\text{sep}}/k)$ is denoted by Gal_k. ⌟

Prop. (3.2.8.3) [Linear Independence of characters, Artin]. Let L be a field, G be a monoid and $\chi_i : G \to L$ be multiplicative maps, then χ_i are linearly independent over L. ⌟

Proof: Let $\sum_{i=1}^n a_i\chi_i = 0$ and $a_i \neq 0$ for any i, we use induction to derive contradictions: for all i. $n = 1$ is trivial, and for general n, assume $a_1, a_2 \neq 0$, then the two equations $\chi_1(h) \neq \chi_2(h)$, then $\sum_{i=1}^n a_i\chi_i(hg) = 0$ and $\sum_{i=1}^n a_i\chi_i(g) = 0$ gives us a equation with smaller n, thus we are done. □

Prop. (3.2.8.4) [Algebraic Independence of Automorphisms, Artin]. Let $K \in \texttt{Field}, \#K = \infty$, and $G = \{\sigma_1, \dots, \sigma_n\}$ be a finite subgroup of automorphisms of K, then $\{\sigma_i\}$ are algebraically independent over K. ⌟

Proof: Cf.[Lang, P311].**?** □

Prop. (3.2.8.5) [Galois Main Theorem, Artin]. Let G be a finite group of automorphisms of K. Then K/K^G is Galois of Galois group G. ⌟

Proof: For every element x, set $\{\sigma_1 x, \dots, \sigma_r x\}$ be distinct conjugates, then $f(X) = \prod_i^r = (X - \sigma_i x)$ shows that K is separable and normal over K^G. And primitive element theorem shows that $[K : K^G] \leq |G|$, so it must equals G. □

Prop. (3.2.8.6). If L/K is a finite Galois extension, then there is an isomorphism:

$$L \otimes_K L \cong L \times L \times \ldots \times L : (a, b) \mapsto (ab, a\sigma_1(b), \dots, a\sigma_{n-1}(b))$$

where σ_i are Galois elements. ⌟

Proof: Choose a primitive element x and its minimal polynomial $f(x)$, then $L \cong K[X]/(f)$, and $L \otimes_K L \cong L[X]/(f)$, but f decomposes completely in $L[X]$, thus by Chinese remainder theorem(3.2.3.18), the given map is an isomorphism of rings. □

Prop. (3.2.8.7) [Infinite Galois Theorem]. The middle fields correspond to the closed subgp of $G(L/K)$. ⌟

Proof: The highlight is that $G(L/L^H) = H$ for a closed subgp H of $G(L/K)$. If σ fixes L^H but is not in H, because for every finite field M, $H \cdot G(L/M)$ corresponds to $M/(M \cap L^H)$, so $\sigma G(L/M) \cap H \neq \varnothing$. So σ is in the closure of H thus in H. □

Prop. (3.2.8.8) [Normal Basis Theorem]. For a finite Galois extension L/K, normal basis exists. ⌟

Proof: Finite case: The Galois group is cyclic, and the linear independent of characters shows that the minimal polynomial of σ is n-dimensional thus equals $X^n - 1$. Regard L as a $K[X]$ module thus by (3.2.4.21) is a direct sum of modules of the form $K[X]/(f(x))$, $f(x)|X^n - 1$ and the minimal polynomial for the action of X is $X^n - 1$. So it must be isomorphic to $K(X)/(X^n - 1)$.

Infinite Case: Let

$$f(\{X_\sigma\}) = \det(t_{\sigma_i, \sigma_j}) \in \mathbb{Z}[\{X_\sigma\}], \quad t_{\sigma,\tau} = X_{\sigma^{-1}\tau}$$

then $f \neq 0$ by substituting 1 for X_{id} and 0 otherwise. So it won't vanish for all $x \in L$ if we substitute $X_\sigma = \sigma(x)$ because $\{(\sigma(x))_\sigma\}$ are algebraically independent(3.2.8.4). Thus there exists $w \in L$ s.t.

$$\det(\sigma^{-1}\tau(w)) \neq 0.$$

Now if

$$\sum a_\tau \tau(w) = 0, \qquad a_\sigma \in K,$$

act by σ for all σ, we get $[\sigma^{-1}\tau(w)]_{\tau,\sigma}[a_\sigma]_\sigma = 0$, thus $a_\sigma = 0$ for each $\sigma \in \text{Gal}(L/K)$. So $\{\tau(w)\}$ is a K-basis of L. □

Prop. (3.2.8.9) [Kummer Theory]. Let K be a field and containing the set n-th roots of unity μ_n where $n \in \mathbb{Z} \cap K^*$, a **Kummer extension** L/K of exponent n is a Galois extension that the Galois group is Abelian of exponent n.

Then there is an inclusion preserving isomorphism between the lattice of Kummer extensions L over K and the lattice of subgroups of $K^\times$ containing $(K^\times)^n$:

$$L \mapsto \Delta = (L^\times)^n \cap K^\times, \qquad \Delta \mapsto K(\sqrt[n]{\Delta}).$$

And $\Delta/(K^\times)^n$ is isomorphic to $\mathrm{Gal}(L/K)^\vee = \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$. ⌟

Proof: The Galois cohomology of the Kummer sequence $1 \to \mu_n \to L^\times \xrightarrow{n} (L^\times)^n \to 0$ says

$$1 \to K^\times \xrightarrow{n} (L^\times)^n \cap K^\times \xrightarrow{\delta} H^1(\mathrm{Gal}(L/K), \mu_n) \to H^1(\mathrm{Gal}(L/K), L^\times) = 1(8.7.3.2)$$

And $\mathrm{Gal}(L/K)$ acts trivially on $\mu_n \subset K^*$, so

$$H^1(\mathrm{Gal}(L/K), \mu_n) = \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$$

and

$$\delta : a \mapsto \chi_a(\sigma) = \sigma(\sqrt[n]{a})/\sqrt[n]{a} \in \mu_n.$$

Now let L/K be the maximal Kummer extension of exponent n, then $(L^\times)^n = K^\times$. So the assertion follows form Galois theory on applied to L/K. □

Prop. (3.2.8.10) [Finite Fields]. $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}/(n)$. and is generated by the Frobenius. ⌟

Proof: □

Prop. (3.2.8.11) [Artin-Schreier Theory]. Let $K \in$ p-`Field` containing $\mathbb{F}_q$, where $q = p^k$, an **Artin-Schreier extension** L/K of exponent q is a Galois extension that the Galois group is Abelian of exponent q.

Then there is an inclusion preserving isomorphism between the lattice of Artin-Schreier extensions L over K of exponent q and the lattice of subgroups of $W^+_{p,k}(K)$ containing $(W^+_{p,k}(\mathrm{Frob}^k_p) - \mathrm{id})(W^+_{p,k}(K))$:

$$L \mapsto \Delta = (W^+_{p,k}(\mathrm{Frob}^k_p) - \mathrm{id})(W^+_{p,k}(L)) \cap W^+_{p,k}(K),$$

$$\Delta \mapsto K(\{b_{i1}, \ldots, b_{ik} | b_i = (b_{i1}, \ldots, b_{ik}), W^+_{p,k}(\mathrm{Frob}^k_p)(b) - b \in \Delta\}).$$

And $\Delta/(W^+_{p,k}(\mathrm{Frob}^k_p) - \mathrm{id})(W^+_{p,k}(K))$ is isomorphic to $\mathrm{Gal}(L/K)^\vee = \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$. ⌟

Proof: The Galois cohomology of this exact sequence

$$0 \to W^+_{p,k}(\mathbb{F}_q) \to W^+_{p,k}(L) \xrightarrow{W^+_{p,k}(\mathrm{Frob}^k_p) - \mathrm{id}} (W^+_{p,k}(\mathrm{Frob}^k_p) - \mathrm{id})(W^+_{p,k}(L)) \to 0,$$

says

$$1 \to W^+_{p,k}(K) \xrightarrow{W^+_{p,k}(\mathrm{Frob}^k_p) - \mathrm{id}} (W^+_{p,k}(\mathrm{Frob}^k_p) - \mathrm{id})(W^+_{p,k}(L)) \cap W^+_{p,k}(K)$$
$$\xrightarrow{\delta} H^1(\mathrm{Gal}(L/K), W^+_{p,k}(\mathbb{F}_q)) \to H^1(\mathrm{Gal}(L/K), W^+_{p,k}(L)) = 0(8.7.3.3)$$

And $\mathrm{Gal}(L/K)$ acts trivially on $W^+_{p,k}(\mathbb{F}_q)$, so by(5.5.3.22),

$$H^1(\mathrm{Gal}(L/K), W^+_{p,k}(\mathbb{F}_q)) = \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$$

and

$$\delta : a \mapsto \chi_a(\sigma) = \sigma(b) - b \in W^+_{p,k}(\mathbb{F}_q), \quad W^+_{p,k}(\mathrm{Frob}^k_p)(b) - b = a.$$

Next we prove for any $b = (b_1, \ldots, b_k), W^+_{p,k}(\mathrm{Frob}^k_p)(b) - b \in W^+_{p,k}(K)$, $K(\{b_1, \ldots, b_k\})/K$ is Abelian of exponent q: Let $K_i = K(\{b_1, \ldots, b_i\})$. By(5.5.3.4),

$$(b_1^q, \ldots, b_k^q) - (b_1, \ldots, b_k) \in W^+_{p,k}(K)$$

implies $b_i^q - b_i \in K_{i-1}$. Thus K_i/K_{i-1} is an Artin-Schreier extension of exponent p. As the Galois action is always of the form $\sigma(s) - s \in \mathbb{F}_q$ for any $\sigma \in \mathrm{Gal}(K_k/K)$ and $s \in K_k$, we see K_k/K is also Artin-Schreier of exponent $q = p^k$.

Now let L/K be the maximal Artin-Schreier extension of exponent q, then $(W^+_{p,k}(\mathrm{Frob}^k_p) - \mathrm{id})(W^+_{p,k}(L)) = W^+_{p,k}(K)$. So the assertion follows form Galois theory on applied to L/K. □

Cor. (3.2.8.12) [Artin-Schreier of Exponent p]. Let K be a field of characteristic $p > 0$, then there is an inclusion preserving isomorphism between the lattice of Artin-Schreier extensions L over K of exponent p and the lattice of subgroups of K^+ containing $\{x^p - x | x \in K\}$:

$$L \mapsto \Delta = \{x^p - x | x \in L\} \cap K,$$

$$\Delta \mapsto K(\{b | b^p - b \in \Delta\}).$$

And $\Delta/\{x^p - x | x \in K\}$ is isomorphic to $\mathrm{Gal}(L/K)^\vee = \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$. ⌟

Applications

Thm. (3.2.8.13) [Unsolvability of the Quintic by Radicals, Abel1826-Galois1832]. ⌟

Proof: □

9 Ordered Rings

Def. (3.2.9.1) [Ordered Rings]. An **ordered ring** is a ring R together with a subset $P \subset R$ that R is a disjoint union $P \coprod \{0\} \coprod (-P)$, and if $x, y \in P$, then $x + y, xy \in P$. Elements in P are called **positive elements**.

An **ordered field** is an ordered ting that is also a field. An **orderable ring/field** is a ring/field that can be given an ordered structure. ⌟

Prop. (3.2.9.2). An orderable field has char0, because $0 \notin P \cup (-P)$.

A square> 0 in an ordered field(trivial). ⌟

Def. (3.2.9.3) [Convex Subgroup]. Let Γ be an ordered Abelian group(3.2.9.1), then a **convex subgroup** of A is a subgroup Δ that if $a < b < c$ and $a, c \in \Delta$, then $b \in \Delta$. Notice this is in fact equivalent to if $0 < c \in \Delta$, then $0 < b < c$ are also in Δ. ⌟

Prop. (3.2.9.4) [Height]. The set of all convex subgroups of Γ is well-ordered, and its ordinal is called the **height** of Γ. ⌟

Proof: If Δ_1, Δ_2 don't contains each other, let $a \in \Delta_1 - \Delta_2$ and $b \in \Delta_2 - \Delta_1$, then changing $\pm a, \pm b$, we may assume $0 < a < b$, so $a \in \Delta_2$, contradiction. □

Prop. (3.2.9.5)[Height 1 Case]. Let Γ be an ordered Abelian group, then the following are equivalent:

1. $\mathrm{ht}(\Gamma) = 1$.
2. for all $a, b \in \Gamma$ that $a > 0$ and $b \geq 0$, there is an integer n that $b \leq na$.
3. there exists an injection from Γ to $\mathbb{R}$.

⌟

Proof: $3 \to 1$ is easy.

$1 \to 2$: Consider the convex subgroup generated by a, then it is Δ by height condition, so b must by in it, i.e. $b \leq na$ for some n.

$2 \to 3$: Choose an $a > 0$, let the injection φ given by $\varphi(b) = \sup\{\frac{n}{k} | na \leq kb\}$ for $b > 0$ and extends to negative elements.

It is easily verified that $\varphi(c) + \varphi(b) \leq \varphi(c+b)$, and if $\varphi(c) + \varphi(b) < \varphi(c+b)$, choose a rational approximation of them, and multiply to get integers, then if $k(c+b) \leq \varphi(c+b)ka > \varphi(b)a + \varphi(c)a + a$, then either $kc \geq \varphi(c)ka + a$ or $kb \geq \varphi(b)ka + a$, contradiction.

So this map is truly a morphism of ordered Abelian groups, and it is injective because if $b > 0$, then by 2, there must be an n that $a \leq nb$, so $\varphi(b) \geq 1/n$. □

10 Real Fields

Def. (3.2.10.1) [Real Fields]. A field K is called **real** if -1 is not a sum of squares in K. A field K is called **real closed** iff it is real, and any alg.extension that is real must be itself. An ordered field is clearly a real field by(3.2.9.2), the converse is in fact true, by(3.2.10.11). In particular, a real field is of characteristic 0. ⌟

Prop. (3.2.10.2). If K is real, $a \in K$, a and $-a$ cannot both be sum of squares. If $-a$ is not a sum of squares in K, then $K(\sqrt{a})$ is real. Hence either $K(\sqrt{a})$ or $K(\sqrt{-a})$ is real. ⌟

Proof: Suppose $K(\sqrt{a})$ is not real. If a is a square, then $K(\sqrt{a}) = K$ is real. So a is not a square,

$$-1 = \sum (b_i + c_i\sqrt{a})^2 = \sum (b_i^2 + ac_i^2 + 2b_ic_i\sqrt{a})$$

Since $\sqrt{a} \notin K$, $-1 = \sum (b_i^2 + ac_i^2)$, so

$$-a = \frac{1 + \sum b_i^2}{\sum c_i^2}$$

This implies that $-a$ is a sum of squares. □

Prop. (3.2.10.3). If the minimal polynomial f of an α algebraic over a real field K is of odd degree, then $K(\alpha)$ is real. ⌟

Proof: If $K(a)$ is not real, then $-1 = \sum g_i(X)^2 + h(X)f(X)$, where g_i has degree smaller than n. This can happen if $h(X)$ has degree odd and $\leq n-2$. Then if β is a root of h, then $K(\beta)$ is also not real. So the proof is finished if we use induction. □

Def. (3.2.10.4) [Real Closure Exists]. For any real field K, there exists a **real closure** K^a of K. That is, it is real closed and algebraic over K. ⌟

Proof: This is an easy consequence of Zorn's lemma. □

Cor. (3.2.10.5) [Real Closed Fields Unique Ordering]. There exists a unique ordering on a real closed field R. The elements> 0 are just the squares in R. Now every real closed field is assumed to have this ordering tacitly. In particular, any real closed field has char0, so does any real field. ⌟

Proof: The set of finite sum of squares in R is closed under addition and multiplication, and all of them are squares, by(3.2.10.2) and maximality of R. Also by(3.2.10.2) either a is a square or $-a$ is a square, but not simultaneously. So it is truly an order on R. □

Prop. (3.2.10.6) [Fundamental Theorem of Algebra]. For $R \in \texttt{Field}$, R is real closed iff $R \neq R[\sqrt{-1}]$ and $\overline{R} = R(\sqrt{-1})$. ⌟

Proof: One direction is trivial, the other follows from the lemma below(3.2.10.7), it satisfies the condition by(3.2.10.2) and maximality. □

Lemma (3.2.10.7) [Equivalent Definition of Real Closed Fields]. If R is a real field that: for all $a \in R$, $\sqrt{a} \in R$ or $\sqrt{-a} \in R$, and any polynomial of odd degree has a root in R, then $K = R(\sqrt{-1})$ is alg.closed. ⌟

Proof: For any order of R, the first condition in fact says that any $a > 0$ in R is a square. Now $\frac{a+\sqrt{a^2+b^2}}{2}$ is non-negative, so there is a $c^2 = \frac{a+\sqrt{a^2+b^2}}{2}$, that is $(c+\frac{b}{2c}i)^2 = a+bi$, so K has all squares.

As R is of char0(3.2.10.5)(3.2.9.2), so it suffices to show any Galois extension L/K is trivial. Let $G = G(L/R)$, and H be its 2-Sylow subgroup, then $G = H$ by condition. Now if $G_1 = G(L/K)$, then G_1 is nontrivial, because otherwise there is a subgroup of index 2, then its fixed field is a square extension of K, which is impossible by what we have proved. So $G = G_1$, that is $L = K$. □

Cor. (3.2.10.8) [Complex Numbers is Alg.Closed, Gauss1799]. $\mathbb{C} = \mathbb{R}[i]$ is alg.closed. ⌟

Prop. (3.2.10.9) [Intermediate Property]. An ordered field is real closed iff it has the intermediate property. ⌟

Proof: If R is real closed, as $R[i]$ is alg.closed(3.2.10.6), f can be decomposed into factors of degree 1 or 2. For a factor $X^2 + \alpha X + \beta$, $4\beta > \alpha^2$, otherwise it has a root hence not irreducible. So the change of sign is because of a linear factor, the rest is easy.

Conversely, if it has the intermediate property, then for $a > 0$, consider $p(X) = X^2 - a$, then $p(0) < 0, p(a+1) > 0$, so p has a root, that is, a is a square. For a polynomial of odd degree, for M large enough, $f(M) > 0, f(-M) < 0$, so f has a root. So by(3.2.10.7) R is real closed. □

Prop. (3.2.10.10) [Artin-Schreier]. If $K \in \texttt{Field}$, $K = K^{\mathrm{sep}}$, and $F \subset_{\mathrm{fin}} K$, then $F = K$ or F is real closed and $K = F(\sqrt{-1})$. ⌟

Proof: Cf.[?]P299. □

<u>**Real Fields and Order**</u>

Prop. (3.2.10.11) [Real Field and Order]. If R is a real field, then it is orderable, in fact, if $-a$ is not a sum of squares in F, then there is an ordering that $a > 0$. So a real field is equivalent to an orderable field. ⌟

Proof: By(3.2.10.2), $F(\sqrt{a})$ is real, so it has a real closure(3.2.10.4) and has the induced order(3.2.10.5), and $a > 0$ because it is a square(3.2.9.2). □

Prop. (3.2.10.12) [Existence and Uniqueness of Real Closure]. For any ordered field F, there is a unique real closure R of F that every positive element of F is a square in R, thus the ordering is compatible. ⌟

Proof: The existence is by adding all the square roots of elements>0 to F, the resulting field is real closed because of(3.2.10.2) and the fact a union of real fields(3.2.10.2) is real.

The uniqueness: because an ordered field is of char0(3.2.9.2), so the primitive element theorem(3.2.6.20) applies that each finite subextension of R_0 is of the form $F(\alpha)$, where α is a root of a irreducible separable polynomial f. Then the roots of f are different so can be ordered $\alpha_1 < \ldots < \alpha_n$. Similarly, f has the same number of different roots in R_1 $\beta_1 < \ldots < \beta_n$ by(3.2.10.14), so there is a map $h : \alpha_i \to \beta_i$, and it is the unique map that a ordered map from $F(\alpha)$ to R_1 extending id on F can be. it is this uniqueness that makes us able to use Zorn's lemma to show that there is a maximal ordered map, must be a map from R_0 to R_1, which is an isomorphism, by primitive element theorem again. □

Prop. (3.2.10.13) [Sturm's Algorithm]. Cf.[Model Theory Marker P327]. ⌟

Cor. (3.2.10.14). If F is an ordered field and R_0, R_1 be two real closure of F that is compatible with the ordering, then any irreducible polynomial has the same number of roots in R_0 and R_1. ⌟

Proof: Cf.[Model Theory Marker P328]. □

Prop. (3.2.10.15) [Hilbert's 17th Problem]. If f is a positive semidefinite rational function over a real closed field F, then f is a sum of squares of rational functions. ⌟

Proof: Let $f(X_1, \ldots, X_n)$ be a positive semidefinite rational function, if f is not a sum of squares of rational functions, then by(3.2.10.11), there is an ordering on $F(\overline{X})$ that $f < 0$. Let R be a real closure of $F(\overline{X})$, then $R \models \exists \overline{v} F(\overline{v}) < 0$, as $F(\overline{X}) < 0$. But RCR is complete, by(2.4.5.6), thus $F \models \exists \overline{v} F(\overline{v}) < 0$ also, contradiction. □

3.3 Polynomials

1 Basics

Prop. (3.3.1.1)[Descartes's Rule of Sign]. Let $p(x) = a_0x^{b_0}+a_1x^{b_1}+\cdots+a_nx^{b_n}$ be a real polynomial with nonzero a_i, where $A_0 < B_1 < \cdots < b_n$, then the number of positive roots of $p(x)$ has the same parity with the number of consecutive changes of signs of $(a_k)_{k=0,\ldots,n}$. ⌟

Proof: Lemma: when $a_0a_n > 0$, the number of positive roots are even and when $a_0a_n < 0$, it is odd. This is seen by consider $p(0)$ and $p(\infty)$.

Then we consider the derivative p' and use induction. Denote the number of changing sign by $v(p)$ and the number of positive roots by $z(p)$, then if $z_0a_1 > 0$, then $v(p) = v(p')$ and $z(p) \equiv z(p') \mod 2$. Then we have $z(p) \equiv v(p) \mod 2$ and middle value theorem shows that $z(p') \leq z(p) - 1$, hence by induction and parity argument, we have $v(p) \geq z(p)$.

If $a_0a_1 < 0$, then the same method shows that $v(p) = v(p') + 1 \geq z(p') + 1 \geq z(p')$ and the have the same parity by the lemma. □

Prop. (3.3.1.2) [Lagrange Interpolation]. if K is a field, a_i are $n+1$ elements of K, b_i are $n+1$ elements of K, then there is a unique polynomial f of degree no greater than n that $f(a_i) = b_i$. ⌟

Proof: The polynomial in search is

$$f(X) = \sum\prod_{j\neq i} b_i\frac{X-a_j}{a_i-a_j}.$$

It is a polynomial of degree smaller than $n+1$, and it satisfies the hypothesis. And clearly there is at most one such polynomial, otherwise their difference has $n+1$ zeros. □

Cor. (3.3.1.3). If $f(X) = a_nX^n + \ldots + a_0$, then for any $n+1$ different integers $a_0, \ldots, a_n$, there exists some $|f(a_i)| \geq \frac{n!}{2^n}|a_n|$. ⌟

Proof: Use Lagrange interpolation and consider the leading coefficient. □

Prop. (3.3.1.4). If a degree n polynomial p satisfies $p(n) = 2^n$ for $n = 0, 1, \ldots, n$, then $p(n+1) = 2^{n+1} - 1$. ⌟

Proof: The polynomial in search is $p(x) = \sum_{k=0}^n \binom{x}{k}$. □

Prop. (3.3.1.5) [Combinatorial Nullstellensatz]. If F is a field and $f \in F[X_1, \ldots, X_n]$ is a polynomial. Let $S_1, \ldots S_n$ be nonempty finite subsets of F and $g_i = \prod_{s\in S_i}(x_i - s)$, then if f vanishes at the common zeros of g_i, then there are polynomials $h_i \in F[X_1, \ldots, X_n]$ that $\deg h_i \leq \deg F - \deg g_i$ and $g = \sum h_ig_i$. ⌟

Proof: The proof is very simple, just replace terms of f by lower degree terms, using equation of g_i, then we get a polynomial that has degree in x_i smaller than $|S_i|$ and vanish on $S_1 \times \ldots \times S_n$, so it must be 0, as easily checked. □

Cor. (3.3.1.6)[Combinatorial Nullstellensatz]. If F is a field and $f \in F[X_1, \ldots, X_n]$ is a polynomial of degree n, if $\prod X_i^{t_i}$ is a highest degree term of f and S_i are arbitrary subsets of F that $|S_i| > t_i$, then there are some $s_i \in S_i$ that $f(s_1, \ldots, s_n) \neq 0$. ⌟

Proof: May assume $|S_i| = t_i + 1$. By combinatorial Nullstellensatz(3.3.1.5), if no such s_i exist, then there are h_i that $f = \sum h_i \prod_{s\in S_i}(x_i - s)$, but the term $\prod X_i^{t_i}$ needs to appear, so it must by some term of h_i times $x_i^{t_i+1}$, which is a contradiction. □

Remark (3.3.1.7). For many combinatorial applications of the combinatorial nullstellensatz, Cf.[Combinatorial Nullstellensatz]. ⌟

Irreducibility

Prop. (3.3.1.8). If $f = a_n x^n + \ldots + a_1 x + p \in \mathbb{Z}[X]$ satisfies p is a prime and $\sum |a_i| < p$, then f is irreducible in p. ⌟

Proof: The ideal is that all of its roots has norm bigger than 1, because otherwise $p = |\sum a_k x^k| \leq \sum |a_k| < p$, contradiction. So if now $f = gh$, then g, h all have roots with norm greater than 1, in particular it has constant coefficients norm greater than 1, which is a contradiction because p is a prime. □

Resultants

Def. (3.3.1.9)[Resultants]. Let $R \in \mathcal{CR}\text{ing}$, the **resultant** $\operatorname{res}(A, B)$ of two polynomials $A, B \in R[X]$ of degree d, e respectively is the determinant of the linear map

$$W_e \times W_d \to W_{d+e} : (X, Y) \mapsto AX + BY,$$

where W_t is the free module of polynomials of degree $< t$. ⌟

Prop. (3.3.1.10). The resultant can be seen as the determinant of the matrix with values the coefficient of A or B in different places, multiplying X^*s with different degree and add to the last row, we can get $A \cdot X^*$s and $B \cdot X^*$s, so: $\operatorname{res}(A, B) = AC + BD$ for some C, D.

Now if $R \subset S$ and A, B has common roots in S, then $\operatorname{res}(A, B) = 0$. ⌟

Cor. (3.3.1.11). Resultant is stable under Euclidean division, so it can be seen as a suitable division remainder of the two polynomial. ⌟

Prop. (3.3.1.12). When $R \subset L$ a field and A, B decompose into linear factors in L, let t_i be roots of A and u_j be roots of B, then

$$\operatorname{res}(A, B) = v_0^d w_0^e \prod_{i=1}^{d} \prod_{j=0}^{e} (t_i - u_j)$$

⌟

Proof: See the resultant as polynomials of the roots of A and B, then we proved that if they has the same root, then $res = 0$, so it is divisible by $(t_i - u_j)$ for all i, j. Then notice the RHS is homogenous of degree d in u_j and homogenous of degree e in t_i, so does res. So they are equal. □

Prop. (3.3.1.13). Let $k \in \texttt{Field}$ and $P \in k[X]$, then $x \in k$ is a double root of P iff $\gcd(P, P')(x) = 0$. ⌟

Proof: □

2 Cyclotomic Polynomials

Cf.[Cyclotomic Polynomials in Olympiad Number Theory].

Def. (3.3.2.1) [Cyclotomic Polynomials]. For $n \in \mathbb{Z}_+$, define the **cyclotomic polynomial**

$$\Psi_n(X) = \prod_{a \in (\mathbb{Z}/(n))^*} (X - e^{2\pi i \frac{a}{n}}) \in \mathbb{C}[X].$$

Then in fact $\Psi_n(X) \in \mathbb{Z}[X]$. ⌟

Proof: Its coefficients are algebraic integers, and it is invariant under action of $\mathrm{Gal}_\mathbb{Q}$, so its coefficients are in $\mathbb{Q} \cap \mathcal{O}_{\overline{\mathbb{Q}}} = \mathbb{Z}$. □

Prop. (3.3.2.2) [Cyclotomic Polynomials are Irreducible]. For any $n \in \mathbb{Z}_+$, the cyclotomic polynomial $\Psi_n(x)$ is irreducible over $\mathbb{Z}$. ⌟

Proof: It suffices to show that for any irreducible factor $f | \Psi_n(x)$, if ξ is a root of f and $(p, n) = 1$, then ξ^p is also a root of f. Cf.[**?**].**?** □

Prop. (3.3.2.3). For $a, n \in \mathbf{P}$ and $(a, n) = 1$, $\Psi_n(X^p) = \prod_{d|a} \Psi_{dn}(X)$. ⌟

Proof: This follows from counting. □

Cor. (3.3.2.4). For $n \in \mathbb{Z}_+$, $X^n - 1 = \prod_{d|n} \Psi_d(X)$. Thus by Möbius inversion, $\Psi_n(x) = \prod_{d|n}(X^d - 1)^{\mu(n/d)}$. ⌟

Prop. (3.3.2.5). For $n \in \mathbb{Z}_+$ and $p \in \mathbf{P}$,

$$\Psi_{np}(X) = \begin{cases} \Psi_n(X^p) & , p | n \\ \frac{\Psi_n(X^p)}{\Psi_n(X)} & , p \nmid n \end{cases}.$$

⌟

Proof: These follows from counting. □

Cor. (3.3.2.6). If $n \in \mathbb{Z}_{\geq 3}$ is odd, then $\Psi_{2n}(X) = \Psi_n(-X)$. ⌟

Proof: It suffices to show that $\Psi_{2n}(X^2) = \Psi_n(X)\Psi_n(-X)$. And this is because $\zeta \mapsto \zeta^2$ is an automorphism between primitive n-th roots, and $\varphi(n)$ is even. □

Prop. (3.3.2.7). For $m \neq n \in \mathbb{Z}_+$, $\Psi_m(X)$ and $\Psi_n(X)$ are coprime in $\mathbb{Q}(X)$. And if $m, n \in \mathbb{Z}_+ \setminus (p)$, then $\Psi_m(X)$ and $\Psi_n(X)$ are also coprime in $\mathbb{F}_p[X]$. ⌟

Proof: It suffices to show that $X^{mn} - 1$ doesn't have multiple roots. By(3.3.1.13), it suffices to notice that

$$\gcd(X^{mn} - 1, mnX^{mn-1}) = 1,$$

which is also true in $\mathbb{F}_p[X]$ if $m, n \in \mathbb{Z}_+ \setminus (p)$. □

Cor. (3.3.2.8). For $p \in \mathbf{P}$ and $n \in \mathbb{Z}_+ \setminus (p), a \in \mathbb{Z}$,

$$p | \Psi_n(a) \iff p \nmid a \quad \& \quad \mathrm{ord}(a, \mathbb{F}_p^\times) = n.$$

⌟

Cor. (3.3.2.9). For $p \in \mathbf{P}$ and $n \in \mathbb{Z}_+ \setminus (p)$, $p|\Psi_n(a)$ for some $a \in \mathbb{Z}$ iff $p \equiv 1 (\mathrm{mod}\ n)$. ⌟

Prop. (3.3.2.10). If $m \geq n \in \mathbb{Z}_+, h \in \mathbb{Z}$, and $A = \gcd(\Psi_n(h), \Psi_m(h)) \neq 1$, then there exists $p \in \mathbf{P}$ s.t. $A \in p^{\mathbb{Z}_+}$, and also $\frac{m}{n} \in p^{\mathbb{Z}_+}$. ⌟

Proof: Suppose $p|A$, and suppose $m = p^a c, n = p^b d, p \nmid cd$, then by(3.3.2.5),

$$\Psi_m(h) \equiv (\Psi_c(h))^{p^a} (\mathrm{mod}\ p), \quad \Psi_n(h) \equiv (\Psi_d(h))^{p^b} (\mathrm{mod}\ p).$$

Then it follows from(3.3.2.7) that $c = d$. Thus $\frac{m}{n} \in p^{\mathbb{Z}_+}$. The assertions follow easily from this. □

Prop. (3.3.2.11). For $n \in \mathbb{Z}_+$,

$$\Psi_n(1) = \begin{cases} p & , n \in p^{\mathbb{Z}_+}, p \in \mathbf{P} \\ 1 & , \text{otherwise} \end{cases}$$

⌟

Proof: This follows easily from induction and the fact

$$X^{n-1} + \ldots + X + 1 = \prod_{d|n, d \neq 1} \Psi_d(X).$$

□

3 Stable Polynomials

Def. (3.3.3.1) [Stable Polynomials]. For $n \in \mathbb{Z}_+$, a **real-stable polynomial** $f \in \mathbb{C}[z_1, \ldots, z_n]$ is either a zero polynomial or it satisfies that

$$f(z_1, \ldots, z_n) \neq 0$$

for any $z_1, \ldots, z_n \in \mathscr{H}$. ⌟

Cor. (3.3.3.2). A real stable univariate polynomial is real-rooted. ⌟

Prop. (3.3.3.3) [Wagner]. If $n \in \mathbb{Z}_+$ and $f \in \mathbb{R}[z_1, \ldots, z_n]$ is real stable, then for any $c \in \mathbb{R}$, $f(z_1, \ldots, z_{n-1}, c)$ is also real stable. ⌟

Proof: Cf.[Multivariate stable polynomials: theory and applications]Lemma2.4.**?** □

Prop. (3.3.3.4) [Borcea-Brändén]. Let $m, n \in \mathbb{Z}_+$ and $A_1, \ldots, A_m \in \mathrm{Pos}_{\geq 0}(n; \mathbb{C})$, then

$$f(z_1, \ldots, z_n) = \det(\sum z_i A_i)$$

is a real stable polynomial(3.3.3.1). ⌟

Proof: **?**Cf.[Applications of stable polynomials to mixed determinants: Johnson's conjectures, unimodality, and symmetrized Fischer products]Prop2.4.. □

Prop. (3.3.3.5) [Borcea-Brändén]. Let $n \in \mathbb{Z}_+$ and $T : \mathbb{R}[z_1, \ldots, z_n] \to \mathbb{R}[z_1, \ldots, z_n]$ be a differential operator of the form

$$T = \sum_{\alpha, \beta \in \mathbb{N}^n} c_{\alpha,\beta} z^\alpha \partial^\beta,$$

and define

$$f_T(\mathbf{z}, \mathbf{w}) = \sum_{\alpha, \beta \in \mathbb{N}^n} c_{\alpha,\beta} z^\alpha w^\beta.$$

Then T preserves real-stable polynomials(3.3.3.1) iff $F_T(\mathbf{z}, -\mathbf{w})$ is real-stable. ⌟

Proof: ?Cf.[Multivariate Polya-Schur classification problems in the Weyl algebra]Thm1.3. □

Cor. (3.3.3.6). For any $a, b \in \mathbb{R}_{\geq 0}$, the operators $T = 1 + a\partial_x$ or $T = 1 + a\partial_x + b\partial_y$ preserves real-stable polynomials. ⌟

Mixed Characteristic Polynomials

Def. (3.3.3.7) [Mixed Characteristic Polynomials]. For $m, d \in \mathbb{Z}_+$ and $A_1, \ldots, A_m \in \mathrm{Mat}(n; \mathbb{C})$, the **mixed characteristic polynomial** of $A_1, \ldots, A_m$ is defined to be

$$\mu[A_1, \ldots, A_m](X) = \Big[\prod_i (1 - \partial_{z_i}) \det(X\mathbf{1} + \sum_i z_i A_i)\Big]\Big|_{z_1 = \ldots = z_m = 0}.$$

It is a monic polynomial. ⌟

Thm. (3.3.3.8) [Mixed Characteristic Polynomials are Real-Rooted]. For $m, d \in \mathbb{Z}_+$ and $A_1, \ldots, A_m \in \mathrm{Pos}_{\geq 0}(n; \mathbb{C})$, the mixed characteristic polynomial $\mu[A_1, \ldots, A_m]$ is monic and real-rooted. ⌟

Proof: It follows from(3.3.3.4)(3.3.3.6) and(3.3.3.3) that $\mu[A_1, \ldots, A_m]$ is real stable. Then it is real-rooted by(3.3.3.2). □

Thm. (3.3.3.9) [Marcus-Spielman-Srivastava]. Let $m, d \in \mathbb{Z}_+$ and $v_1, \ldots, v_m$ be independent random column vectors in $\mathbb{C}^d$ with finite support, and let $A_i = \mathbf{E}\, v_i v_i^*$, then

$$\mathbf{E}\det(X\mathbf{1} - \sum_i v_i v_i^*) = \mu[A_1, \ldots, A_m](X)(3.3.3.7).$$

⌟

Proof: Using induction on m, it suffices to show that for any $A \in \mathrm{Mat}(d; \mathbb{C})$,

$$\mathbf{E}\det(A - vv^*) = \Big[(1 - \partial_t)\det(A + t\,\mathbf{E}\, vv^*)\Big]\Big|_{t=0}.$$

If A is invertible, then by(3.5.7.15), the LHS equals

$$\mathbf{E}\det(A)(1 - v^* A^{-1} v) = \det(A)\,\mathbf{E}(1 - \mathrm{tr}(Av^*v)) = \det(A) - \det(A)\,\mathrm{tr}(A^{-1}\,\mathbf{E}\, vv^*).$$

And this equals the RHS by(3.5.7.25).

The case that A being non-invertible follows from continuity. □

Cor. (3.3.3.10). Let $m, n \in \mathbb{Z}_+$ and $u_1, \ldots, u_m, v_1, \ldots, v_m \in \mathbb{C}^n$, $D \in \mathrm{Pos}(n; \mathbb{C})$, and $p_1, \ldots, p_m \in [0, 1]$, then the univariate polynomial

$$P(X) = \sum_{S \subset [m]_+} \prod_{i \in S} p_i \prod_{i \notin S} (1 - p_i) \det(X\mathbf{1} + D + \sum_{i \in S} u_i u_i^* + \sum_{i \notin S} v_i v_i^*)$$

is real-rooted. ⌟

Proof: This follows from(3.3.3.9) with binomial distributions, and also the fact that D is a sum of rank-1 matrices. □

Interlacing Polynomials

Def. (3.3.3.11) [Interlacing Sequences]. For $n \in \mathbb{Z}_+$ and $A = \{\alpha_1 \le \alpha_2 \le \dots \alpha_n\} \in \mathbb{R}$ and $B = \{\beta_1 \le \beta_2 \le \dots \le \beta_{n+1}\} \in \mathbb{R}$, A is said to interlace B iff

$$\beta_1 \le \alpha_1 \le \beta_2 \le \alpha_2 \le \dots \le \alpha_n \le \beta_{n+1}.$$

⌟

Def. (3.3.3.12) [Interlacing Polynomials]. For two real-rooted monic polynomials $f(X), g(X) \in \mathbb{R}[X]$ s.t. $\deg(f) = \deg(g) + 1$, g is said to **interlace the polynomial** f iff the roots of g interlaces the roots of f(3.3.3.11). ⌟

Prop. (3.3.3.13). Let $k \in \mathbb{Z}_+$ and $f_1, \dots, f_k$ be real-rooted polynomials of the same degree, then they have a common interlacing polynomial(3.3.3.12) iff for any $t \in \mathbb{R}$, $|\#\operatorname{Zero}(f) \cap [t, \infty) - \#\operatorname{Zero}(g) \cap [t, \infty)| \le 1$. ⌟

Thm. (3.3.3.14) [Chudnovsky-Seymour]. Let $k \in \mathbb{Z}_+$ and $f_1, \dots, f_k \in \mathbb{R}[X]$ be monic real-rooted polynomials of the same degree, then the following are equivalent:

- $\sum_i \lambda_i f_i$ is real-rooted for any $\lambda_1, \dots, \lambda_k \in \mathbb{R}_{\ge 0}$.
- $f_1, \dots, f_k$ have a common interlacing polynomial.
- Any two f_i, f_j have a common interlacing polynomial.
- $f_i + c f_j$ is real-rooted for any $c \in \mathbb{R}_+$.

⌟

Proof: $1 \to 4$ is trivial.

$4 \to 3$: By(3.3.3.13), it suffices to show that for any $t \in \mathbb{R}$, $|\#\operatorname{Zero}(f_i) \cap [t, \infty) - \#\operatorname{Zero}(f_j) \cap [t, \infty)| \le 1$ for any i, j. We may assume that f_i, f_j have no common zeros. Suppose for the contrary that there exists a maximal $t \in \mathbb{R}$ s.t. $\#\operatorname{Zero}(f_i) \cap [t, \infty) - \#\operatorname{Zero}(f_j) \cap [t, \infty) \ge 2$. then $f_i(t) = 0, f_j(t) \ne 0$. Take $\varepsilon \in \mathbb{R}_+$ small s.t. $f_j, f_i \ne 0 on [t - \varepsilon, t)$. Now for any $\lambda \in [0, 1]$, consider the number of zeros of $F_\lambda = \lambda f_1 + (1 - \lambda) f_2$ on the region $\{x + \mathrm{i}\, y \in \mathbb{C} | x > t - \varepsilon\}$, then it is a constant function of λ. But $F_0 = f_1, F_1 = f_2$, contradicting the assumption. So we proved that $|\#\operatorname{Zero}(f_i) \cap [t, \infty) - \#\operatorname{Zero}(f_j) \cap [t, \infty)| \le 1$ for any i, j.

$3 \to 2$: This follows easily from(3.3.3.13).

$2 \to 1$: This follows easily from the intermediate property. □

Cor. (3.3.3.15) [Derivatives of Interlacing Polynomials]. Let $k \in \mathbb{Z}_+$ and $f_1, \dots, f_k \in \mathbb{R}[X]$ be monic real-rooted polynomials of the same degree with a common interlacing polynomial, then so does $\{f_1', \dots, f_k'\}$. ⌟

Proof: This follows from the fact that the derivative of a real-rooted polynomial is also real-rooted. □

Def. (3.3.3.16) [Interlacing Families]. Let $m, n \in \mathbb{Z}_+, S_1, \dots, S_m \in \operatorname{fin}\mathcal{S}\mathrm{et}$, and $\{f_{s_1, \dots, s_m}\}$ be real-rooted degree n-polynomials with positive leading coefficients indexed over $S_1 \times \dots \times S_m$. For any $k \in [m-1]_+$ and $s_1 \in S_1, \dots, s_k \in S_k$, define

$$f_{s_1, \dots, s_k} = \sum_{s_{k+1} \in S_{k+1}, \dots, s_m \in S_m} f_{s_1, \dots, s_k, s_{k+1}, \dots, s_m},$$

and

$$f_\varnothing = \sum_{s_1 \in S_1, \dots, s_m \in S_m} f_{s_1,\dots,s_m}.$$

Then $\{f_{s_1,\dots,s_m}\}$ is called an **interlacing family of polynomials** if for any $k \in [m-1]_+$ and $s_1 \in S_1, \dots, s_k \in S_k$, the family of polynomials

$$\{f_{s_1,\dots,s_k,t}\}_{t \in S_{k+1}}$$

has a common interlacing. ⌟

Prop. (3.3.3.17). Let $k \in \mathbb{Z}_+, f_1, \dots, f_k \in \mathbb{R}[X]$ be real-rooted polynomials with positive leading coefficients such that $\deg(f_1) = \dots = \deg(f_k)$, and having a common interlacing polynomial(3.3.3.12), then the polynomial

$$f_\varnothing = \sum_i f_i.$$

is also real-rooted, and there exists $i \in [k]_+$ s.t. the roots of f_i is bounded by the largest root of $f_\varnothing$. ⌟

Proof: $f_\varnothing$ is real-rooted by(3.3.3.14).

Let g interlaces each f_i, and α_{n-1} the largest root of g, then $f_i(\alpha_{n-1}) \leq 0$ for any i. So $f_\varnothing(\alpha_{n-1}) \leq 0$. But $f_\varnothing$ has positive leading coefficients, so the largest root β_n of $f_\varnothing$ satisfies $\beta_n \geq \alpha_{n-1}$.

But now $f_i(\beta_n) \geq 0$ for some i. Then this f_i has a root in $[\alpha_{n-1}, \beta_n]$, which is its largest root. So the roots of f_i is bounded by the largest root of $f_\varnothing$. □

Cor. (3.3.3.18). Let $m, n \in \mathbb{Z}_+, S_1, \dots, S_m \in \mathrm{fin}\,\mathcal{S}\mathrm{et}$, and $\{f_{s_1,\dots,s_m}\}$ be an interlacing family of real polynomials, then there exists $s_i \in S_i$ s.t. the roots of $f_{s_1,\dots,s_m}$ is bounded by the largest root of $f_\varnothing$. ⌟

Proof: This follows easily by inductively using(3.3.3.17). □

Thm. (3.3.3.19)[Interlacing Families from Independent Random Vectors]. Let $m, d \in \mathbb{Z}_+$ and $v_1, \dots, v_m$ be independent random column vectors in $\mathbb{C}^d$ with finite support, and let v_i take values $w_{i1}, \dots, w_{il_i}$ with probabilities $p_{i1}, \dots, p_{il_i}$ resp.. For $j_i \in [l_i]_+$, define

$$q_{j_1,\dots,j_m}(X) = \prod_i p_{ij_i} \det(X\mathbf{1} - \sum_i w_{ij_i} w_{ij_i}^*) \in \mathbb{C}[X],$$

then these polynomials form an interlacing family(3.3.3.16). ⌟

Proof: Notations as in(3.3.3.16), it suffices to show that for any $k \in [m]_+$ and $j_i \in [l_i]_+$, the family

$$\{q_{j_1,\dots,j_k,t}\}_{t \in [l_{k+1}]_+}$$

has a common interlacing. By(3.3.3.14), it suffices to show that for any $\lambda_1, \dots, \lambda_{l_{k+1}} \in [0,1]$ s.t. $\sum_j \lambda_j = 1$,

$$\sum_{j=1}^{l_{k+1}} \lambda_j q_{j_1,\dots,j_k,t}$$

is real-rooted. But then this follows from(3.3.3.8) with a suitable choice of the probability distribution. □

4 Invariant Theory

Prop. (3.3.4.1)[Elementary Symmetric Polynomial]. For n indeterminants x_i, define the **elementary polynomials**

$$\sigma_k=\sum_{1\leq i_1<\ldots<i_k\leq n} x_{i_1}x_{i_2}\ldots x_{i_k}\in\mathbb{Z}[x_1,\ldots,x_n]$$

where for $k>n$ this expression means 0. Then any symmetric polynomial is a polynomial of the fundamental symmetric polynomials. ⌟

Proof: Set the first coordinate to 0, then the rest is a polynomial of the fundamental symmetric polynomials by induction, $f(0,x)=h(\sigma_1,\ldots,\sigma_n)$, then consider $f-h$, with h the same expression but x_n is included, we get it is a symmetric polynomial, and it is divisible by x_1, thus also divisible by $\prod x_i$, thus divide it by $\prod x_i$ and use induction, we get f is a polynomial of elementary symmetric polynomials. □

Prop. (3.3.4.2)[Newton Identities]. For n indeterminants x_i, define

$$s_k=\begin{cases}\sum x_i^k & ,k\geq 0\\ 0 & ,k<0\end{cases}\in\mathbb{Z}[x_1,\ldots,x_n],$$

then there are **Newton Identities**:

$$s_k-\sigma_1 s_{k-1}+\ldots+(-1)^n\sigma_n s_{k-n}=0.$$

⌟

Proof: The case of $k\geq n$ is simple. Now if $k<n$, then we prove by induction on n: If n is already proven, then the term is 0 if one of them is 0, but this implies that this equation is divisible by $\prod_{i=1}^{n+1}x_i$, but is has degree $k\leq n$, so it must by 0. □

Prop. (3.3.4.3) [Chern Polynomials]. By(3.3.4.2) and induction there are polynomials $P_k\in\mathbb{Z}[x_1,\ldots,x_k]$ s.t. $P_k(\sigma_1,\ldots,\sigma_k)=s_k, k\geq 0$, called the **Chern polynomials**. Then they satisfy:

$$\log(1+c_1+c_2+\ldots+c_n+\ldots)=\sum_{p\geq 1}(-1)^{p-1}\frac{P_p}{p}\in\mathbb{Q}[[c_1,\ldots,c_n,\ldots]].$$

In particular, we can easily calculate via homogeneity that

$$P_1=c_1,\quad P_2=c_1^2-2c_2,\quad P_3=c_1^3-3c_1c_2+3c_3,\quad P_4=c_1^4-4c_1^2c_2+4c_1c_3+2c_2^2-4c_4.$$

⌟

Proof: We can define elementary power series

$$\sigma_k=\sum_{1\leq i_1<\ldots<i_k} x_{i_1}x_{i_2}\ldots x_{i_k}\in\mathbb{Z}[[x_1,\ldots,x_n,\ldots]],$$

and also

$$s_k=\begin{cases}\sum x_i^k & ,k\geq 0\\ 0 & ,k<0\end{cases}\in\mathbb{Z}[[x_1,\ldots,x_n,\ldots]].$$

Then the Newton identities also holds by taking limits. There is an injection

$$\mathbb{Q}[[c_1,\ldots,c_n,\ldots]]\to\mathbb{Q}[[x_1,\ldots,x_n,\ldots]]:c_i\mapsto\sigma_i,$$

and the LHS is mapped to

$$\log(\prod_i(1+x_i))=\prod_i\log(1+x_i)=\sum_{p\geq 1}(-1)^p\frac{s_p}{p}$$

is the image of the RHS. □

Prop. (3.3.4.4) [Todd Polynomials]. There are **Todd polynomials** $Q_p\in\mathbb{Q}[\sigma_1,\ldots,\sigma_p],p\geq 1$ homogenous of degree p s.t.

$$\mathrm{Todd}(x_1,\ldots,x_n,\ldots)=\prod_{i=1}^n\frac{x_i}{1-e^{-x_i}}=1+\sum_{p\geq 1}Q_p\in\mathbb{Q}[[x_1,x_2,\ldots]]$$

for any $n\in\mathbb{Z}_+$, and

$$Q_1=\frac{1}{2}c_1,\quad ,Q_2=\frac{1}{12}(c_1^2+c_2),\quad Q_3=\frac{1}{24}c_1c_2,\quad Q_4=\frac{1}{720}(-c_1^4+4c_1^2c_2+3c_2^2+c_1c_3-c_4).$$

⌟

Proof: ? □

Prop. (3.3.4.5) [Conjugate Invariant Polynomials]. Any polynomial on the entries of matrixes $M_n(k)$ that is invariant under conjugation is generated by coefficients of $\det(\lambda I+X)$ and can also be generated by $\mathrm{tr}(X^k)$. ⌟

Proof: We notice that the matrixes having disjoint eigenvalues is dense in $M_n(k)$, thus the restriction of the polynomial on these matrixes is a symmetric polynomial(3.3.4.1) thus identical to a polynomial described above. Hence they are equal. □

Prop. (3.3.4.6). For any polynomial on the entries of matrixes $M_n(k)$ that $f(BA)=f(A)$ for $B\in O(n)$, there is a polynomial F that $f(A)=F(A^*A)$. Cf.[Heat Equation and the Index Theorem Atiyah P323]. ⌟

Prop. (3.3.4.7) [Weyl]. Any linear map f from $(\mathbb{R}^m)^{\otimes n}$ to R that is $O(m,\mathbb{R})$-equivariant is a linear combinations of maps of the form:

$$v_1\otimes v_2\otimes\cdots\otimes v_n\mapsto\langle v_{i_1},v_{i_2}\rangle\langle v_{i_3},v_{i_4}\rangle\cdots\langle v_{n-1},v_n\rangle.$$

Where $i_1,\ldots,i_n$ is a permutation of $1,2,\cdots,n$ when n is even and when n is odd, f must be 0. ⌟

Proof: Cf,[Heat Equation and the Index Theorem]. □

3.4 Orthogonal Polynomials

References are [Special Functions].

3.5 Linear Algebra

Main references are [H-K71], [线性代数 谢启鸿], [Rom07] and [Determinant, 高等代数 notes, 安金鹏].

In this section, the category of vector spaces over a field k is studied, without considering any topology on k or V. More generally, the category of free modules over a commutative unital ring R is studied.

Def. (3.5.0.1) [Notations].

- Let $k \in$ `Field`.
-

⌟

1 Basics

Def. (3.5.1.1) [Vector Spaces]. ⌟

Def. (3.5.1.2) [Linear Operators]. A **linear operator** on a R-module V is an element of the endomorphism ring $\mathrm{End}_R(V)$ ⌟

Def. (3.5.1.3) [Basis]. Let R be a field, then the sets S that are linearly independent over R has maximal objects by Zorn's lemma, and such a maximal object must span M, called a **basis** of M. ⌟

Prop. (3.5.1.4) [Dimension]. All basis of a linear k-vector space V have the same cardinality, this cardinality is called the **dimension** $\dim_k(V)$ of V. This follows immediately from(3.2.4.4). ⌟

Prop. (3.5.1.5) [Canonical way of Writing a Basis]. After so many years, I still find it confusing to write a basis and observing change of basis, so I will write it here:

A vector should always be written vertically, and so a basis should be $\overrightarrow{e} = (e_1, \ldots, e_n)$(horizontal), and a vector with basis $\overrightarrow{a}$(vertical) is in fact $\overrightarrow{e}\overrightarrow{a}$.

A change of basis should be written $\overrightarrow{e'} = ea$, with $a \in GL_n$, and then if an operator has matrix A w.r.t. the basis $\overrightarrow{e}$, it then map in the basis $\overrightarrow{e'}$ $v = \overrightarrow{e'}x = \overrightarrow{e}ax \mapsto \overrightarrow{e}Aax = \overrightarrow{e'}a^{-1}Aax$, so it has matrix $a^{-1}Aa$ w.r.t the basis $\overrightarrow{e'}$. ⌟

Prop. (3.5.1.6) [Extension of Basis]. ⌟

Proof: □

Prop. (3.5.1.7). Let F is a subfield of K and U is a K-vector space with a F-subspace U'. Then if every finite F-linearly independent subset of U' is K-linearly independent, then $\dim_F(U') \leq \dim_K(U)$. ⌟

Proof: If the converse is true, there is a F-basis u'_j of U', then some of u'_j is K-linearly dependent, contradiction. □

Def. (3.5.1.8) [Matrices]. Let R be a commutative ring, the set of **matrices** of size $m \times n$ over R is an (non-commutative) algebra $\mathrm{Mat}(m \times n; R)$ over R whose underlying module is $R^{\oplus n^2} = \bigoplus_{1 \leq i \leq m, 1 \leq j \leq n} e_{ij}R$, and the algebra structure is given by

$$e_{ij}e_{ij} = e_{ik}.$$

An element $A = \sum_{1 \leq i \leq m, 1 \leq j \leq n} a_{ij}e_{ij} \in M_{m \times n}(R)$ is denoted by $A = (a_{ij})$. ⌟

Def. (3.5.1.9) [Common Matrices]. Let

$$\mathbf{1} = \mathbf{1}_n \triangleq \mathrm{diag}(1, 1, \ldots, 1) \in \mathrm{Mat}(n; \mathbb{Z}),$$

and

$$\mathbf{J} = \mathbf{J}_n \triangleq \sum_{1 \le i,j \le n} e_{ij}.$$

⌟

Prop. (3.5.1.10). A, B are two $n \times n$-matrices, if $1 - AB$ is invertible, then so does $1 - BA$, and

$$(1 - BA)^{-1} = 1 + B(1 - AB)^{-1} A.$$

⌟

Proof: Immediate from(3.2.1.5) or(3.5.7.12). □

Cor. (3.5.1.11). AB and BA has the same characteristic polynomials. ⌟

Prop. (3.5.1.12). For a ring R, there is an isomorphism of rings

$$\mathrm{Mat}(n; R)^{\mathrm{op}} \cong \mathrm{Mat}(n; R^{\mathrm{op}}).$$

The isomorphism is given by $A \mapsto A^t$. ⌟

Def. (3.5.1.13) [Notation for Matrix Group]. Let R be a ring, denote

- $\mathrm{GL}(n, R)$ be the subgroup of $\mathrm{End}_R(\oplus R^{\oplus n})$ consisting of invertible matrices.
- $\mathrm{SL}(n, R)$ be the subgroup of $GL(n, R)$ consisting of matrices of determinant 1(3.5.7.1).
- $U_n(R)$ be the subgroup of $GL(n, R)$ consisting of upper-triangular matrices.
- $P_n(R)$ be the subgroup of $GL(n, R)$ consisting of matrices $A = (a_{ij})$ that $a_{ni} = 0$ for $i < n$.
- $Q_n(R)$ be the subgroup of $GL(n, R)$ consisting of matrices $A = (a_{ij})$ that $a_{ni} = 0$ for $i < n$ and $a_{nn} = 1$.

⌟

Prop. (3.5.1.14). Let K be a topological field, there is a decomposition of spaces

$$U_n(K)\backslash GL(n, K) \cong GL(1, K) \times U_2(K)\backslash GL(2, K) \times \ldots \times Q_n(K)\backslash GL(n, K)$$

where $\mathrm{GL}(n-1, K)$ embeds $\mathrm{GL}(n, K)$ obviously. ⌟

Remark (3.5.1.15). **?** This is wrong. ⌟

Proof: By induction, it suffices to show

$$U_n(K)\backslash \mathrm{GL}(n, K) \times U_{n-1}(K)\backslash GL(n-1, K) \times Q_n(K) \times GL(n, K).$$

Consider the map $GL(n-1, K) \times GL(n, K) \to U_n(K)\backslash GL(n, K) : (x, y) \mapsto xy$, then $x_1 y_1 = x_2 y_2$ iff $x_1 y_1 = u x_2 y_2$ for some $u \in U_n(K)$, iff $y_1 y_2^{-1} = x_1^{-1} u x_2$. This is possible iff $y_1 y_2^{-1} \in Q_n$, and for all (y_1, y_2) that $y_1 y_2^{-1} \in Q_n$, $x_1 y_1 = u x_2 y_2$ iff $x_1 = u x_2 y_2 y_1^{-1}$. □

2 Rank

Prop. (3.5.2.1) [Rank Nullity Theorem]. For $k \in \texttt{Field}$ and $T : V \to W \in \mathcal{V}\mathrm{ect}_k$, then $\mathrm{rank}(T) + \dim \mathrm{Nul}(T) = V$. ⌟

Proof: This follows from the exact sequence $0 \to \ker(T) \to V \to \mathrm{Im}(T) \to 0$. □

Prop. (3.5.2.2) [Row Rank equals Column Rank]. The row rank of a $m \times n$ matrix A is the same as the column rank. ⌟

Proof: Let A be the matrix of a linear map $T : V \to W$, then column rank equals the range of T, and the row rank equals the range of T^t, so they are equal by(3.5.3.7). □

Prop. (3.5.2.3) [Sylvester's Inequality]. For U a $m \times n$ matrix and V a $n \times k$ matrix,

$$\mathrm{Rank}(UV) \geq \mathrm{Rank}(U) + \mathrm{Rank}(V) - n$$

⌟

Proof: This comes from $\dim \ker fg \leq \dim \ker f + \dim \ker g$, which is because $\ker fg = g^{-1}(\ker f)$. □

Prop. (3.5.2.4) [Finite Field General Linear Group]. Over finite field $\mathbb{F}_{p^k}$, $|GL_n(\mathbb{F}_{p^k})| = (p^n - 1)(p^n - p)\ldots(p^n - p^{n-1})$. ⌟

Proof: This is because choose the rows are equivalent to choosing a basis for $V = \oplus_{i=1}^n \mathbb{F}_{p^k}$, and when choosing n-th row, it suffices to avoid an element in the span of the first $n-1$ rows. □

Prop. (3.5.2.5) [Wedge and Rank]. Let $T : V \to V'$ be a linear map, then $\wedge^k(T) = 0$ iff $\mathrm{rank}(T) < k$. ⌟

Proof: If $\mathrm{rank}(T) < k$, then $\mathrm{Im}(\wedge^k(T)) \subset \wedge^k \mathrm{Im}(T) = 0$. Conversely, if $\mathrm{rank}(T) \geq k$, choose $\{Te_1, \ldots, Te_k\}$ linearly independent, then $T(e_1 \wedge \ldots \wedge e_k) = Te_1 \wedge \ldots \wedge Te_k \neq 0$. □

3 Dual spaces

Def. (3.5.3.1) [Dual Spaces]. Let V be a vector space over a field k, the set of linear functionals on V with value in k form another vector space, which is denoted by V^*, called the **dual space** of V. ⌟

Def. (3.5.3.2) [Annihilator]. Let V be a vector space and $W \subset V$ a subspace, then the **annihilator** $W^\perp$ is the subspace of W^* consisting of linear functionals l on V s.t. $l(W) = 0$. ⌟

Def. (3.5.3.3) [Dual Basis]. Let $V \in \mathcal{V}\mathrm{ect}_k$ and $(e_1, \ldots, e_n)$ is a basis of V, then there exists unique elements $\alpha_1, \ldots, \alpha_n$ of V^* s.t. $(e_i, \alpha_j) = \delta_{ij}$. Any such elements $\alpha_1, \ldots, \alpha_n$ constitute a basis for V^*, and is called the **dual basis** of $(e_1, \ldots, e_n)$. ⌟

Prop. (3.5.3.4) [Dimension of the Annihilator]. Let $W \subset V$ be f.d. vector spaces, then $\dim W + \dim W^\perp = \dim V$. ⌟

Proof: Let $\{e_1, \ldots, e_k\}$ be a basis of W and extend it to a basis $\{e_1, \ldots, e_k, e_{k+1}, \ldots, e_n\}$ of V by(3.5.1.6). Consider the dual space $e_1^*, \ldots, e_n^*$, then the annihilator of W is just $\mathrm{span}\{e_{k+1}^*, \ldots, e_n^*\}$. Thus $k + (n - k) = n = \dim V$. □

Def. (3.5.3.5) [Transpose]. Let $T : V \to W$ be a linear map of f.d. vector spaces, then T induces a map $T^t : W^* \to V^*$ given by $T^t(l) = l \circ T$. This is a linear map, called the **transpose** of T. ⌟

Prop. (3.5.3.6)[Adjoint Map and Transpose]. Let $T : V \to W$ be a linear map of f.d. vector spaces, such that w.r.t. a basis $\{e_1, \ldots, e_n\}$ of V and $\{f_1, \ldots, f_m\}$ of W, T is given by matrix $A = (a_{ij})$. Then w.r.t. the dual basis $\{f_1^*, \ldots, f_m^*\}$ of W^*, $\{e_1^*, \ldots, e_n^*\}$ of V^*, the transpose map(3.5.3.5) $T^t : W^* \to V^*$ is given by the a matrix $A^t = (b_{ij})$, where $b_{ij} = a_{ji}$. A^t is called the **transpose matrix** of A. ⌟

Proof: $\langle e_j, T^t(f_i^*)\rangle = \langle Te_j, f_i^*\rangle = a_{ji}$, thus $b_{ij} = a_{ji}$. □

Prop. (3.5.3.7) [Tranpose Range Nullity Duality]. Let $f : V \to V'$ be a linear map between f.d. vector spaces over a field k, then

- $\mathrm{rank}(T^t) = \mathrm{rank}(T)$.
- The range of T^t is the annihilator of the null space of T.

⌟

Proof: 1: Notice that $T^t(g) = 0$ iff $\langle g, T(v)\rangle = 0$ for any $v \in V$, thus the null space of T^t is just the annihilator of the range of T, which equals $\dim V' - \mathrm{rank}(T)$ by(3.5.3.4). But this space has dimension $\dim\ker(T^t) = \dim V' - \mathrm{rank}(T')$, so $\mathrm{rank}(T) = \mathrm{rank}(T^t)$.

2: This follows from the fact that $(T^t)^t = T$ and the argument above. □

Cor. (3.5.3.8). A linear map between f.d. vector spaces is surjective iff its transpose is injective. ⌟

Prop. (3.5.3.9) [Infinite Dual space]. If $\dim_K V = \infty$, then $\dim_K V < \dim_K V^*$. ⌟

Proof: Notice $\mathrm{Hom}(\oplus_{i\in I} Ke_i, K) = \prod Ke_i^*$.

We prove first that if $|K|$ is at most countable, then $|V| = |I|$. Notice the set $S_n(I)$ of all n-element subsets of I is of the same cardinality of I(2.2.8.3). And the finite sums of K and e_i can be seen as a subset of $S_n(I) \times K^n$, so it has the same cardinality of I.

Now we can prove if $\#K < \aleph_0$, then $\dim V < \dim V^*$. This is because V^* equals the functions from V to K, which is bigger than the functions from V to $\{0, 1\}$, which is the power set of V, so having cardinality $2^{|V|}$ which is bigger than $|V|$, by Cantor theorem(2.2.7.4).

Now generally, K is not countable, but it has a base field F, which is countable, so we consider the F-vector space $W = \oplus_{i\in I} Fe_i$, then $\dim_F W = \dim_K V$, and $\dim_F W < \dim_F W^*$. If we can show $\dim_F W^* \leq \dim_K V^*$, then we are done.

For this, first consider the natural F-linear mapping $W^* \to V^*$, which is clearly an imbedding. Now we want to use(3.5.1.7), so we check the conditions, for F-linearly independent $\varphi_1, \ldots, \varphi_n$, if $\sum c_i\varphi = 0$, $c_i \in K$, then if we can find $w_k \in W$ that $\varphi_i(w_j) = \delta_{ij}$, then this is a contradiction. But this is true, by a simple argument, using the F-linearity of F. □

4 Rational Form and Jordan Form

Prop. (3.5.4.1) [Elementary and Invariant Factors]. A linear operator in $L(V)$ is equivalent to a $\mathbb{K}[X]$-module structure on V, and two operators are similar iff the module structure are isomorphic.

As $K[X]$ is a PID, the elementary factors, invariant factors, cyclic and elementary decomposition theorems(3.2.4.22) can be applied to the case. ⌟

Proof: Cf.[Advanced Linear Algebra P168]. □

Cor. (3.5.4.2) [Jordan Forms].

- For a matrix over an alg.closed field, it is similar to a matrix of blocks $\lambda_i I + N, Nx_i = x_i + 1$, called the **Jordan form**.
- For a real matrix, it is similar to a matrix of blocks of the above form together with $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ on the diagonal and $I_{2\times 2}$ on the lower side.

⌟

Proof: 1: Over an alg.closed field, the elementary factors are all of the form $(x-c_i)^{m_{ij}}$. Now in the basis $v, (T-c_i)v, \ldots, (T-c_i)^{m_i-1}v$, the matrix is just the Jordan form.

2: Over $\mathbb{R}$, the elementary factors are all of the form $(x-c_i)^{m_{ij}}$ and $((x-a)^2+b^2)^{m_{ij}}$. Then complexify it and consider a cyclic vector v, for $(T-(a+bi)I)$, let $v_{n+1} = (T-(a+bi)I)v_n$, and let $v_n = X_n + iY_n$, then it can be verified that T is of the Jordan form given in the basis X_i, Y_i. □

Def. (3.5.4.3) [Companion matrix]. The **companion matrix** for a monic polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in F[X]$ is the matrix

$$T_{p(x)} = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \vdots & \ddots & 0 & \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{bmatrix}$$

⌟

Prop. (3.5.4.4) [Companion Matrix is Nonderogatory]. An operator is cyclic iff it is similar to a companion matrix.

A companion matrix is nonderogatory(3.5.7.28). In fact, the minimal polynomial and the maximal polynomial of the companion matrix of $p(X)$ are both $p(X)$. ⌟

Proof: The operator of the companion matrix is an operator A with a basis $\{v, Av, A^2v, \ldots, A^{n-1}v\}$ and $A^n v = -\sum_{i<n} a_i A^i v$, which just equivalent to the fact the action of A is cyclic.

The determinant of $T_{p(X)}$ equals $p(X)$ by(3.5.4.13), and for the minimal polynomial, in the basis of $\{v, Av, A^2v, \ldots, A^{n-1}v\}$, clearly for a polynomial $f(X)$ of degree $m < n$, $f(A)v \neq 0$, and $p(A)v = \sum_{i<n} a_i A^i v + A^n v = 0$. So the minimal polynomial of A is $p(X)$. □

Prop. (3.5.4.5) [Rational Canonical Form]. Every matrix is similar to splint of companion matrixes(3.5.4.3) corresponding to its elementary divisors. ⌟

Prop. (3.5.4.6) [Invariant Factor Form]. Every matrix is similar to splint of companion matrixes, corresponding to its invariant factors. ⌟

Computing the Invariant Factors

Def. (3.5.4.7) [Elementary Row Operation]. An **elementary row operation** for a matrix M over an algebra A is one of the following:

- Multiplying one row of M by a non-zero scalar in A.
- plus the r-th row by c-times the s-th row, where c is invariant A.

And an **elementary matrix** is a matrix obtained by the identity matrix by an elementary row operation.

Two matrix is called **row equivalent** iff they can be connected by f.m. elementary row operations, and this is equivalent to $M = PN$, where P is a product of f.m. elementary matrices, because left multiplication by an elementary matrix is equivalent to an elementary row operation.

Similarly we can define elementary column operations. ⌟

Lemma (3.5.4.8). The elementary row operation change the determinant only by an invariant element in A. (Clear). ⌟

Prop. (3.5.4.9). Let P be a matrix with entries in $F[X]$, then the following are equivalent:

- P is invertible.
- The determinant is a nonzero scalar.
- P is row equivalent to identity matrix.
- P is a product of elementary matrices.

⌟

Proof: The only hard part is $2 \to 3$: this is because it has determinant in F^*, thus the greatest common divisor of the first column is a scalar, thus we can use row operation to make it $(1, 0 \ldots, 0)^t$, and then we can continue to make it a upper triangular matrix with 1 in the diagonal, and also kill the upper half part. So it is row equivalent to the identity matrix. □

Cor. (3.5.4.10). Let M, N be two matrices with entries in $F[X]$, then they are equivalent iff $N = PM$ for some P that has determinant in F. ⌟

Def. (3.5.4.11). We call M, N **equivalent** iff M, N are connected by a sequence of elementary row operations and column operations. This is equivalent to $M = PNQ$ for P, Q invertible matrices in $M_n(F[X])$. ⌟

Prop. (3.5.4.12) [Normal Form of Companion Matrix]. For a monic polynomial $p(X)$, consider its companion matrix T_p, then the matrix $xI - T_p \in M_n(F[X])$ is equivalent to $\mathrm{diag}(p(X), 1, \ldots, 1)$. ⌟

Proof: Clear, if one reduces the x in the diagonal from the bottom row to the top row one by one. □

Cor. (3.5.4.13). For a companion matrix A of p, $\det(xI - A) = p$. ⌟

Proof: This is from(3.5.4.8), and the fact both the side are monic polynomials. □

Def. (3.5.4.14) [Smith Normal Form]. A matrix in $M_n(F[X])$ is called a **Smith normal form** iff it is diagonal and diagonal entries $f_i \in F[X]$ is monic and satisfies f_k divides f_{k+1}. ⌟

Prop. (3.5.4.15). Any matrix M with entries in $F[X]$ is equivalent to a unique Smith normal form. ⌟

Proof: This is immediate from(12.11.5.7) applied to the PID $F[X]$(3.2.3.17). □

Cor. (3.5.4.16) [Computing Invariant Factors]. The diagonal entries of the Smith form of the matrix $xI - M \in M_n(F[X])$ are just the invariant factors of M. ⌟

Proof: This is because of the uniqueness of Smith form(3.5.4.15) and the invariant factor(3.5.4.6) and(3.5.4.12). □

Applications

Prop. (3.5.4.17). For any two matrices $A, B \in M_{n\times n}(K)$, $(AB)^n$ and $(BA)^n$ are similar. ⌟

Proof: It suffices to show that they have the same elementary factors. Notice that for any irreducible polynomial p, if $p \neq x$, then if $p^k(AB)v = 0$, then $p^k(BA)Bv = 0$, if $p^k(BA)v = 0$, then $p^k(AB)Av = 0$. Thus there are maps $B : N(p^k(AB)) \to N(p^k(BA))$ and $A : N(p^k(BA)) \to N(p^k(AB))$. Now their composition are both injective, thus they have the same dimension.

And for $p = x$, these two both have nullity as the multiplicity of 0 in the charpoly of AB, BA(3.5.7.13), thus the same. So they have the same elementary factors, thus similar. □

Prop. (3.5.4.18) [Matrix Similar to Transpose]. Any matrix is similar to its transpose. ⌟

Proof: This is because the invariant factors can be computed using the greatest common divisors of minors by(3.5.4.15) and(3.5.4.16), and they are clearly invariant under conjugation. □

5 Tensor Algebras

Def. (3.5.5.1) [Tensor Algebras]. The tensor product and tensor algebras of modules are defined in(3.2.4.13) and(5.1.1.21). In this subsection, we focus on tensor algebras of vector spaces. ⌟

Def. (3.5.5.2) [Symmetrized Tensors]. If $k \in \texttt{Field}^0$ and $V \in \mathcal{V}\mathrm{ect}_k$, for any $n \in \mathbb{Z}_+$, we can define a multilinear map

$$V^n \to T^n(V) : (v_1, \ldots, v_n) \mapsto \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(n)}.$$

and descends to a linear map $\sigma : S^n(V) \to T^n(V)$, called the **symmetrizer map**. Elements in $\mathrm{Im}(\sigma) = \widetilde{S}^n(V)$ is called **symmetrized tensors**.

Then $\sigma^2 = \sigma$, and $\ker(\sigma) = I \cap T^n$, where $I = \ker(T(V) \to \mathrm{Sym}(V))$. In particular,

$$T^n(V) = \widetilde{S}^n(V) \oplus (T^n(V) \cap I).$$

⌟

Proof: $\sigma^2 = \sigma$ is easy. So $V = \mathrm{Im}(\sigma) \oplus \ker(\sigma)$. Now $T^n(V) \cap I \subset \ker(\sigma)$, and because $\mathrm{Im}(\sigma) \to S^n(V)$ is surjective, $T^n(V) \cap I = \ker(\sigma)$. □

Def. (3.5.5.3) [Anti-Symmetrized Tensors]. Let $k \in \texttt{Field}^0$ and $V \in \mathcal{V}\mathrm{ect}_k$, for any $n \in \mathbb{N}$, we define a multilinear map

$$V^n \to T^n(V) : (v_1, \ldots, v_n) \mapsto \frac{1}{n!}\sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(n)}.$$

and descends to a linear map $\sigma : \wedge^n(V) \to T^n(V)$, called the **anti-symmetrizer map**. Elements in $\mathrm{Im}(\tau) = \widetilde{\wedge}^n(V)$ is called **anti-symmetrized tensors**.

Then $\tau^2 = \tau$, and $\ker(\tau) = I \cap T^n$, where $I = \ker(T(V) \to \wedge(V))$. In particular,

$$T^n(V) = \widetilde{\wedge}^n(V) \oplus (T^n(V) \cap I).$$

⌟

Proof: $\sigma^2 = \sigma$ is easy. So $V = \mathrm{Im}(\sigma) \oplus \ker(\sigma)$. Now $T^n(V) \cap I \subset \ker(\sigma)$, and because $\mathrm{Im}(\sigma) \to S^n(V)$ is surjective, $T^n(V) \cap I = \ker(\sigma)$. □

Prop. (3.5.5.4). Let $k \in \texttt{Field}$, $A \in \mathrm{Mat}(k)$, then the eigenvalues of $\mathrm{Sym}^n A$ and $\wedge^n A$ are all known. ⌟

Proof: Because we can pass to $\overline{k}$, and over there A is upper-triangularizable. □

6 Supervector Spaces(Berezin)

Def. (3.5.6.1)[Supervector Spaces]. For $k \in \mathtt{Field}^0$, a **supervector space** over k is a $\mathbb{Z}/(2)$-graded vector spaces over k, i.e. $V = V_0 \oplus V_1$. If $\dim V_0 = n$ and $\dim V_1 = m$, then V is denoted by $k^{n|m}$. ⌟

Prop. (3.5.6.2)[Tensors of Supervector Spaces]. There is a natural notion of tensors of supervector spaces, and $\mathcal{S}_2$ acts on $V \otimes V$ by

$$\sigma(v \otimes w) = (-1)^{ij} w \otimes v, \quad v \in V_i, w \in V_j.$$

And then we can define the **symmetric algebra** $S(V) = \oplus_{i\in\mathbb{N}} S^i(V)$ and the **exterior algebra** $\wedge(V) = \oplus_{i\in\mathbb{N}} \wedge^i (V)$ s.t.

$$S(V) = S(V_0) \otimes \wedge(V_1), \quad \wedge(V) = \wedge(V_0) \otimes S(V_1).$$

⌟

7 Homogenous Invariants

Determinants

Def. (3.5.7.1)[Determinant]. For $T \in \mathrm{End}(V)$, as $\dim \wedge^n V^* = 1$, the **determinant** $\det(T) \in R$ is an identity $\det(T) \in R$ determined by the identity $\wedge^n(T^t) = \det T . \mathrm{id}_{\wedge^n V^*}$. That is: $L(T\alpha_1, \ldots, T\alpha_n) = \det T . L(\alpha_1, \ldots, \alpha_n)$. And the determinant of a matrix is defined by the linear operator it associates in a canonical basis. ⌟

Prop. (3.5.7.2)[Properties of Determinants].

1. $\det(\mathrm{id}_V) = 1$.
2. $\det(UV) = \det U \cdot \det V$.
3. T is invertible iff $\det T$ is invertible, in which case $\det(T^{-1}) = (\det T)^{-1}$.
4. If $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for V, and f_i is its dual basis, then $\det T = f_1 \wedge \ldots \wedge f_n(T\alpha_1, \ldots T\alpha_n)$.

⌟

Proof: All these are not hard. □

Cor. (3.5.7.3). $\det(P^{-1}AP) = \det(A)$. ⌟

Prop. (3.5.7.4). $\det T = \det T^t$. ⌟

Proof: Use(3.5.7.2), if $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for V, and f_i is its dual basis, then

$$\det T^t = \alpha_1 \wedge \ldots \wedge \alpha_n(T^t f_1, \ldots, T^t f_n) = f_1 \wedge \ldots \wedge f_n(T\alpha_1, \ldots T\alpha_n) = \det T$$

□

Prop. (3.5.7.5)[Expansion of Determinants]. If A_i be the i-th column of A, then

$$\det A = f_1 \wedge \ldots \wedge f_n(A\varepsilon_1, \ldots, A\varepsilon_n) = f_1 \wedge \ldots \wedge f_n(A_1, \ldots, A_n) = \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) \prod_{1\leq i\leq n} A_{\sigma(i)i}.$$

⌟

Prop. (3.5.7.6). For a matrix, the determinant satisfies the following properties:

1. adding a multiple of a column/row to another column/row, the determinant doesn't change.
2. Multiplying a row or a column with a scalar, then the determinant multiplies with this scalar.
3. Changing two rows or two columns makes the determinant multiply by -1.

⌟

Proof: All this follows from 4 of(3.5.7.2). Notice the last one follows from the first two. □

Prop. (3.5.7.7) [Laplacian Expansion Formula]. Cf.[Determinant 安金鹏 P15]. ⌟

Prop. (3.5.7.8). Adjunction matrix, Cf.[Determinant 安金鹏 P16]. ⌟

Proof: □

Cor. (3.5.7.9). If $AB = 1$, then $BA = 1$. ⌟

Prop. (3.5.7.10) [Cramer's Rule]. Cf.[Determinant 安金鹏 P16]. ⌟

Prop. (3.5.7.11) [Binet's Formula]. Let F/E be a Hermitian pair(3.5.10.13), $A \in \mathrm{Mat}(n \times m; F)$, then

$$\det(A^*A) = \sum_{I\in\{0,\ldots,n\},\#I=m} |\det(A_I)|^2.$$

⌟

Proof: Let $L : F^m \to F^n$ be the corresponding map, then $\wedge^n(L^*) \circ \wedge^n(L) = \wedge^n(L^* \circ L)$. In the canonical basis, the matrices for $\wedge^n(L^*)$(resp. $\wedge^n(L)$) have only one column(resp. one row) with entries $\det(A_I)$ by definition(3.5.7.1), thus the assertion follows by(3.5.7.1) again. □

Prop. (3.5.7.12) [Sylvester's Determinant Identity]. If A and B are matrices of sizes $m \times n$ and $n \times m$, then

$$\det(\mathbf{1}_m + AB) = \det(\mathbf{1}_n + BA)$$

⌟

Proof: Notice

$$\begin{bmatrix} 1 & A \\ B & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ B & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1-BA \end{bmatrix} \begin{bmatrix} 1 & A \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & A \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1-BA & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ B & 1 \end{bmatrix}$$

and use(3.5.7.2). □

Cor. (3.5.7.13). Multiplying by X, we see that the characteristic polynomial of AB and BA are the same. ⌟

Remark (3.5.7.14). There is another proof in case $m = n$: It suffices to show

$$\det(\mathbf{1} + (A + X\mathbf{1})(B + X\mathbf{1})) = \det(\mathbf{1} + (B + X\mathbf{1})(A + X\mathbf{1})).$$

But notice $A + X\mathbf{1}$ and $B + X\mathbf{1}$ are invertible in $\mathrm{Mat}(n; K(X))$, thus

$$\det(\mathbf{1} + (A + x\mathbf{1})(B + x\mathbf{1})) = \det((A + x\mathbf{1})((A + x\mathbf{1})^{-1} + (B + x\mathbf{1}))) = \det(\mathbf{1} + (B + x\mathbf{1})(A + x\mathbf{1})).$$

⌟

Cor. (3.5.7.15). Let $n \in \mathbb{Z}_+, A \in \mathrm{GL}(n;\mathbb{C})$ and $u, v \in \mathbb{C}^n$, then

$$\det(A + uv^t) = \det(A) \cdot (1 + v^t A^{-1} u).$$

⌟

Prop. (3.5.7.16).

$$\det \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \det(A)\det(D - CA^{-1}B).$$

⌟

Proof: As before, consider $\det \begin{bmatrix} A + x\mathbf{1} & B \\ C & D + x\mathbf{1} \end{bmatrix}$, then $A + xI$ is invertible, and this equals

$$\det \begin{bmatrix} A + xI & B \\ C & D + x\mathbf{1} - C(A + x\mathbf{1})^{-1}B \end{bmatrix} = \det(A + xI)\det(D + xI - C(A + xI)^{-1}B).$$

The assertion follows by substituting $x = 1$. □

Prop. (3.5.7.17) [Symplectic Group Determinant]. The determinant of a symplectic matrix in $\mathrm{Sp}(2n, \mathbb{R})$ has determinant 1. ⌟

Proof: A symplectic matrix preserves the symplectic structure thus the symplectic form ω, hence preserves ω^n which is $n!$ times the volume form, so it has determinant 1 by definition(3.5.7.1). □

Prop. (3.5.7.18) [Vandermonde Matrix]. For $R \in \mathcal{CR}\mathrm{ing}$ and $x_1, \ldots, x_n \in R$, the $n \times n$ **Vandermonde matrix** is defined to b $\mathrm{Van}(x_1, \ldots, x_n) \overset{\triangle}{=} (x_i^{j-1})_{i,j}$. Then it has determinant $\prod_{i<j}(x_i - x_j)$. So it is invertible when x_i are pairwisely different. ⌟

Proof: Eliminate the first row by adding columns. □

Prop. (3.5.7.19) [Pfaffian]. There is a **Pfaffian polynomial** $\mathrm{Pf}(M)$ s.t. $\det M = \mathrm{Pf}(M)^2$ for a skew-symmetric matrix. This is because a skew symmetric is equal to $A^t \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^k A$ for A an orthogonal matrix (3.5.10.18), so it has determinant $(\det A)^2$ and A and depends polynomially on the entries of M. ⌟

Cor. (3.5.7.20).

$$\mathrm{Pf}(A^t M A) = \det A \cdot \mathrm{Pf}(M).$$

Because we only need to consider the sign and it is determined by letting $A = \mathbf{1}$. ⌟

Prop. (3.5.7.21) [Determinants of Hermitian Pairs]. ⌟

Characteristic Polynomials

Def. (3.5.7.22) [Characteristic Polynomials]. For $k \in \mathtt{Field}, V \in \mathcal{V}\mathrm{ect}_k$ and $T \in \mathrm{End}(V)$, the **characteristic polynomial** of T is defined to be

$$P(X;T) = \det(X\mathbf{1} - T|V) \in \mathbb{Z}[X](3.5.7.1),$$

where $X\mathbf{1} - T$ is regarded as an element in $\mathrm{End}(V \otimes k(X))$. ⌟

Traces

Def. (3.5.7.23) [Trace]. For a $n \times n$-matrix A, define its **trace** $\mathrm{tr}(A)$ to be the minus of the coefficient of x^{n-1} in $\det(x\mathbf{1} - A)$. It is clear that $\mathrm{tr}(A) = \sum_{i=1}^n a_{ii}$, and by(3.5.7.3) that traces are invariant under conjugacy. ⌟

Prop. (3.5.7.24). $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. ⌟

Proof: This is because $\det(x - AB) = \det(x - BA)$ by Sylvester determinant identity(3.5.7.12). □

Prop. (3.5.7.25). If $A, B \in \mathrm{Mat}(n; \mathbb{C})$ and A is invertible, then

$$\frac{\partial}{\partial t}\det(A + tB) = \det A\,\mathrm{tr}(A^{-1}B).$$

⌟

Prop. (3.5.7.26) [Trace Formula]. For $V \in \mathcal{V}\mathrm{ect}/k, F \in \mathrm{End}(V), d \in \mathbb{Z}_+$,

$$t\frac{\partial}{\partial t}\log\det(1 - FT^d)^{-1} = \sum_{i\geq 1} d\,\mathrm{tr}(F^i|V)T^i \in 1 + Tk[[T]].$$

In particular, if $\mathrm{char}\, k = 0$,

$$\det(1 - FT^d|V)^{-1} = \exp(\sum_{i\geq 1}\mathrm{tr}(F^i|V)\frac{T^{di}}{i}) \in 1 + Tk[[T]].$$

⌟

Proof: Pass to $\overline{k}$ and let $k_1, \ldots, k_r$ be the eigenvalues of F. □

Minimal Polynomials

Def. (3.5.7.27) [Minimal Polynomials]. The **minimal polynomial** of a matrix A is the polynomial p of minimal degree that $p(A) = 0$. It is equivalent to the maximal invariant factor of A, by(3.5.4.1). ⌟

Def. (3.5.7.28) [Non-derogatory Operator]. An operator is called **nonderogatory** iff it has only one invariant factor. ⌟

Prop. (3.5.7.29) [Generalized Cayley-Hamilton]. The characteristic polynomial of A is the product of the elementary divisors of A, thus the characteristic polynomial and minimal polynomial(3.5.7.27) of A have the same set of irreducible factors, but may not with the same multiplicity.

In particular, the characteristic polynomial is divisible the minimal polynomial. ⌟

Proof: Because charpoly and minipoly are both invariant under similarity, assume A is in rational form(3.5.4.5), so the result follows from(3.5.4.4). □

Prop. (3.5.7.30). For $k \in \texttt{Field}$ and $A, C \in \mathrm{Mat}(n; k)$, the linear map $\mathrm{Mat}(n; k) \to \mathrm{Mat}(n; k) : X \to AX - XC$ is an isomorphism iff the minimal polynomials of A and C has no common factor. ⌟

Proof: Notice if $AX = XC$, then we have $P(A)X = XP(C)$ for every polynomial P, in, particular for the minimal polynomials of A and C, thus $P(C)$ is non-invertible and A, C has a characteristic value in common. Conversely, if they have a characteristic value, then we upper triangularize A to see clearly that there is a X that $AX = XC$ (X has only the first row). □

Characteristic Polynomial Images

In this subsubsection, we consider the set of characteristic polynomials of elements in a subgroup of $GL(n,k)$ as a whole.

8 Diagonalization and Triangulation

Prop. (3.5.8.1). If a linear map has matrix form T in a basis (X_i) and there is another basis (Y_i) that $(Y_i) = (X_i)P$, then it has matrix form PTP^{-1} in the basis (Y_i). In particular, if T can be diagonalized, with eigenvectors (X_i), then $T = (X_i)D(X_i)^{-1}$. ⌟

Prop. (3.5.8.2) [Relation with Minimal Polynomial].

- An $n \times n$-matrix A is upper-triangulable over a field K iff its minimal polynomial is a product of linear factors.
- An $n \times n$-matrix A is diagonalizable over a field K iff its minimal polynomial is a product of linear factors with no multiple roots.

⌟

Proof: 1: If it is upper-triangulable, its minimal polynomial is a product of factors because its characteristic polynomial does(3.5.7.29). Conversely, we can find an eigenvector for A, then we quotient this vector and use induction.

2: If it is diagonalizable, then the minimal polynomial is clearly polynomials. Conversely, its elementary factors are all linear factors, thus its Jordan form is just diagonal(3.5.4.2). □

Cor. (3.5.8.3) [Upper Triangulation over Alg.Closed Field]. If $k \in \texttt{Field}, k = \overline{k}$, then any $A \in \mathrm{Mat}(n,k)$ is upper-triangulable over k. Dually, it is lower-triangulable. ⌟

Proof: It suffices to find an eigenvector of A and then use induction. This is clear, as the characteristic polynomial of A has a root in k. □

Prop. (3.5.8.4) [Simultaneously Triangulation]. If A_i is a commutating family of upper-triangulable $n \times n$-matrices, then they are simultaneously triangulable. ⌟

Proof: As in the proof of(3.5.8.3), by induction, it suffices to show there is a common eigenvector. Now assume there are f.m. matrices in $\mathcal{F}$, we induct on the number of matrices to show there is an eigenvector. Let λ be an eigenvalue of A_1 because it is upper-triangulable, then $N(A_1 - \lambda I)$ is invariant under $\mathcal{F}$, and all the matrices are upper-triangulable on $N(A_1 - \lambda I)$, which is seen by intersecting the flag with $N(A_1 - \lambda I)$. So by induction, there is a common eigenvector for $\mathcal{F}$. □

Prop. (3.5.8.5) [Simultaneously Diagonalizable]. If A_i is a commutating family of diagonalizable $n \times n$-matrices, then they are simultaneously diagonalizable.

If A_i is a commutating family of real symmetric matrixes, then they are simultaneously orthogonally diagonalizable. ⌟

Proof: We may assume there are f.m. matrices and use induction. Consider the diagonal decomposition V_i of V for A_1, then each V_i is invariant under $\mathcal{F}$. Notice then each A_i is diagonalizable on V_i, thus by induction, $\mathcal{F}$ is simultaneously diagonalizable on each V_i, then $\mathcal{F}$ is simultaneously diagonalizable.

For the second, induction on the numbers of matrices. If some matrix is cI, then clear, if some are not cI, then choose its eigenvalue decomposition, we conclude by induction hypothesis. □

Prop. (3.5.8.6) [Invariance of Field Extension]. Let $A \in M_n(F)$, and E be the subfield generated by the entries of A, then the invariant factors of A are polynomials over E. In particular, two matrix are similar over the smallest field that they are defined. ⌟

Proof: Clear, because we know how an irreducible polynomial over E factors through $\overline{E}$. □

Prop. (3.5.8.7) [Jordan Decomposition]. Let $k \in \mathtt{Field}, k^{\mathrm{sep}} = k$, and $A \in \mathrm{Mat}(n;k)$, then there exists unique matrices A_s, A_n that A_s is semisimple, A_n is nilpotent, $A = A_s + A_n$, and A_s, A_n are polynomials of A, in particular, A_s commutes with A_n.

Moreover, if A is invertible, then there exists unique matrices A_s, A_u that A_s is semisimple, A_u is unipotent, $A = A_s \cdot A_u$, and A_s, A_u are polynomials of A, in particular, A_s commutes with A_u. ⌟

Proof: If k is alg.closed, then use(3.5.8.3). And Lagrange interpolation shows A_s, A_n are polynomials in A. For the uniqueness, notice that because they are polynomials in A, if there are two sets of Jordan decompositions $A = A_s + A_n = A'_s + A'_n$, then $(A_s - A'_s) = (A'_n - A_n)$, but the sum of commuting semisimple/nilpotent matrices is semisimple/nilpotent, so it is semisimple and nilpotent, so it can only be 0, so $A_s = A'_s$.

In general, because k is perfect, taking a Galois field extension k'/k containing all eigenvalues of A, then $A = A_s + A_n$ where A_s, A_n has entries in k'. But then taking Galois action and using the uniqueness, A_s, A_n has entries in k.

Finally, by the Galois action again, A_s, A_n are polynomials in A.

If A is invertible, then A_s is also invertible, seen by base change to alg.closure. Then $A = A_s(1 + A_s^{-1}A_n)$, where $1 + A_s^{-1}A_n$ is unipotent. □

Prop. (3.5.8.8). If T is a diagonalizable operator on a subspace V, then for any invariant subspace V', $T|_{V'}$ is also diagonalizable. ⌟

Proof: Use the eigenvalue decomposition $V = \oplus_i V_{\lambda_i}$, then $V' = \oplus_i (V_{\lambda_i} \cap V')$, which is because if $\sum v_i \in V'$, where v_i are in different eigenspaces, then each $v_i \in V'$. □

9 Complex Structures

Def. (3.5.9.1) [Complex Pairs]. Let $F \in \mathtt{Field}$, E/F a Galois extension of degree 2 with involution $\mathtt{c} \in \mathrm{Gal}(E/F)$ or $E = F \oplus F$ with involution $\mathtt{c}(x,y) = \overline{(x,y)} = (y,x)$. Such a pair E/F is called a **complex pair**. ⌟

Prop. (3.5.9.2) [Complex Structures]. Let $g \in \mathbb{Z}_+$ and $V \in \mathcal{V}\mathrm{ect}^{2g}/\mathbb{R}$, then the following are equivalent:

- A complex structure on V.
- An endomorphism $J \in \mathrm{End}_{\mathbb{R}}(V)$ s.t. $J^2 = -\mathrm{id}$.
- A representation $\rho : U^1 \to \mathrm{End}_{\mathbb{R}}(V)$ s.t. $V \otimes_{\mathbb{R}} \mathbb{C}$ has weights ± 1, each with multiplicity g.

⌟

Proof: $1 \to 2$: Take J to be multiplication by .

$2 \to 1$: The complex structure is given by $(a + b\,\mathrm{i})x = ax + bJx$.

$2 \to 3$: The representation is given by $\rho(\theta) =\mapsto \cos\theta + \sin\theta J$. Then $V_{\mathbb{C}} = \ker(J - \mathrm{i}) \oplus \ker(J + \mathrm{i})$, and conjugation interchanges these two spaces.

$3 \to 2$: Given such a representation, $J = \rho(\mathrm{i})$ satisfies $J^2 = -1$. □

10 Bilinear & Hermitian Forms

Real Quadratic Spaces

For symmetric bilinear forms and more about quadratic forms, see Quadratic Forms over Fields.

Real Spectral Theory

Remark (3.5.10.1). The general spectral theory4 applies to this case. ⌟

Prop. (3.5.10.2). For a normal operator N on a real inner product space, $N\alpha = 0$ iff $N^t\alpha = 0$. In particular, N and N^t has the same number of eigenvalues and dimension of eigenspaces. ⌟

Proof: This is because

$$(N\alpha, N\alpha) = (N^tN\alpha, \alpha) = (NN^t\alpha, \alpha) = (N^t\alpha, N^t\alpha).$$

□

Cor. (3.5.10.3). For a normal operator N on a real inner product space, $\mathrm{Im}(N) = \ker(N)^\perp$. ⌟

Proof: $\mathrm{Im}(N) = \ker(N^*) = \ker(N)$. □

Cor. (3.5.10.4). For a normal operator N on a real inner product space, if $N^2\alpha = 0$, then $N\alpha = 0$. ⌟

Proof: This is because $N\alpha \in \ker(N) \cap \mathrm{Im}(N) = \varnothing$. □

Lemma (3.5.10.5). If f, g are relatively prime polynomials and T is a normal operator, $f(T)\alpha = 0$ and $g(T)\beta = 0$, then α is orthogonal to β. ⌟

Proof: Choose polynomials a, b that $af + bg = 1$, then $\alpha = b(T)g(T)\alpha$, and

$$(\alpha, \beta) = (b(T)g(T)\alpha, \beta) = (b(T)\alpha, g(T)^*\beta)$$

Notice $g(T)$ is also normal, and $g(T)\beta = 0$, thus by(3.5.10.2) $g(T)^*\beta = 0$. Thus α, β are orthogonal. □

Lemma (3.5.10.6). Let V be a real inner product space and S an operator that $S^2 = -1$. Suppose $\alpha \in V$ and $S\alpha = -\beta$, then

$$S^*\alpha = \beta, \quad S^*\beta = -\alpha,$$

α, β are orthogonal, and $||\alpha|| = ||\beta||$. ⌟

Proof: Because

$$0 = ||S\alpha + \beta||^2 + ||S\beta - \alpha||^2 = ||S\alpha||^2 + ||\beta||^2 + 2(S\alpha, \beta) + ||S\beta||^2 + ||\alpha||^2 - 2(S\beta, \alpha),$$

and S is normal, we get

$$0 = ||S^*\alpha||^2 + ||\beta||^2 - 2(S^*\alpha, \beta) + ||S^*\beta||^2 + ||\alpha||^2 + 2(S^*\beta, \alpha) = ||S^*\alpha - \beta||^2 + ||S^*\beta + \alpha||^2,$$

which gives the desired equation. And also

$$(\alpha, \beta) = (-S^*\beta, \beta) = -(\beta, S\beta) = -(\beta, \alpha)$$

which implies $(\alpha, \beta) = 0$. □

Prop. (3.5.10.7) [Real Normal Operators]. Let A be a normal matrix, then A is orthogonally congruent to matrixes of the form $\mathrm{diag}(B_1,\ldots,B_n)$, where B_i are 1×1 or 2×2 matrices of the form $\begin{bmatrix} a & b \\ -b & a\end{bmatrix}$. ⌟

Proof: Firstly the minimal polynomial of A is a product of different irreducible polynomials $p = p_1\ldots p_k$, by(3.5.10.4). Let $f_i = p/p_i$, then $f_1,\ldots,f_k$ are relatively prime, so there are polynomials g_i that $1=\sum f_i g_i$. Then for any $v\in V$, $v=\sum f_i(T)g_i(T)v$, and $f_i(T)g_i(T)v$ is annihilated by $p_i(T)$. Let $W_i = \ker(p_i(T))$, then $V=\sum W_i$, and W_i is orthogonal to W_j by(3.5.10.5).

The restriction of T on W_i has minimal polynomial p_i. If p_i has degree1, then T is a scalar on W_i. If p_i has degree2, then $p_i = (x-a_i)^2 + b_i^2$ for some $a_i, b_i\in\mathbb{R}, b\neq 0$. Then we choose a maximal k that there exists subspaces $V_j\in W_i, j\leq k$ that

- $\dim V_j = 2$.
- V_j are pairwisely orthogonal.
- V_j is invariant under T, T^*, and $T|_{V_i}$ is orthogonal congruent to $\begin{bmatrix} a_i & b_i \\ -b_i & a_i\end{bmatrix}$.

Then denote $W=\oplus_{j=1}^k V_j$, we prove that $W=V$: Suppose not, then $W^\perp\neq 0$ is invariant under T and T'. Denote $S=b^{-1}(T-a)$, then $S^2+1=0$. Let $\alpha\neq 0\in W^\perp$, $\beta=-S\alpha$, then $S\beta=\alpha$, $\alpha,\beta\in W^\perp$. Since $T=aI+bS$, we have

$$T\alpha = a\alpha - b\beta,\quad T\beta = b\alpha + a\beta.$$

Now lemma(3.5.10.6) implies $\{\alpha,\beta\}$ is invariant under S,S^* thus also T,T^*, so this gives another V_{k+1}, contradiction. □

Cor. (3.5.10.8) [Unitary Equivalence of Normal Operators]. Let T, T' be real(complex) normal matrices, then T is orthogonally(unitarily) congruent to T' iff T and T' have the same characteristic polynomial. ⌟

Proof: This follows from(3.5.10.7)(or (3.5.10.19)). □

Cor. (3.5.10.9) [Complex Structure Form]. A real normal matrix J s.t. $J^2+1=0$ is orthogonal congruent to $\langle\begin{bmatrix} 0 & -1 \\ 1 & 0\end{bmatrix}\rangle_n$.

In particular, as such J is equivalent to a complex structure on $\mathbb{R}^n$, so the set of complex structures is bijective to $O(n)/U(\frac{n}{2})$ thus can be endowed with a structure of a homogenous space. ⌟

Proof: This is because J and $\langle\begin{bmatrix} 0 & -1 \\ 1 & 0\end{bmatrix}\rangle_n$ are both normal and they have the same characteristic polynomial, by(3.5.7.29). □

Def. (3.5.10.10) [Cayley-transformation]. For a field k of char$k\neq 2$ and a matrix $P\in\mathrm{Mat}(n;k)$ that has no eigenvalue -1, there is a **Cayley transformation** $A=\frac{1-P}{1+P}$,. $1+A$ is invertible, and $P=\frac{1-A}{1+A}$.

Then A is skew-symmetric iff P is orthogonal. ⌟

Proof: If $Av=-v$, then $v-Pv=-v-Pv$, so $2v=0$, so $v=0$. So $A+1$ is invertible.

If P is orthogonal, then $A^t=\frac{1-P^t}{1+P^t}=\frac{1-P^{-1}}{1+P^{-1}}=-A$. Conversely, if $A^t=-A$, then $P^t=\frac{1+A}{1-A}=P^{-1}$. □

Prop. (3.5.10.11). If char$k \neq 2$ and P is an orthogonal matrix of odd dimension, then $\det P$ is an eigenvalue of P. ⌟

Proof: multiplying by -1, we can assume $\det P = 1$. Then the action of P on S^{n-1} has a fixed point by Lefschetz trace formula. Thus 1 is an eigenvalue of P. Contradiction. □

Hermitian Spaces

Prop. (3.5.10.12) [Hermitian Forms]. Given a complex vector space (V, J)(3.5.9.2), a **Hermitian form** on (V, J) is an R-bilinear mapping $(-,-) : V \times V \to \mathbb{C}$ that satisfies

$$(Ju, v) = \mathrm{i}(u, v), \quad (u, v) = \overline{(v, u)}.$$

If we write $(u, v) = \varphi(u, v) - \mathrm{i}\,\psi(u, v)$, then

- φ is symmetric and $\varphi(Ju, Jv) = \varphi(u, v)$.
- ψ is alternating and $\psi(Ju, Jv) = \psi(u, v)$.
- $\psi(u, v) = -\varphi(u, Jv), \varphi(u, v) = \psi(u, Jv)$.

Conversely, if φ satisfies these conditions, then

$$(u, v) = \varphi(u, v) + \mathrm{i}\,\varphi(u, Jv).$$

is a Hermitian form. Also $(-,-)$ is positive or non-singular iff φ is. ⌟

Def. (3.5.10.13) [Hermitian Space]. Given a complex pair E/F(3.5.9.1), a **Hermitian space** over F/E is a free E-module V with a E-map $(\cdot, \cdot) : V \times V \to E$ s.t.

- $(cx, y) = (x, \bar{c}y) = c(x, y)$ for $c \in E$.
- $(x, y) = \overline{(y, x)}$.
- the pairing is non-degenerate.

⌟

Def. (3.5.10.14) [Hermitian Transpose]. Let $L : V \to W$ be a map between Hermitian spaces, then there is a **Hermitian transpose** $L^* : W^* \to V^*$ which is a F-anti-linear map that satisfies

$$(Lu, w) = (u, L^* w).$$

As the pairing on V is non-degenerate(3.5.10.13), this is map is uniquely determined.

If $V = W$, then in coordinate forms, it can be verified that $[L^*] = \overline{[L]}^t$. ⌟

Prop. (3.5.10.15) [Gram Matrix]. Let V be a n-dimensional vector space with a canonical basis $e_1, \ldots, e_n$, then a $n \times n$ symmetric(Hermitian) matrix M defines a bilinear(sesqui-linear) form B on V by $(x, y) \mapsto x^t M y (x^t M \overline{y})$. Conversely, for any bilinear(sesqui-linear) form B on V, let $M = (a_{ij})$ where $a_{ij} = (e_i, e_j)$, then M is symmetric(Hermitian) matrix, called the **Gram matrix** of B.

so we will interchange freely between a symmetric(Hermitian) matrix and a bilinear(sesqui-linear) form on V. ⌟

Proof: Trivial. □

Def. (3.5.10.16) [Hermitian Matrices]. Situation as in(3.5.10.13), then a **Hermitian matrix** w.r.t. E/F is a matrix $A \in \mathrm{Mat}(n; E)$ s.t. $A^t = \mathsf{c}\,A$, which corresponds to an E-linear map $L : E^n \to E^n$ s.t. $L^* = L$(3.5.10.14). ⌟

Complex Hermitian Matrices and Real Symmetric Matrices

Prop. (3.5.10.17) [Hermitian Eigenvalues are Real]. Any eigenvalue of a Hermitian(e.g., real symmetric) matrix M is real. ⌟

Proof: Consider the bilinear form defined by the matrix M, then if x is an eigenvector with eigenvalue λ, then $\lambda(x,x) = (Hx,x) = (x,Hx) = \overline{\lambda}(x,x)$, so if λ is not real, $x = 0$. □

Thm. (3.5.10.18) [Principal Axis Theorem]. A symmetric matrix A is orthogonally diagonalizable. Similarly, a Hermitian matrix is unitarily diagonalizable. ⌟

Proof: Firstly, we can find an eigenvector of A: Only the real case needs proof, and this is because any eigenvalue of A is real(3.5.10.17).

Let v be an eigenvector of A of length 1, then the orthogonal complement of v is preserved by A, so we can use induction to find an orthonormal basis consisting of eigenvectors of A, then these together with v forms an orthonormal basis consisting of eigenvectors of A. □

Prop. (3.5.10.19) [Complex Normal operators]. More generally, a normal operator over $\mathbb{C}$ is unitarily diagonalizable using resolution of identity(11.9.4.3) because the spectrum are discrete thus the point projection is orthogonal. ⌟

Prop. (3.5.10.20) [Gram-Schimidt]. Any symmetric matrix over fields of characteristic$\neq 2$ is congruent to a diagonal matrix. ⌟

Proof: Any symmetric matrix defines a bilinear form on V. If B is not identically 0, then there is a x that $x^tBx \neq 0$, by polarization identity. Then $W = \{Kx\}$ is non-degenerate, so we have $W \oplus W^\perp = V$ by(14.5.1.8). And by induction, we are done. □

Prop. (3.5.10.21) [Antonne-Takagi]. For any complex symmetric matrix A, there is unitarily matrix U that UAU^t is a real diagonal matrix with non-negative entries. ⌟

Proof: Consider $B = A^*A$ is Hermitian and positive-semi-definite, thus there is a unitary matrix V that V^*BV is diagonal with non-negative real entries by(3.5.10.18). Now $C = V^tAV$ is complex symmetric with C^*C real diagonal. If we let $C = X + iY$, then $XY = YX$. So by(3.5.8.5), there is a real orthogonal matrix W that WXW^t and WYW^t are diagonal. Now set $U = WV^t$, which is unitary, UAU^t is complex diagonal. And easily we can modify the diagonal entries to be non-negative. □

Prop. (3.5.10.22) [Skew-Symmetric Forms]. For any f.d. skew-symmetric vector space V over a field k with $\operatorname{char} k \neq 2$, then there exists a basis $\{x_1, \ldots, x_r, y_1, \ldots, y_r, z_1, \ldots, z_k\}$ s.t. $(x_i, y_i) = -(y_i, x_i) = 1$, and the inner product of other pairs in this basis vanish.

In particular, if V is non-degenerate, then $\dim V$ is even. ⌟

Proof: Use induction on $\dim V$. If $\dim V = 0$, this is clear. For $\dim V > 0$, if there exists a pair $(x,y) \neq 0$, then we can take $(x,y) = 1$, and we can look at the complement $\{x,y\}^\perp \subset V$ and use induction. □

Prop. (3.5.10.23). Given a bilinear form on a field, the relation of orthogonality is symmetric iff it is symmetric or alternating, i.e. $B(x,x) = 0$. ⌟

Proof: Let $w = B(x,z)y - B(x,y)z$, then $B(x,w) = 0$, hence we have $B(w,x) = 0$, that is

$$B(x,z)B(y,x) - B(x,y)B(z,x) = 0.$$

Let $z = x$, then $B(x,x)[B(x,y) - B(y,x)] = 0$.

If some $B(u,v) \neq B(v,u)$ and $B(w,w) \neq 0$, then $B(u,u) = B(v,v) = 0, B(w,v) = B(v,w), B(w,u) = B(u,w)$, Let $x = u$ or v se get $B(w,v) = B(v,w) = 0 = B(w,u) = B(u,w)$. Now $B(u,w+v) \neq B(w+v,u)$, hence $B(w+v,w+v) = 0 = B(w,w)$, contradiction. □

Prop. (3.5.10.24). If B is a non-degenerate bilinear form on an associative algebra V, choose a basis $\{x_i\}$ of V, then choose a dual basis y_i, then $\sum x_i \otimes y_i \in T(V)$ is independent of x_i chosen. ⌟

Proof: Let $V^\vee$ be the dual of the vector space V. There is an isomorphism $V \otimes V^\vee \cong \mathrm{End}(V)$ given by mapping (v,f) to the operator $v' \mapsto f(v')v$. The non-degenerate bilinear form induces naturally an isomorphism $\beta : V \cong V^\vee : v \mapsto (\cdot, v)$. Then under the isomorphisms

$$\mathrm{End}(V) \cong V \otimes V' \cong V \otimes V,$$

where the second isomorphism is $(\mathrm{id}_V, \beta^{-1})$. The identity map $\mathrm{id}_V \in \mathrm{End}(V)$ is send to $\sum x_i \otimes y_i \in T(V)$, so $\sum x_i \otimes y_i$ is independent of the basis chosen. □

11 Positivity(Inner Spaces)

Def. (3.5.11.1) [Inner Spaces]. A **real inner space** is a f.d. real quadratic space that $B(v,v) \in \mathbb{R}_+$ for $v \neq 0$. It is necessarily non-degenerate.

A **complex inner space** is a f.d. Hermitian space V w.r.t. $\mathbb{C}/R$(3.5.10.13) s.t. $B(v,v) \in \mathbb{R}_+$ for $v \neq 0$. ⌟

Prop. (3.5.11.2). An inner metric on a vector space will induce an inner metric on the dual space, that is, asserting the dual basis of an orthonormal basis to be orthonormal. On an arbitrary basis, the matrix on the dual basis is written as A^{-1}. because we can write $A = P^tP$, and the dual basis transformation is like $(P^t)^{-1}$, so the metric matrix is A^{-1}. ⌟

Prop. (3.5.11.3) [Positivity and Principal Minors]. A matrix is positive symmetric(Hermitian) iff it is symmetric, and all its upper principle minors has positive determinants.

A positive symmetric(Hermitian) matrix is equivalent to a real(complex) inner space. ⌟

Proof: Cf.[Hoffman P328]. □

Prop. (3.5.11.4) [Positive Eigenvalues are Positive Real]. The spectrum of a Hermitian matrix(e.g. positive symmetric matrix) A is positive and real. ⌟

Proof: Let x be an eigenvector of A with eigenvalue λ, then λ is real by(3.5.10.17), and $0 < (x,x) = x^*Ax = \lambda x^*x$, so $\lambda > 0$. □

Prop. (3.5.11.5) [Positivity of Traces]. Let $A, B \in \mathrm{Pos}_{\geq 0}(n;\mathbb{R})$, $\mathrm{tr}(A) \geq 0$, and $\mathrm{tr}(AB) \geq 0$. ⌟

Proof: $\mathrm{tr}(A) \geq 0$ because we can write $A = P^{-1}DP$ where D is diagonal and P is orthogonal. Then the entries of D are non-negative, and $\mathrm{tr}(A) = \mathrm{tr}(D) \geq 0$.

Also, write $A = P^tP$, then $\mathrm{tr}(AB) = \mathrm{tr}(PBP^t) \geq 0$, because PBP^t is also a semi-positive matrix. □

Prop. (3.5.11.6) [Farkas' Lemma]. For a matrix A, and a vector b, exactly one of the following equation has a solution:

$$\begin{cases} AX = b, X \geq 0 \\ Y^t A \leq 0, Y^t b > 0 \end{cases}$$

⌟

Proof: First notice if both have a solution, then $0 \geq Y^t AX > 0$, contradiction. The rest follows form the Hahn-Banach separation theorem. □

Cor. (3.5.11.7) [Gordan's Theorem]. exactly one of the following has a solution:

$$\begin{cases} AX > 0 \\ Y^t A = 0, Y \geq 0, Y \neq 0 \end{cases}$$

⌟

Proof: If both have a solution, then $0 = Y^t AX > 0$, contradiction. If the first has no solution, then $A'x = e, z \geq 0$, where $A' = [A, -A, -I]$ has no solution, by Farkas' lemma, there is a solution of $Y^t A' \leq 0$ and $Y^t b = 0$. Which shows that $Y^t A = 0$ and $Y \neq 0$. □

Cor. (3.5.11.8). For any subspace in $\mathbb{R}^m$, either it has an intersection with the open first quadrant, or its orthogonal complement has an intersection with the closed first quadrant minus 0. (Regard it has the image of a AX). ⌟

12 (Real)Quaternion Algebra

Remark (3.5.12.1). The argument below are largely true for $\mathbb{R}$ replaced by any skew field. ⌟

Def. (3.5.12.2) [Real Quaternion Algebra]. The **real quaternion algebra** $\mathbb{H}$ is the space $\mathbb{R}\{1, i, j, k\}$ subjects to the relations

$$ij = -ji = k, jk = -kj = i, ki = -ik = j, i^2 = j^2 = k^2 = -1.$$

In fact, by(14.5.5.6), any quaternion algebra over $\mathbb{R}$ is isomorphic to $\mathbb{H}$. ⌟

Prop. (3.5.12.3) [Module of Quaternion Algebras]. There is an involution on $\mathbb{H}$ s.t. if $x = a + bi + cj + dk$, then $\overline{x} = a - bi - cj - dk$. Then we define a the modulus of $x \in \mathbb{H}$ as

$$|x|^2 = x\overline{x} = \overline{x}x = a^2 + b^2 + c^2 + d^2.$$

Then every non-zero element of $\mathbb{H}$ is invertible. In particular, it is a skew field. ⌟

Prop. (3.5.12.4). $\mathbb{H}$ is isomorphic to subalgebra of matrices in $\mathrm{Mat}(2; \mathbb{C})$ consisting of elements of the form

$$\{\begin{bmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{bmatrix} | \alpha, \beta \in \mathbb{C}\}$$

⌟

Prop. (3.5.12.5). The center of $\mathbb{H}$ is $\mathbb{R}$, by(14.5.4.3). ⌟

Prop. (3.5.12.6) [Invertible Quaternion Matrices]. Denote $\mathrm{GL}(n; \mathbb{H})$ the set of invertible matrices in $\mathrm{Mat}(n; \mathbb{H})$. If $A \in \mathrm{Mat}(n; \mathbb{H})$, A acts on $\mathbb{H}^n$, and determines a complex matrix A' in $\mathrm{Mat}(2n; \mathbb{C})$.

- If $A, B \in \mathrm{Mat}(n;\mathbb{H})$ satisfies $AB = 1$, then $BA = 1$.
- $A \in M = \mathrm{GL}(n;\mathbb{H})$ iff $A' \in \mathrm{GL}(2n;\mathbb{C})$. In particular if we define the determinant of $A \in \mathrm{Mat}(n;\mathbb{H})$ as the determinant of A', then $\det(A) \neq 0$ iff A is invertible.

⌟

Proof: 1: $(AB)' = A'B'$, thus $\mathrm{Mat}(n;\mathbb{H})$ is a subalgebra of $\mathrm{Mat}(2n;\mathbb{C})$. Thus $B'A' = 1$ by(3.5.7.9).

2: If A' is invertible, then A is a bijection, thus there are vectors $v_1, \ldots, v_n$ that $Av_i = e_i$. This means

$$(v_1, \ldots, v_n)A = 1.$$

Thus by item1 A is invertible. □

Def. (3.5.12.7) [Sesquilinear Form on $\mathbb{H}^n$]. Let $V = \mathbb{H}^n$, then a **sesquilinear form** on $\mathbb{H}^n$ is a bi-additive function $(-,-) : V \times V \to \mathbb{H}$ such that

$$(x\alpha, y\beta) = \overline{\alpha}(x, y)\beta, \quad \alpha, \beta \in \mathbb{H}.$$

Moreover if it is called a Hermitian form iff $(x, y) = \overline{(y, x)}$, and skew-Hermitian iff $(x, y) = -\overline{(y, x)}$. ⌟

Prop. (3.5.12.8) [Quaternion Hermitian Forms].

- Every non-degenerate Hermitian quaternion form is of the form

$$(x, y) = \overline{x}_1 y_1 + \ldots \overline{x}_p y_p - \overline{x_{p+1}} y_{p+1} - \ldots - \overline{x}_n y_n$$

  in some basis. And p is uniquely determined.

- Every non-degenerate skew-Hermitian quaternion form is of the form

$$(x, y) = \overline{x}_1 j y_1 + \ldots + \overline{x}_n j y_n$$

  in some basis.

⌟

Proof: Firstly, there are some v that $(v, v) \neq 0$: If $(v, v) = 0$ for all v, then $(x, y) + (y, x) = 0$ for all x, y. If it is skew-Hermitian, this means (x, y) is real, which is impossible, unless $(x, y) = 0$. If it is Hermitian, this means (x, y) is imaginary, but $(x, yi), (x, yj), (x, yk)$ are all imaginary, thus $(x, y) = 0$.

Then choose this v, and take the orthogonal complement of v, then by induction we can find $v_1, \ldots, v_n$ that is mutually orthogonal.

If it is Hermitian, then $(v_i, v_i) \in \mathbb{R}$, thus we can find some $t_i \in \mathbb{R}$ that $(tv_i, tv_i) = \pm 1$. $2p$ is the multiplicity of the eigenvalue 1 of the eigenspace of to the matrix corresponding to the form, so p is uniquely defined.

If it is skew-Hermitian, then (v_i, v_i) is imaginary, thus by(12.12.0.8), there are $u_i \in \mathbb{H}$ that $(u_i v_i, u_i v_i) = \overline{u}_i (v_i, v_i) u_i = j$. □

Cor. (3.5.12.9).

- Every non-degenerate Hermitian quaternion form is of the form

$$(x, y) = B_1(x, y) + jB_2(x, y)$$

  in some basis, where $B_1(x, y)$ is the usual canonical Hermitian form of signature $(2p, 2q)$, and B_2 is the usual canonical skew-symmetric bilinear form. Also $B_2(x, y) = B_1(xj, y)$.

- Every non-degenerate skew-Hermitian quaternion form is of the form

$$(x, y) = B_1(x, y) + jB_2(x, y)$$

in some basis, where $B_1(x, y)$ is the usual canonical skew-Hermitian form that iB_1 is Hermitian of signature $(n, -n)$, and B_2 is the usual canonical symmetric bilinear form. Also $B_2(x, y) = B_1(xj, y)$. in some basis.

⌟

13 Matrix Analysis

Thm. (3.5.13.1). Let $K \in \mathrm{Pos}_{\geq 0}(n, \mathbb{C})$, and the eigenvalues of K be $\kappa_1 \geq \kappa_2 \geq \ldots \geq \kappa_n \geq 0$(3.5.11.4), then for any $x \in \mathbb{C}^n$,

$$\kappa_n ||x||^2 \leq x^t K x \leq \kappa_1 ||x||^2.$$

⌟

Proof: By Principal Axis Theorem(3.5.10.18), we can assume that $K = U^{-1} \operatorname{diag}(\kappa_1, \ldots, \kappa_n) U$, where $U \in U(n)$. Then

$$\kappa_n ||x||^2 \leq \kappa_n ||Ux||^2 \leq x^t K x = x^t U^t \operatorname{diag}(\kappa_1, \ldots, \kappa_n) U x \leq \kappa_1 ||Ux||^2 = \kappa_1 ||x||^2$$

□

Thm. (3.5.13.2) [Weyl]. Let $\varphi : [0, \infty) \to \mathbb{R}$ be an non-decreasing function s.t. $\varphi(0) = 0$, and $\varphi(e^\xi)$ is a convex function of ξ. Suppose $A \in \mathrm{Mat}(n, \mathbb{C})$, and $K = A^* A$, and let the eigenvalues of A be $\alpha_1, \ldots, \alpha_n$ with $\lambda_i = |\alpha_i|^2$ satisfying $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$, and the eigenvalues of K be $\kappa_1 \geq \kappa_2 \geq \ldots \geq \kappa_n \in \mathbb{R}_+$(3.5.11.4).

Then for any $1 \leq m \leq n$,

$$\varphi(\lambda_1) + \ldots + \varphi(\lambda_m) \leq \varphi(\kappa_1) + \ldots + \varphi(\kappa_m).$$

In particular, for $s \in \mathbb{R}_+$,

$$\lambda_1^s + \ldots + \lambda_m^s \leq \kappa_1^s + \ldots + \kappa_m^s.$$

⌟

Proof: Notice first that by(11.3.13.4), it suffices to show that

$$\prod_{i=1}^m \lambda_i \leq \prod_{i=1}^m \kappa_i, \forall 1 \leq m \leq n.$$

Then notice $\prod_{i=1}^m \lambda_i$ is the largest module of eigenvalues of $\wedge^m A$, and $\prod_{i=1}^m \kappa_i$ is the largest eigenvalue of $(\mathrm{Sym}^m A)^* \operatorname{Sym} A$ by(3.5.5.4), so it reduces to show that $\lambda_1 \leq \kappa_1$. For this, notice that if $Ax = \alpha_1 x$, then $x^t K x = \lambda_1 ||x||^2$. But $x^t K x \leq \kappa_1 ||x||^2$(3.5.13.1), so we are done. □

Cor. (3.5.13.3). If $A \in \mathrm{GL}(n, \mathbb{C})$ is invertible, then we can apply the theorem to A^{-1} to show that: For any non-increasing function $\varphi : [0, infty) \to \mathbb{R}$ s.t. $\lim_{x \to \infty} \varphi(x) = 0$, and $\varphi(e^\xi)$ is a convex function of ξ, and any $1 \leq m \leq n$,

$$\varphi(\lambda_1) + \ldots + \varphi(\lambda_m) \leq \varphi(\kappa_1) + \ldots + \varphi(\kappa_m).$$

In particular, for $s \in \mathbb{R}_+$,

$$\frac{1}{\lambda_1^s} + \ldots + \frac{1}{\lambda_m^s} \leq \frac{1}{\kappa_1^s} + \ldots + \frac{1}{\kappa_m^s}.$$

⌟

14 Others

Prop. (3.5.14.1). Let $H^* = \oplus_{i=0}^{2d} H^i$ be a graded algebra over a field s.t. $\dim H^i < \infty$ for each i. Assume that for each $0 \le i \le 2d$, there is a perfect pairing

$$H^i \times H^{2d-i} \to K$$

induced from an isomorphism $\mathrm{tr} : H^{2d} \cong K$, Let φ be a ring endomorphism of H^* that satisfies

- $\varphi(H^i) \subset H^i$,
- $\varphi_{2d} = \mathrm{id}$

Then each φ_i is invertible, and $\varphi_i^{-1} = \varphi_{2d-i}^t$, where φ_{2d-i}^t is the transpose of φ_{2d-i} w.r.t. the perfect pairing $H^i \times H^{2d-i} \to K$. ⌟

Proof: Let $a \in H^i$ be any element, if $a \ne 0$, then because the pairing $H^i \times H^{2d-i} \to K$ is perfect, there exists some $b \in H^{2d-i}$ s.t. $ab \ne 0$. Thus $\varphi_i(a)\varphi_{2d-i}(b) \ne 0$, thus φ_i is injective. Now $\mathrm{tr}(\varphi_i^{-1}(a)b = \mathrm{tr}(\varphi_{2d}(\varphi_i^{-1}(a)b)) = \mathrm{tr}(a\varphi_{2d-i}(b))$, thus $\varphi_i^{-1} = \varphi_{2d-i}^t$. □

3.6 More on (Non-Commutative)Algebras

Main references are [Noncommutative Rings, T.Y.Lam], [?]Chap17 and [Sta]Chap11.

Notation (3.6.0.1).
- Use notations defined in Abstract Algebra.

⌟

1 Semisimplicity

Def. (3.6.1.1). For $R \in \mathcal{R}\mathrm{ing}$, a **simple R-module** is a $E \in \mathcal{M}\mathrm{od}_R$ that no submodules other than 0 and E. It is called **faithful** iff there is no nonzero element $a \in R$ that $ax = 0$ for any $x \in E$.
It is called **non-degenerate** if $RE = E$. ⌟

Prop. (3.6.1.2) [Shur's lemma]. For $R \in \mathcal{R}\mathrm{ing}$ and E a simple R-module, $\mathrm{End}_R(E)$ is a division ring, this is because the kernel and image are all 0 or E. ⌟

Cor. (3.6.1.3) [Uniqueness of Decomposition of Modules]. If an R-module E can be written as a finite direct sum of simple R-modules in multiple ways, then the multiplicity of the irreducible modules appearing in it is uniquely determined. ⌟

Proof: Cf.[Lang, Algebra, P643] □

Def. (3.6.1.4) [Semisimple Modules]. For $R \in \mathcal{R}\mathrm{ing}$, a **semisimple R-module** is a $E \in \mathcal{M}\mathrm{od}_R$ iff it satisfies the following equivalent conditions:
- It is a sum of simple modules.
- It is a direct sum of simple modules.
- Any submodule F of E has a complement in E.

⌟

Proof: 3 → 2: By Zorn's lemma, it suffices to show any non-zero semisimple module contains a simple submodule: Take a $m \neq 0 \in M$, then we may assume $M = Rm$, and by Zorn's lemma there is a maximal submodule N that $m \notin N$, and let $N \oplus N' = M$, then we show N' is simple. because any submodule N'' satisfies $m \in N \oplus N''$ thus $N'' = N'$.

2 → 1 is immediate, it suffices to show 1 → 3: for any submodule $N \subset M$, consider all the simple modules that intersect N trivially, denote their sum by V, I claim $N \oplus V = M$, otherwise, let S be a simple submodule that contained in $N + V$, then $S \cap (N + V) = 0$, so $N \cap (S + V) = 0$, contradicting the maximality. □

Cor. (3.6.1.5). For $R \in \mathcal{R}\mathrm{ing}$, any submodule and quotient module of a semisimple R-module is semisimple. ⌟

Proof: The quotient is clearly a sum of simple modules, and for a submodule, its submodule has a complement. □

Density Theorems

Def. (3.6.1.6). If E be a semisimple R-module, let $R' = \mathrm{End}_R(E)$, then E is also a R'-module, where the action is given by $(\varphi, x) \mapsto \varphi(x)$. Then any element of R defines an element of $\mathrm{End}_{R'}(E)$ by left multiplication. If we called $\mathrm{End}_{R'}(E)$ the **bicommutatant** of E over R, then ⌟

Lemma (3.6.1.7). For a module E over R, let $\mathrm{End}_{R'}(E)$ be the bicommutant. If $f \in \mathrm{End}_{R'}(E)$ and $x \in E$, then there is an element $\alpha \in R$ that $\alpha x = f(x)$. ⌟

Proof: Since E is semisimple, write $E = Rx \oplus F$, and let π be the projection unto Rx, then $\pi \in \mathrm{End}_R(E)$, and $f(x) = f(\pi(x)) = \pi f(x) \in Rx$. □

Prop. (3.6.1.8) [Jacobson Density Theorem]. Let E be semisimple over R and let $R' = \mathrm{End}_R(E)$. If $f \in \mathrm{End}_{R'}(E)$ and $x_1, \ldots, x_n \in E$, then there is an element $\alpha \in R$ that $\alpha x_i = f(x_i)$ for all i.

In particular, if E is f.g. over R', the natural map $R \to \mathrm{End}_{R'}(E)$ is surjective. ⌟

Proof: Consider $f^n \in \mathrm{End}_R(E^n)$, then it is just a $n \times n$ matrix with entries in $R' = \mathrm{End}_R(E)$. Consider the lemma(3.6.1.7) shows there is an $\alpha \in R$ that

$$(\alpha x_1, \ldots, \alpha x_n) = (f(x_1), \ldots, f(x_n))$$

which is the result. □

Cor. (3.6.1.9) [Wedderburn Theorem]. Let $R \in \mathcal{R}\mathrm{ing}$ and E is a faithful simple R-module. Let $D = \mathrm{End}_R(E)$. If E is of f.g. over D, then $R = \mathrm{End}_D(E)$. ⌟

Proof: The density theorem(3.6.1.8) and the fact E is f.g. over D shows that $R \to \mathrm{End}_k(E)$ is surjective, and also injective because it is faithful, thus $R = \mathrm{End}_k(E)$. □

Cor. (3.6.1.10) [Burnside's Theorem]. Let E is an R-module that is f.d over an alg.closed field k and R is a subalgebra of $\mathrm{End}_k(E)$. If E is simple as an R-module, then $R = \mathrm{End}_k(E)$. ⌟

Proof: It follows from Shur's lemma(3.6.1.2) and(3.2.1.10) $R' = \mathrm{End}_R(E)$ is just k, so we can use Wedderburn's theorem(3.6.1.9). □

Cor. (3.6.1.11) [F.d. Simple Module over Commutative Algebra]. If R is commutative and E is a simple R-module of f.d. over an alg.closed field k, then E is of 1-dimensional. ⌟

Proof: The theorem shows the image of R in $\mathrm{End}_k(E)$ is all of $\mathrm{End}_k(E)$, but Shur's lemma(3.6.1.2) and(3.2.1.10) that the image of R consists of scalars, thus $\dim_k E = 1$. □

Prop. (3.6.1.12) [Projection Operators]. Let k be a field and R is a k-algebra. If $V_1, \ldots, V_n$ are pairwise non-isomorphic simple R-modules of f.d. over k, then there exists elements e_i in R that acts as identity on V_i and 0 on other V_j. ⌟

Proof: This is an immediate consequence of Jacobson density theorem(3.6.1.8) applied to the projection operator on $\oplus_i V_i$. □

Prop. (3.6.1.13)[Characters Determine F.D. Representations(Bourbaki)]. Let R be an algebra over a field k of char0, E_1, E_2 be two f.d. semisimple R-module over k, then if the character $\chi_1 = \chi_2$, then the R-modules E_1, E_2 are isomorphic. ⌟

Proof: E, F are isomorphic to direct sums of simple R-modules, so it suffices to show the multiplicities m, n of any simple module V is the same. We can find an element e that is identity on E and 0 on other simple modules V_i by(3.6.1.12), thus the trace of e on E, F are $m \dim_k(V), n \dim_k(V)$ respectively, thus $m = n$ because k is of char0. □

Def. (3.6.1.14) [Matrix Coefficients]. For an algebra R and an R-module M over a field k, then a **matrix coefficient** of M is a function $c : R \to k$ of the form $c(r) = L(rx)$, where L is a linear functional on M and $x \in M$. ⌟

Cor. (3.6.1.15). If R is an algebra over a field k and two simple R-modules that is f.d. over k have a nonzero matrix coefficient in common, then they are isomorphic. ⌟

Proof: Let $c(r) = L_1(rx_1) = L_2(rx_2)$. If they are non-isomorphic, then we can find a $e \in R$ that is identity on M_1 and 0 on M_2 by(3.6.1.12). Let $c(u) \neq 0$, then

$$c(ue) = L_1(uex_1) = L_1(ux_1) = c(u) \neq 0, \quad c(ue) = L_2(uex_2) = L_2(0) = 0$$

contradiction. □

Prop. (3.6.1.16) [Simple Modules of Tensor Product]. Let A, B be algebras over a field Ω, $R = A \otimes B$, then:

- If P be a simple R-module of f.d. over Ω, then there is a simple A-module M and a simple B-module N that P is isomorphic to a quotient of $M \otimes N$. Also the isomorphism classes of M, N are uniquely determined.
- If Ω is alg.closed and M, N are simple modules of A, B of f.d. over Ω, then $M \otimes N$ is a simple module over $A \otimes B$.

⌟

Proof: 1: because P is f.d., it contains a simple A-module M. Let $N_1 = \mathrm{Hom}_A(M, P)$, then it is a B-module as A, B commutes in $A \otimes B$. Then we can define a map $\lambda : M \otimes N_1 \to P$, which is a $A \otimes B$-module morphism. Now N_1 is also of f.d., so it contains a simple B-module N, and λ is clearly non-zero on $M \otimes N$, thus its image is all of P, as P is simple.

For the uniqueness, let $d = \dim N$, then P is isomorphic to $k \leq d$ copies of M as an A-module, so the isomorphism class of M is determined, so does that of N.

2: Consider the map of A, B to $\mathrm{End}_\Omega(M), \mathrm{End}_\Omega(N)$ are surjective by(3.6.1.10). Then it suffices to show that $M \otimes N$ are simple over $\mathrm{End}_\Omega(M) \otimes \mathrm{End}_\Omega(N)$, but this is just $\mathrm{End}_\Omega(M \otimes N)$, over which $M \otimes N$ is clearly simple. □

Semisimple Rings and Simple Rings

Def. (3.6.1.17) [Semisimple Ring]. A (left)**semisimple** ring is a ring R s.t. it is a (left)semisimple module over itself. In(3.6.1.23), we will see a semisimple ring is semisimple in both sides. ⌟

Prop. (3.6.1.18). Any semisimple ring is left Artinian and Noetherian. ⌟

Proof: Consider the decomposition $R = \oplus_\alpha \mathfrak{A}_\alpha$, where $\mathfrak{A}_\alpha$ are simple left R-ideals. Then by considering the decomposition of $1 \in R$, clearly this is a finite sum. The rest is easy. □

Prop. (3.6.1.19). If R is a semisimple ring, then any R-module is semisimple. ⌟

Proof: Any R-module is a quotient of a free R-module, thus semisimple, by(3.6.1.5). □

Prop. (3.6.1.20). R is semisimple iff all R-modules are projective. ⌟

Proof: If R is left-semisimple, for any R-module P and an exact sequence

$$0 \to N \to M \to P \to 0$$

by(3.6.1.19), there is a complement of N in M, thus this sequence splits and P is projective. The converse is also clear that any submodule of any R-module has a complement. □

Lemma (3.6.1.21). Let D be a division ring and $R = \mathrm{Mat}(n; D)$, then

- R is simple, left semisimple and left Noetherian.
- R has a unique left simple module V, and R acts faithfully on V, with $R \cong nV$.
- $\mathrm{End}_R(V) \cong D$.

⌟

Proof: Cf.[Lam, P31]. □

Prop. (3.6.1.22) [Wedderburn-Artin]. Any left semisimple ring is of the form $R \cong \mathrm{Mat}(n_1, D_1) \times \ldots \times \mathrm{Mat}(n_r, D_r)$, and D_k are uniquely determined division rings. There are exactly r different left simple R-modules and D_i are uniquely determined. ⌟

Proof: Consider the decomposition

$$R \cong n_1 V_1 \oplus \ldots \oplus n_r V_r$$

where V_i are simple left R-modules. Then we can use Schur's lemma(3.6.1.2) and(3.6.1.21) to calculate the endomorphism ring, so

$$R \cong \mathrm{End}(n_1 V) \times \ldots \times \mathrm{End}(n_r V_r) \cong \mathrm{Mat}(n_1, D_1) \times \ldots \times \mathrm{Mat}(n_r, D_r).$$

For the uniqueness, we use(3.6.1.21), which shows D_i and V_i both can be recovered. □

Cor. (3.6.1.23). $R \in \mathcal{R}\mathrm{ing}$ is left semisimple iff it is right semisimple.((3.5.1.12) is used). ⌟

Cor. (3.6.1.24). A semisimple commutative ring is a finite direct product of fields. ⌟

Def. (3.6.1.25) [Semisimple Categories]. Let $k \in$ `Field` and $\mathcal{A}$ a k-linear Abelian category that $\mathrm{End}(X)$ are all finite k-modules for $X \in \mathcal{A}$, then $\mathcal{A}$ is semisimple iff $\mathrm{End}(X)$ is a semisimple k-algebra for any X. ⌟

Proof: If $\mathcal{A}$ is semisimple, then any $X \in \mathcal{A}$ is a direct sum of simple objects, so $\mathrm{End}(X)$ is semisimple.

Conversely, if $\mathrm{End}(X)$ is semisimple thus a product of matrix algebras over division algebras, so X can be indecomposable only if $\mathrm{End}(X)$ is a division algebra. Now if $f : M \to N$ is a morphism of indecomposable objects, if there is a map $g : N \to M$ that $g \circ f \neq 0$, then $g \circ f$ is an automorphism of M, and $(g \circ f)^{-1} \circ g$ is a right inverse to f, so N is a direct sum of M, and thus f is an isomorphism because M is indecomposable.

Now it suffices to show any indecomposable object is simple. If M is an indecomposable object properly contained in another indecomposable object, then

$$\begin{bmatrix} 0 & 0 \\ \mathrm{Hom}(M, N) & 0 \end{bmatrix} \subset \begin{bmatrix} \mathrm{End}(M) & \mathrm{Hom}(N, N) \\ \mathrm{Hom}(M, N) & \mathrm{End}(N) \end{bmatrix} = \mathrm{End}(M \oplus N)$$

is a two sided nilpotent nonzero ideal, contradicting the fact $\mathrm{End}(M \oplus N)$ is semisimple. □

Prop. (3.6.1.26) [Semisimplicity and Base Change]. If $A \in \mathcal{A}\mathrm{lg}_k$ and $A \otimes_k K$ is semisimple for some field extension K/k, then A is semisimple. Conversely, if A is semisimple, then $A \otimes_k K$ is semisimple for every separable field extension K/k. ⌟

Proof: Cf.[Milne, Lie Algebras, Lie Groups and Algebraic Groups]P48. □

Prop. (3.6.1.27) [Characters Determine F.D. Representations]. If R is a semisimple ring over a field k of characteristic 0, then its f.d. representations are determined by their characters, by(3.6.1.13). ⌟

Prop. (3.6.1.28) [Simple Artinian Algebras]. For a simple ring R(3.2.1.2), the following are equivalent:

- R is left semisimple.
- R is left Artinian.
- R has a minimal left ideal.
- $R \cong \mathrm{Mat}(n; D)$ for some division ring D.

⌟

Proof: The equivalence of $1, 4$ is by Wedderburn theorem(3.6.1.22) and(3.6.1.21). $2 \to 3$ is easy, and for $1 \to 2$, R is a finite direct sum of minimal ideals by Wedderburn theorem(3.6.1.22), so it is Artinian.

For $3 \to 1$, consider all the ideals in R that is isomorphic to the minimal ideal $\mathfrak{A}$, then it is also a right ideal of R, so equals R, hence R is semisimple. □

Cor. (3.6.1.29). And finite simple k-algebra A is of the form $\mathrm{Mat}(n; D)$ where D is a finite division ring over k. This is because A is clearly left Artinian. ⌟

Prop. (3.6.1.30) [Double Centralizer Property]. Let R be a simple ring and $\mathfrak{A}$ a nonzero left ideal. Let $D = \mathrm{End}_R(\mathfrak{A})$, then the natural map $f : R \to \mathrm{End}(\mathfrak{A}_D)$ is an isomorphism. ⌟

Proof: since R is simple, f is injective. To show it is surjective, let $E = \mathrm{End}(\mathfrak{A}_D)$, then for any $a, r \in \mathfrak{A}$ and $h \in E$, we have $h(ra) = h(r)a$, thus

$$(h \cdot f(r))a = h(ra) = h(r)a = f(h(r))a$$

which shows $f(R)$ is a left ideal in E. And because $\mathfrak{A}R = R$, we have $f(R) = f(\mathfrak{A})f(R)$, then

$$Ef(R) = Ef(\mathfrak{A})f(R) \subset f(\mathfrak{A})f(R) = f(R).$$

which shows $f(R)$ is a left ideal in E, and it contains 1, so $f(R) = E$. □

2 Jacobson Radical Theory

Def. (3.6.2.1) [Jacobson Radical]. For $R \in \mathfrak{Ring}$, the **Jacobson radical** is defined to be the intersection of all maximal left ideals in R.

R is called **Jacobson semisimple** if $\mathrm{rad}\, R = 0$.

R is called **semi-local** if $\overline{R} = R/\mathrm{rad}\, R$ is semisimple.

R is called **semi-primary** if R is semi-local and $\mathrm{rad}\, R$ is nilpotent. ⌟

Prop. (3.6.2.2) [Characterizing Jacobson Radicals]. For $y \in R$, the following are equivalent:

- $y \in \mathrm{rad}\, R$.
- $1 - xy$ is left-invertible for any $x \in R$.
- $yM = 0$ for any simple left R-module M.
- $1 - xyz$ is invertible for any $x, z \in R$.

⌟

Proof: $1 \to 2$: If $1 - xy$ is not left invertible, then it is contained in a maximal left ideal $\mathfrak{m}$, but $y \in \mathfrak{m}$, then $1 \in \mathfrak{m}$, contradiction.

$2 \to 3$: If $ym \neq 0$, then we must have $Rym = M$, so $xym = m$ for some $x \in R$, which shows $(1 - xy)m = 0$, but then $m = 0$.

$3 \to 1$: Consider the simple left R-module $R/\mathfrak{m}$ for any maximal left ideal $\mathfrak{m}$.

$4 \to 2$ is trivial, for $1 + 2 + 3 \to 4$: By item3 we know $\operatorname{rad} R$ is an ideal, so $yz \in \operatorname{rad} R$ and there is a u that $u(1 - xyz) = 1$. But then $u = 1 + u(xyz)$ is also left-invertible, so u is invertible and $1 - xyz$ is invertible. □

Cor. (3.6.2.3). $\operatorname{rad} R$ is the largest ideal $\mathfrak{A}$ of R that $1 + \mathfrak{A}$ are all units. In particular, the left radical agrees with the right radical. ⌟

Def. (3.6.2.4) [Locally Nilpotent Subsets]. A subset of a unital ring R is called **locally nilpotent** iff every element of it is nilpotent. ⌟

Lemma (3.6.2.5). if a left or right ideal $\mathfrak{A} \subset R$ is locally nilpotent, then $\mathfrak{A} \subset \operatorname{rad} R$. ⌟

Proof: Suppose $y \in \mathfrak{A}$, then $xy \in \mathfrak{A}$ is nilpotent. So $1 - xy$ has an inverse, for any x. Then $y \in \operatorname{rad} R$, by(3.6.2.2). □

Prop. (3.6.2.6) [Artinian Radical Nilpotent]. In a left Artinian ring, $\operatorname{rad} R$ is the largest nilpotent left ideal, and it is also the largest nilpotent right ideal. ⌟

Proof: By the above lemma, it suffices to show $J = \operatorname{rad} R$ is nilpotent. By Artinian property, the descending chain $J \supset J^2 \supset J^3 \supset \ldots$ is stabilizing, so there exists k s.t. $J^k = J^{k+1} = I$. Then $I = 0$, because otherwise we can choose a minimal non-zero left ideal $\mathfrak{A}$ s.t. $IA = 0$. Then if $a \neq 0 \in \mathfrak{A}$,

$$I(Ia) = I^2 a = Ia = 0,$$

so $\mathfrak{A} = Ia$, and $a = ya$ for some $y \in J$, so $(1 - y)a = 0$. But $1 - y$ is a unit by(3.6.2.2), contradiction. □

Cor. (3.6.2.7). In a left Artinian ring, any 1-sided locally nilpotent ideal is nilpotent. By left Artinian, there is a k that $(\operatorname{rad} R)^k = (\operatorname{rad} R)^{k+1} = I$. Now if $I \neq 0$, then we can choose a minimal left ideal $\mathfrak{A}$ that $I\mathfrak{A} \neq 0$ by Artinian property. Now there is an $a \in \mathfrak{A}$ that $Ia \neq 0$, so $I(Ia) = Ia \neq 0$, so $Ia = \mathfrak{A}$ and $a = ya$ for some $y \in I$. But $1 - y$ is invertible, so $a = 0$, contradiction. ⌟

Prop. (3.6.2.8) [Semisimplicity and Jacobson Semisimplicity]. For $R \in \mathfrak{Ring}$, the following are equivalent:

- R is semisimple.
- R is Jacobson semisimple and left Artinian.
- R is Jacobson semisimple and satisfies DCC on principal left ideals.

⌟

Proof: $1 \to 2$: R is left Artinian by(3.6.1.18), and consider $R = \operatorname{rad} R \oplus \mathfrak{B}$, then $\mathfrak{B}$ is contained in a maximal left ideal $\mathfrak{m}$, which cannot contain $\operatorname{rad} R$, unless $\operatorname{rad} R = 0$.

$3 \to 1$: 3 implies that ay left ideal $\mathfrak{A}$ contains a minimal left ideal I(the minimal principal one), and every minimal left ideal I is a direct summand of ${}_R R$(by choosing the maximal left ideal $\mathfrak{m}$ not containing I, because $I \oplus \mathfrak{m} = R$).

Then we can deduce 1: If R is not semisimple, then take a minimal left ideal $\mathfrak{B}_1$, then $R = \mathfrak{B}_1 \oplus \mathfrak{A}_1$, and $\mathfrak{A}_1 \neq 0$ otherwise R is semisimple, and we can choose a minimal left ideal $\mathfrak{B}_2 \subset \mathfrak{A}_1$, then $\mathfrak{A}_1 = \mathfrak{B}_2 \oplus \mathfrak{A}_2$. Continuing this way, we get a chain of left ideals $\mathfrak{A}_1 \supset \mathfrak{A}_2 \supset \ldots$, and they are both principal because they are direct summands of ${}_R R$, contradicting item3. □

Prop. (3.6.2.9) [Hokins-Levitzki Theorem]. Let R be a semi-primary ring(3.6.2.1), then for any R-module M, the following are equivalent:

- M is Noetherian.
- M is Artinian.
- M has a composition series.

In particular, a ring is left Artinian iff it is left Noetherian and semi-primary. ⌟

Proof: It suffices to prove if M is Noetherian or Artinian, M has a composition series. Denote $J = \operatorname{rad} R$, then J^n for some $n > 0$. We consider

$$0 \subset J^{n-1}M \subset \ldots \subset JM \subset M,$$

and the quotient $J^{k-1}M/J^kM$ is Artinian or Noetherian over $\overline{R} = R/\operatorname{rad} R$ which is semisimple, so it is a direct sum of simple modules, and the sum is finite, so there is a compostion series.

The last assertion: A left Artinian ring is semi-primary, by(3.6.2.6) and(3.6.2.8). So the assertion follows from the equivalence of item1 and 2. □

Lemma (3.6.2.10). Let $x \in \operatorname{rad} R$ where R is a k-algebra, then x is algebraic over k iff x is nilpotent. ⌟

Proof: One direction is trivial. For the other, if $x^r + a_1x^{r+1} + \ldots + a_nx^{r+n} = 0$, then because

$$1 + a_1x^1 + \ldots + a_nx^n$$

is invertible, we have $x^r = 0$. □

Prop. (3.6.2.11) [Amitsur]. Suppose k is a field and R is a k-algebra that $\dim_k R < |k|$, then $\operatorname{rad} R$ is the largest locally nilpotent ideal of R. ⌟

Proof: If $|k| < \infty$, then R is Artinian, so $\operatorname{rad} R$ is nilpotent by(3.6.2.6), and it is the largest by(3.6.2.6) again. Suppose now k is infinite. By the lemma above, it suffices to show every $r \in \operatorname{rad} R$ is algebraic over k. Notice that $a - r$ is invertible for $a \in k^*$, and $\{(a-r)^{-1}\}$ cannot be k-linearly independent because $\dim_k R < |k|$, so there is a dependence relation

$$\sum_{i=1}^n b_i(a_i - r)^{-1} = 0.$$

Hence r is algebraic over k. □

Prop. (3.6.2.12) [Amitsur]. Let R be a ring and $S = R[T]$. Let $J = \operatorname{rad} S$ and $N = R \cap J$, then N is a locally nilpotent ideal in R, and $J = N[T]$. In particular, if R is Jacobson semisimple, then S is also Jacobson semisimple(3.6.2.5). ⌟

Proof: Cf.[Lam, P71]. □

Lemma (3.6.2.13). Let $R \in \mathcal{R}\text{ing}/k$ and K/k is a separable algebraic field extension, then if R is Jacobson semisimple, so is $R \otimes_k K$. ⌟

Proof: Cf.[Lam, P76]. □

Prop. (3.6.2.14) [Jacobson Radical Under Base Change of Fields]. Let $R \in \mathcal{R}\text{ing}/k$ and K/k a separable algebraic extension, then $\text{rad}(R \otimes_k K) = (\text{rad}\, R) \otimes_k K$. ⌟

Proof: Cf.[Lam, P76]. □

3 Finite Semisimple k-Algebras

Reference for this subsection is [Sta]Chap 11.

Def. (3.6.3.1) [Azumaya Algebras]. A **central k-algebra** is an algebra A that the center of A is the image of $k \to A$. ⌟

Def. (3.6.3.2) [Azumaya Algebras]. An **Azumaya algebra** over k is defined to be a finite central k-algebra. The category of Azumaya algebras over k is denoted by Az_k. ⌟

Lemma (3.6.3.3). Let D be a division ring with central field k and $A \in \mathcal{R}\text{ing}/k$, then any two-sided ideal I of $A \otimes_k D$ is of the form $J \otimes_k D$ for some two-sided ideal J of A. In particular, if A is simple, then $A \otimes_k D$ is also simple. ⌟

Proof: Cf.[Sta]074C. □

Lemma (3.6.3.4). Let $R \in \mathcal{R}\text{ing}$ and $n \in \mathbb{Z}_+$, then

- The functors $M \mapsto M^{\oplus n}, N \mapsto e_{11}n$ defines an equivalence of categories between $\mathcal{M}\text{od}_R$ and $\mathcal{M}\text{od}_{\text{Mat}(n,R)}$.
- Any two-sided ideal of $\text{Mat}(n, R)$ is of the form $\text{Mat}(n, I)$ for some two-sided ideal I of R.
- Then center of $\text{Mat}(n, R)$ is the equal to the center of R.

⌟

Prop. (3.6.3.5). if A, A' are two simple k-algebras that A is finite central over k, then $A \otimes_k A'$ is simple. ⌟

Proof: Let A' be finite central over k, then by(3.6.1.28), $A' \cong \text{Mat}(n, D)$ for some finite central division algebra over k. Then

$$A \otimes_k A' \cong \text{Mat}(n, A \otimes D),$$

which is simple by(3.6.3.3) and(3.6.3.4). □

Cor. (3.6.3.6). The tensor product of two Azumaya k-algebras is an Azumaya k-algebra. ⌟

Proof: Combine the proposition with(3.2.1.15). □

Cor. (3.6.3.7) [Base Change]. If $k \in \texttt{Field}$ and $A \in \mathcal{R}\text{ing}/k$, then for any field extension k'/k, $A \otimes_k k' \in \text{Az}_{k'}$ iff $A \in \text{Az}_k$. ⌟

Proof: Combine(3.2.1.15) with(3.6.3.5). □

Prop. (3.6.3.8) [Skolem-Noether]. Let A be a finite central simple k-algebra and B is a simple k-algebra that $f, g : B \to A$ are two k-algebra homomorphisms. Then there exists an invertible element $x \in A$ that $f = x^{-1}gx$. ⌟

Proof: Choose a simple A-module M, then $L=\mathrm{End}_A(M)$ is a skew field, and M has two $B\otimes_k L^{op}$ structures by f and g. The k-algebra $B\otimes_k L^{op}$ is simple by(3.6.3.5), and also B is finite simple because there is a k-homomorphism $B\to A$, so $B\otimes_k L^{op}$ is finite simple, thus the two $B\otimes_k L^{op}$-structures on M are isomorphic, which means there is a $\varphi: M\to M$ intertwining these two structures. But φ commutes with L, meaning that φ is justing multiplying by some $x\in A$, so x is what we want. □

Cor. (3.6.3.9). Let A be a finite simple k-algebra, then any automorphism of A is inner. ⌟

Proof: Because the center of A is a finite field extension k' of k that A is central simple over k', thus the Skolem-Noether theorem applies. □

Splitting Fields

Prop. (3.6.3.10)[Centralizer Theorem]. Let $k\in\texttt{Field}$ and $A\in\mathrm{Az}_k$, and B a simple sub k-algebra of A, then

- $C=C_A(B)$ is also simple.
- $\dim_k A=\dim_k B\cdot\dim_k C$.
- $C_A(C)=B$.

⌟

Proof: Cf.[Sta]074T.**?** □

Cor. (3.6.3.11). Let $k\in\texttt{Field}$ and $B\subset A\in\mathrm{Az}_k$, then $C=C_A(B)$ is also in Az_k, and $A\cong B\otimes_k C$.

In particular, if a division ring D is of f.d. over its center k, then $D\in\mathrm{Az}_k$, and $\dim_k D$ is a square. ⌟

Proof: $\dim_k A=\dim_k(B\otimes_k C)$ by(3.6.3.10), and $B\otimes_k C$ is simple by(3.6.3.5), so the natural map $B\otimes_k C\to A$ is an isomorphism, and the center of C is k by(3.6.3.5). □

Prop. (3.6.3.12). For $k\in\texttt{Field}$, $A\in\mathrm{Az}_k$, If $K\subset A$ is a sub k-field, then the following are equivalent:

- $\dim_k A=[K:k]^2$.
- $C_A(K)=K$.
- K is a maximal commutative subring of A.

⌟

Proof: $1,2$ are equivalent by(3.6.3.10), and $2,3$ are clearly equivalent, as C_AK is a commutative subring containing K. □

Cor. (3.6.3.13). If D is a division ring with center k, then every maximal subfield of D satisfies $\dim_k D=[K:k]^2$. ⌟

Proof: This is because any commutative subring of A is a field. □

Def. (3.6.3.14)[Splitting Fields]. For $k\in\texttt{Field}$ and B a finite semisimple k-algebra, then B is said to **split** if B is isomorphic to a product of matrix algebras over k. A field extension K/k is called a **splitting field** of B if B_K is split. ⌟

Prop. (3.6.3.15). If $k\in\texttt{Field}, k=\overline{k}$, then any finite semisimple k-algebra is split. ⌟

Proof: This follows from(3.6.1.22) and(3.2.1.10). □

Cor. (3.6.3.16) [Central Simple Algebras are of Square Dimensions]. Let $k \in \texttt{Field}$, $A \in \mathrm{Az}_k$, then $\dim_k A$ is a square. ⌟

Proof: This is true because $A \otimes_k \overline{k}$ is a matrix algebra. □

Prop. (3.6.3.17) [Maximal Subfields are Splitting]. Let $k \in \texttt{Field}$, $A \in \mathrm{Az}_k$, k'/k a finite field extension, then k is a splitting field of A iff there exists a $B \in \mathrm{Az}_k$ similar to A(10.2.1.5) s.t. $k' \subset B$ and $\dim_k B = [k' : k]^2$.

In particular, if D is a division ring, any maximal subfield of D is a splitting field of D, by(3.6.3.12), ⌟

Proof: Cf.[Sta]074Z.? □

Cor. (3.6.3.18). If $k \in \texttt{Field}$ and D is a central division ring with $\dim_k D = d^2, d \in \mathbb{Z}_+$ by(3.6.3.16), then for any splitting field k'/k, $d|[k' : k]$. ⌟

Proof: By(3.6.3.17), there exists $B \in \mathrm{Az}_k$ similar to D s.t. $\dim_k B = [k' : k]^2$. Then it follows from(10.2.2.1) that $B \cong \mathrm{Mat}(n, D)$ for some $n \in \mathbb{Z}_+$. Then $n^2 d^2 = [k' : k]^2$, so $d|[k' : k]$. □

Prop. (3.6.3.19)[Galois Splitting Fields, Noether-Köthe]. If $k \in \texttt{Field}$ and D is a central division ring over k, then there exists a maximal subfield $K \subset D$ s.t. K/k is finite separable. In particular, by(10.2.2.1)(3.6.3.17), any central simple algebra has a finite Galois splitting field. ⌟

Proof: Notice it suffices to prove that: if $D \neq k$, there exists $\alpha \in D \backslash k$ s.t. $k(\alpha)/k$ is separable. This is because if we find such α, then $D' = C_D(k(\alpha))$ is another simple division algebra with center $k(\alpha)$, by(3.6.3.10), so we can use induction on $D'/k(\alpha)$.

We may assume k is non-perfect of characteristic $p \in \mathbf{P}$, thus an infinite field. Suppose we cannot find such an element, then every element satisfies an equation of the form $T^{p^r} - a = 0$, where $a \in k$. And because $\dim_k D < \infty$, there exists an r s.t. $x^{p^r} \in k$ for any $x \in D$. Then we can use the fact $\#k = \infty$ to show that $x^{p^r} \in \overline{k}$ for any $x \in D \otimes_k \overline{k}$. But then every p^r-th power of $D \otimes_k \overline{k} \cong \mathrm{Mat}(n, \overline{k})$ is central, which is not true, as $n > 1$ and we can take e_{11}. □

Cor. (3.6.3.20). Let $k \in \texttt{Field}$, then for $A \in \mathcal{R}\mathrm{ing}/k$, $A \in \mathrm{Az}_k$ iff $A \otimes_k k^{\mathrm{sep}} \cong \mathrm{Mat}(n, k^{\mathrm{sep}})$ for some $n \in \mathbb{Z}_+$, by(3.6.3.7). ⌟

Def. (3.6.3.21) [Reduced Degree]. For $k \in \texttt{Field}$ and B a finite semisimple k-algebra, suppose $B = \prod_i B_i$ where B_i are simple k-algebras with center k_i, define the **reduced degree** of B over k to be

$$[B : k]_{\mathrm{red}} = \sum_i [B_i : k_i]^{1/2} [k_i : k],$$

which is an integer by(3.6.3.16). And for any field extension k'/k,

$$[B_{k'} : k']_{\mathrm{red}} = [B : k]_{\mathrm{red}}.$$

⌟

Proof: To show it is invariant, pass to the algebraic closure, then $B = \prod_j \mathrm{Mat}(n_j, \overline{k})$, and $[B : k]_{\mathrm{red}} = \sum n_j$. □

Def. (3.6.3.22)[Reduced Norms]. Let $k \in \texttt{Field}$ and B an Azumaya k-algebra. If $x \in B$, let $P(T)$ be the characteristic polynomial of $r(T) : B \to B$, Then by passing to Galois splitting fields(3.6.3.19), we get $P(T) = Q(T)^n$ where $\dim_k B = n^2$. Then because there are Galois actions, we get $Q(T) \in k[T]$, and this $Q(T)$ is called the **reduced characteristic** of x. We can also routinely define **reduced norms** and **reduced trace**, denoted by $\mathrm{Nmrd}_{B/k}$ and $\mathrm{trrd}_{B/k}$.

Then this reduced characteristic is just the usual one when $B \cong \mathrm{Mat}(n; k)$. And when K is a splitting field of B containing x, then this equals the characteristic polynomial of x in K/k.

More generally, if B is a simple algebra over k with center L, then we can define $\mathrm{Nmrd}_{B/k} = \mathrm{Nm}_{K/k} \circ \mathrm{Nmrd}_{B/K}$ and $\mathrm{trrd}_{B/k} = \mathrm{tr}_{K/k} \circ \mathrm{trrd}_{B/K}$ ⌟

Proof: For the last assertion, notice $B = K \oplus Kx_1 \oplus \ldots Kx_n$ as modules over K. □

Prop. (3.6.3.23). For $k \in \texttt{Field}$ and B a finite semisimple k-algebra, any maximal étale k-subalgebra of B has rank $[B : k]_{\mathrm{red}}$ over k. ⌟

Proof: This follows from(3.6.3.13). □

Prop. (3.6.3.24). For $k \in \texttt{Field}$ and B a finite semisimple k-algebra, then for any faithful B-module M,

$$\dim_k M \geq [B : k]_{\mathrm{red}}.$$

And the equality holds iff B is split. ⌟

Proof: This is clear from(3.6.1.21). □

Prop. (3.6.3.25). If $k \in \texttt{Field}$ and $A \in \mathrm{Az}_k$, then $A \otimes_k A^{\mathrm{op}} \cong \mathrm{Mat}(n, k)$, where $n = \dim_k A$. ⌟

Proof: There is a map $A \otimes_k A^{\mathrm{op}} \to \mathrm{End}_k(A) : (a \otimes a') \mapsto (x \mapsto axa')$. By(3.6.3.6), $A \otimes_k A^{op}$ is simple, thus this is an injective map, but both sides have the same dimension, thus this is an isomorphism. □

Finite Semisimple k-Algebras with Involution

Def. (3.6.3.26) [Involution]. Let $*$ be an involution on a semisimple algebra B over a field k. It is called an **involution of first kind** if it fixes elements in the center of B. It is called an **involution of second kind** otherwise. ⌟

Prop. (3.6.3.27) [Decomposition]. Let $(B, *)$ be a f.d. semisimple k-algebra with an involution, if k is alg.closed and has characteristic 0, then it decomposes as products of pairs of the following types:

- $(A) : M_n(k) \times M_n(k), (a, b)^* = (b^t, a^t)$.
- $(C) : M_n(k), b^* = b^t$.
- $(BD) : M_{2n}(k), b^* = Jb^tJ^{-1}$, where $J = \begin{bmatrix} 0 & -I \\ I & 0 \end{bmatrix}$.

⌟

Proof: Let $B = B_1 \times \ldots \times B_r$ be the decomposition into products of simple k-algebras, where B^* are the minimal two-sided ideals of B. Applying $*$, $B = B_1^* \times \ldots \times B_r^*$ so B_i^* is a permutation of B_i, so B is a a product of algebras either simple or product of two simple algebras that $*$ interchanges them.

If B is simple, then $B \cong M_n(k)$ as k is alg.closed, so $b^* = ub^tu^{-1}$ for some $u \in M_n(k)$ by Skolem-Noether(3.6.3.8). Then $b = b^{**} = (u^tu^{-1})^{-1}bu^tu^{-1}$, so u^tu^{-1} is in the center, denote it by c, then

$u^t = cu$, $u = c^2u$, so $c = \pm 1$, and u is symmetric or skew-symmetric. Up to a congruence, we see the situation is (C) or (BD).

The other case is also easy. □

4 Idempotented Algebras

Lemma (3.6.4.1). Let R be a ring and e, f be idempotents of R that $ef = fe = e$, then $f = e + e'$, where e' is an idempotent and $M[f] = M[e] \oplus M[e']$.

Moreover, if R is an algebra over an alg.closed field k and $M[e]$ is a simple $R[e]$-module of f.d. over k, then $\dim \mathrm{Hom}_{R[e]}(M[e], M[f]) = 1$. ⌟

Proof: Let $e' = f - e$, then it is easily verified to be an idempotent, and $ee' = e'e = 0$, thus $M[f] = M[e] \oplus M[e']$ is clear.

For the second, because $R[e]$ acts by 0 in $R[e']$, $\mathrm{Hom}_{R[e]}(M[e], M[f]) = \mathrm{Hom}_{R[e]}(M[e], M[e])$ has dimension 1, by Shur's lemma(3.6.1.2) and(3.2.1.10). □

Def. (3.6.4.2) [Idempotented Algebra]. An **idempotented algebra** $\mathscr{H}$ is an algebra over a field k together with a set $\mathscr{E}$ of idempotents that if $e_1, e_2 \in \mathscr{E}$, then there exists $e_0 \in \mathscr{E}$ that

$$e_0e_1 = e_1e_0 = e_1, e_0e_2 = e_2e_0 = e_2,$$

and also for any $\varphi \in \mathscr{H}$, there exists $e \in \mathscr{E}$ that $e\varphi = \varphi e = \varphi$.

We can define a partial order on $\mathscr{E}$: $e < f$ iff $ef = fe = f$, then this order is cofinal.

If e is an idempotent, denote $\mathscr{H}[e] = e\mathscr{H}e$, which is a subring of $\mathscr{H}$ with unit e. Also if M is an $\mathscr{H}$-module, we denote $M[e]$ the $R[e]$-module eM. ⌟

Prop. (3.6.4.3). If $0 \to M_1 \to M_2 \to M_3 \to 0$ is an exact sequence of $\mathscr{H}$-modules, $e \in \mathscr{E}$, then $0 \to M_1[e] \to M_2[e] \to M_3[e] \to 0$ is also exact. ⌟

Proof: Because tensoring an idempotent is exact. □

Def. (3.6.4.4) [Smooth Representations of Idempotented Algebras]. Let $(\mathscr{H}, \mathscr{E})$ be an idempotented algebra, a **smooth $\mathscr{H}$-module** M is an $\mathscr{H}$-module $M = \cup_{e \in \mathscr{E}} M[e]$, and an **admissible $\mathscr{H}$-module** is a smooth $\mathscr{H}$-module that each $M[e]$ is of f.d. over k.

A smooth $\mathscr{H}$-module is clearly non-degenerate. ⌟

Def. (3.6.4.5) [Contragradient Module]. If M be a smooth $\mathscr{H}$-module, then we can define a **contragradient** $\widehat{M}$ of M, which is the smooth $\mathscr{H}$-module consisting of smooth vectors in M^*, where the action is defined as $((\varphi)\lambda)(m) = \lambda(\iota(\varphi)m)$. Notice if M is admissible, then so does $\widehat{M}$, because an element in $\widehat{M}[e]$ is determined by its restriction on $M[\iota(e)]$, so $\widehat{M}[e]$ is of f.d. if $M[\iota(e)]$ does. ⌟

Prop. (3.6.4.6) [Simpleness Checked on Idempotents]. Let M be a non-zero module over an idempotented algebra $(\mathscr{H}, \mathscr{E})$ over $\mathbb{C}$, $\mathscr{E}^0$ be a cofinal subset of $\mathscr{E}$, then M is a simple $\mathscr{H}$-module iff $M[e]$ is simple $\mathscr{H}[e]$-modules for any $e \in \mathscr{E}^0$. ⌟

Proof: If there exists a proper $\mathscr{H}$-submodule M_1 of M, let $M/M_1 = M_2$, then $M[e]/M_1[e] = M_2[e]$ for all e by(3.6.4.3), Thus we can choose e s.t. $M_1[e] \neq 0, M_2[e] \neq 0$, thus $M[e]$ is reducible. Conversely, If $W_0 \subset M[e_K]$ is a proper non-zero $\mathscr{H}[e_K]$-submodule, then $[\pi(\mathscr{H})W_0][e] = W_0$, thus $\pi(\mathscr{H})W_0$ is a proper submodule of M. □

Prop. (3.6.4.7) [Isomorphism Checked on Idempotents]. Let V_1, V_2 be two simple admissible modules over an idempotented algebra $(\mathscr{H}, \mathscr{E})$, if $e \in E$ that $V_1[e] \cong V_2[e] \neq 0$, then $V_1 \cong V_2$. ⌟

Proof: Choose an isomorphism $j: V_1[e] \to V_2[e]$, then the subspace $V' = \{(x, jx)\} \subset V_1[e] \oplus V_2[e] \subset V_1 \oplus V_2$ is a $\mathcal{H}[e]$-submodule. Let $V = \pi(\mathcal{H})V'$, then $V[e] = V'$, so V is not contained or contains any of V_1 or V_2, thus $V \cap V_1 = V \cap V_2 = 0$ as V_i are irreducible. Thus the projections $V \to V_1, V \to V_2$ are isomorphisms as V_i are irreducible, and $V_1 \cong V_2$. □

Prop. (3.6.4.8) [Extension Theorem]. Let $(\mathcal{H}, \mathcal{E})$ be an idempotented algebra and $e \in E$. If V_e is a simple $\mathcal{H}[e]$-module, then there is a simple $\mathcal{H}$-module V that $V[e] = V_e$. ⌟

Proof: Let $V_e \cong \mathcal{H}[e]/I$, where I is a left ideal of V_e. Let E_1, E_2 be the module generated by I and $\mathcal{H}[e]$ in $\mathcal{H}$ by left action of $\mathcal{H}$, then $E_1[e] = I$ and $E_2[e] = \mathcal{H}[e]$, thus $(E_3 = E_1/E_2)[e] \cong V_e$ by(3.6.4.3). Now if E' is a submodule of E_3, then either $E'[e] = 0$ thus $(E_3/E')[e] \cong L$, or $E'[e] = L$, thus $E' = E_3$ by(3.6.4.7). Thus if we choose the proper submodule E' that E_3/E' is irreducible by(18.1.2.8), then $E_3/E'[e] = L$. □

Prop. (3.6.4.9). If $\mathcal{H}$ is an idempotented algebra, then $\mathcal{M}(\mathcal{H})$ has enough projectives. ⌟

Proof: For any idempotent $e \in \mathcal{H}$, consider the module $\mathcal{H}e$, then it is projective, because $\mathrm{Hom}_{\mathcal{H}}(\mathcal{H}e, X) = eX$, thus it is clearly exact. Now any $m \in V$ has an idempotent $e \in \mathcal{H}$ that $ev = v$(use definition). Thus by taking the direct sum, we are done. □

Spherical Idempotents

Def. (3.6.4.10)[Spherical Idempotents]. Let $(\mathcal{H}, \mathcal{E})$ be an idempotented algebra over a field Ω. Then an idempotent $e \in \mathcal{E}$ is called **spherical idempotent** if there exists an anti-involution $\iota : \mathcal{H} \to \mathcal{H}$ that $\iota(x) = x$ for any $x \in \mathcal{H}[e^0]$. Notice this implies $\mathcal{H}[e^0]$ is commutative, as $xy = \iota(xy) = yx$. ⌟

Def. (3.6.4.11) [Spherical Vectors]. Let e^0 be a spherical idempotent of the idempotented algebra $(\mathcal{H}, \mathcal{E})$ and ι is the corresponding involution. If M is an admissible $\mathcal{H}$-module, then a **spherical(unramified) module** is a $\mathcal{H}$-module M that $M[e^0] \neq 0$, and elements in $M[e^0]$ are called **spherical vectors**.

Then if M is simple and spherical, then M has at most one spherical vector up to scalar, and $\widehat{M}$ is also spherical. Thus the space of spherical vectors is fixed by $\mathcal{H}[e^0]$, and the action of $\mathcal{H}[e^0]$ on that defines a **spherical character**. ⌟

Proof: In fact, $M[e^0]$ is a simple $\mathcal{H}[e^0]$-module(3.6.4.6), and is of f.d., and $\mathcal{H}[e^0]$ is commutative(3.6.4.10), so(3.6.1.11) shows it is of dimension 1. so if $m^0 \neq 0 \in M[e^0]$, then we can define a $\widehat{m}^0 \neq 0 \in \widehat{M}[e^0]$ as:

$$e^0 m = \widehat{m}^0(m) \cdot m^0.$$

□

Prop. (3.6.4.12) [Isomorphism Checked on Spherical Idempotents]. Let $(\mathcal{H}, \mathcal{E})$ be an idempotented algebra over a field Ω and e^0 is a spherical idempotent. If M, N are simple admissible spherical $\mathcal{H}$-modules that $M[e^0] \cong N[e^0]$ over $\mathcal{H}[e^0]$, then $M \cong N$ as $\mathcal{H}$-modules. ⌟

Proof: This follows from(3.6.4.7). □

Restricted Tensor Product

Def. (3.6.4.13) [Restricted Tensor Product]. Give an infinite number of vector spaces V_v indexed by a set Σ and elements $x_v^0 \in V_v$ be given for a.e. v, we can define the **restricted tensor product** $\bigotimes' V_v$ as the direct limit

$$\varinjlim_{S\subset\Sigma \text{ finite}} \otimes_{v\in S} V_v.$$

It can be thought of as the vector spaces spanned by all symbols $\otimes_v x_v$ where $x_v = x_v^0$ for a.e. v.

Notice if V_v are idempotented algebras and $x_v^0 \in V_v$ are idempotents for a.e. v, then $\prod' V_v$ also has a natural idempotented algebra structure. ⌟

Def. (3.6.4.14) [Tensor Product Module of Idempotented Algebras]. Given a set of idempotented algebras $(\mathscr{H}_v, \mathscr{E}_v)$ and specify an idempotent e_v^0 for a.e. v. Let M_v be $\mathscr{H}_v$-modules over k for all v, and assume $M_v[e_v^0]$ be of dimension 1 a.e. v, and specify a.e. a non-zero element $m_v^0 \in M_v[e_v^0]$

Then we can define tensor product(3.6.4.13) $\prod' \mathscr{H}_v$ which is an idempotented algebra and $\prod' M_v$. Then we can define an **restricted tensor module** structure of M_v over $\prod' \mathscr{H}_v$ by the action

$$(\otimes_v \varphi_v)x_v = \otimes_v(\varphi_v)x_v.$$

⌟

Lemma (3.6.4.15) [Simple Module of Tensor Product]. Let $(\mathscr{H}_1, \mathscr{E}_1), (\mathscr{H}_2, \mathscr{E}_2)$ be idempotented algebras over an alg.closed field Ω, and let $(\mathscr{H}, \mathscr{E})$ be the tensor product. If M_1, M_2 are simple admissible modules over $\mathscr{H}_1, \mathscr{H}_2$, respectively, then $M_1 \otimes M_2$ are simple admissible modules over $\mathscr{H}_1 \otimes \mathscr{H}_2$, and any simple admissible module over $\mathscr{H}$ comes uniquely from a pair (M_1, M_2) like this. ⌟

Proof: If M_1, M_2 are simple admissible over H_1, H_2 respectively, then if $e_1 \in \mathscr{E}_1, e_2 \in \mathscr{E}_2$, then $(M_1 \otimes M_2)[e_1 \otimes e_2] = M_1[e_1] \otimes M_2[e_2]$ is simple and of f.d. by(3.6.4.6) and(3.6.1.16), so $M_1 \otimes M_2$ is simple by(3.6.4.6).

Now if M is simple admissible over $\mathscr{H}_1 \otimes \mathscr{H}_2$, then we find an $e_1^0 \otimes e_2^0 \in \mathscr{E}$ that $M[e_1^0 \otimes e_2^0] \neq 0$. Let $\mathscr{E}_i^0 = \{e_i \in \mathscr{E}_i | e_i < e_i^0\}$, then $\mathscr{E}_i^0$ is cofinal in $\mathscr{E}_i$. Then for any $e_i \in \mathscr{E}_i^0$, $M[e_1 \otimes e_2]$ is non-zero thus simple, thus it is of the form

$$M[e_1 \otimes e_2] = M_1(e_1, e_2) \otimes M_2(e_1, e_2)$$

where $M_i(e_1, e_2)$ are simple $\mathscr{H}[e_i]$-modules by(3.6.1.16).

Now we show that $M_2(e_1, e_2)$ depends only on e_1: it suffices to show $M_2(e_1, e_2) = M_2(f_1, e_2)$ for $f_1 < e_1$. For this, notice that for any idempotents g_1, g_2,

$$M[g_1 \otimes g_2] = M_1(g_1, g_2) \otimes M_2(g_1, g_2)$$

is a finite direct sum of simple modules $M_2(g_1, g_2)$ as an $\mathscr{H}_2[g_2]$-module. Notice that by(3.6.4.1), $M[e_1 \otimes e_2] = M[f_1 \otimes e_2] \oplus M[e' \otimes e_2]$ for $e' = f_1 - e_1$, so by(3.6.1.3), $M_2(f_1, e_2) = M_2(e_1, e_2)$. Similarly we know $M_1(e_1, e_2)$ only depends on e_1.

Next we have:

$$\dim_k \operatorname{Hom}_{H_1[e_1]}(M_1[e_1], M_1[f_1]) \geq 1, \quad f_1 \leq e_1.$$

and similar for $\mathscr{H}_2$. For this, it suffices to prove that $\dim_k \operatorname{Hom}_{H_1[e_1]}(M[e_1 \otimes e_2], M[f_1 \otimes e_2]) \geq 1$, by what we just said, but this is by the decomposition

$$M[e_1 \otimes e_2] = M[f_1 \otimes e_2] \oplus M[e' \otimes e_2]$$

above. But

$$\dim_k \operatorname{Hom}_{H_1[e_1]\otimes H_2[e_2]}(M_1(e_1)\otimes M_2(e_2), M_1(f_1)\otimes M_2(f_2)) = 1, \quad f_1 \le e_1, f_2 \le e_2$$

by(3.6.4.1), so the $\geq$ above should change to $=$.

Now we know the homomorphism is of dimension 1, we want to choose a family of maps that is compatible for $g_1 \le f_1 \le e_1 \le e_1^0$. For this, we can choose the maps $\lambda(e_1, e_1^0)$ arbitrarily, then choose $\lambda(e_1, f_1)$ to be be compatible with $\lambda(e_1, e_1^0)$ and $\lambda(f_1, e_1^0)$, then these are compatible choices. Hence we can define a direct limit

$$M_1 = \varinjlim_{(\mathscr{E}^0)^{op}} M(e_1).$$

It is easy to see $M_1(e_1) \to M_1$ are all injective, and $M_1(e_1) = M[e_1]$. Similarly, we can define an M_2 that $M_2[e_2] = M_2(e_2)$.

Finally, we have

$$M[e_1 \otimes e_2] = M_1[e_1] \otimes M_2[e_2] = (M_1 \otimes M_2)[e_1 \otimes e_2]$$

for all $e_1 \in \mathscr{E}_1^0, e_2 \in \mathscr{E}_2^0$, thus $M \cong M_1 \otimes M_2$ by(3.6.4.7).

As for the uniqueness of M_1, M_2, notice the decomposition of $M[e_1 \otimes e_2]$ is unique by(3.6.1.16), so $M_i[e_i]$ is uniquely determined, thus by(3.6.4.7) M_i are determined. □

Prop. (3.6.4.16)[Flath Theorem]. let $(\mathscr{H}_v, \mathscr{E}_v)$ be an indexed family of idempotented k-algebras, and for a.e. v let $e_v^0 \in \mathscr{E}_v$ be a spherical idempotent. Let $(\mathscr{H}, \mathscr{E})$ be the restricted tensor product of $\mathscr{H}_c$ w.r.t. e_v^0, which is an idempotented algebra. For each $v \in \Omega$, there is a simple $\mathscr{H}_v$-module M_v and for a.e. v we specify a non-zero spherical vector. Let $\otimes_v M_v$ be the tensor product module, then it is a simple admissible $\mathscr{H}$-module, and every simple admissible module is of this type, with M_v uniquely determined. ⌟

Proof: Firstly the tensor product is simple and admissible: For any idempotent $e = \otimes e_v \in \mathscr{E}$, there is a finite set S that if $v \notin S$, then $e_v = e_v^0$, hence for these v $\dim M_v[e_v] = 1$. Then

$$M[e] = \otimes_{v\in S} M_v[e_v].$$

which is simple of f.d. by(3.6.4.15), so M is simple admissible by(3.6.4.6).

Conversely, for any simple $\mathscr{H}$-module M, we need to show it is a tensor product. If there are only f.m. indices, then this follows from(3.6.4.15).

Suppose first that e_v^0 is defined and spherical for all v, and $e = \otimes_v e_v^0$, and $M[e] \neq 0$. Then $\dim M[e] = 1$(3.6.4.11). Let m be a spherical vector, then there is a ring homomorphism $\gamma : \mathscr{H}[e] \to k$ defined by $hm = \gamma(h)m$. Because $\mathscr{H}[e] = \otimes_v' \mathscr{H}_v[e_v^0]$, we have

$$\gamma(\otimes_v h_v) = \prod_v \gamma_v(h_v).$$

Now if we decompose $\mathscr{H} = \mathscr{H}_v \otimes \mathscr{H}_v'$, then by(3.6.4.15), there exists simple admissible module M_v over $\mathscr{H}_v$, M_v' over $\mathscr{H}_v'$ respectively, that $M = M_v \otimes M_v'$, thus $M[e] = M_v[e_v^0] \otimes M_v'[e_v']$. Now consider M_v for all v, and $N = \otimes_v' M_v$ w.r.t. m_v, then it is simple admissible $\mathscr{H}$-module, and we have $N[e] = \otimes_v' M_v[e_v^0] \cong M[e]$ as $\mathscr{H}[e]$-modules of dimension 1, which is because they are both simple and have the same character

$$\gamma(\otimes_v h_v) = \prod_v \gamma_v(h_v).$$

Hence $M \cong N$, by(3.6.4.12).

Now the general case follows from the two situations above: choose $e \in \mathscr{E}$ that $M[e] \neq 0$, then let S be large that for $v \notin S$, $e_v = e_v^0$. Then we decompose $\mathscr{H}$ as $\mathscr{H} = \bigotimes_{v\in S} \mathscr{H}_v \otimes (\bigotimes_{v\notin S} H_v)$, then

$$M = \bigotimes_{v\in S} M_v \otimes M' = \bigotimes_{v\in S} M_v \otimes (\bigotimes_{v\notin S} M_v) = \otimes_v M_v.$$

□

5 Miscellaneous

Lemma (3.6.5.1). Let R be a (possibly non-commutative) unital ring of characteristic 0 with the following properties:

- R has no zero-divisors,
- $\operatorname{rank}_{\mathbb{Z}} R \leq 4$,
- R has an involution $(-)^\wedge : R \to R^{\mathrm{op}}$,
- For any $\alpha \in R$, $\alpha\widehat{\alpha} \in \mathbb{N}$, and $\alpha\widehat{\alpha} = 0$ iff $\alpha = 0$.

Then R is isomorphic to exactly one of the following:

- $\mathbb{Z}$.
- a $\mathbb{Z}$-order in an imaginary quadratic extension over $\mathbb{Q}$.
- a $\mathbb{Z}$-order in a definite quaternion algebra over $\mathbb{Q}$.

And the third case won't happen in characteristic 0, by(15.11.1.25). ⌟

Proof: It suffices to show $K = R \otimes \mathbb{Q}$ is either $\mathbb{Q}$, an imaginary quadratic field or a definite quaternion algebra. For $\alpha \in K$, denote $N\alpha = \alpha\widehat{\alpha}, \operatorname{tr}\alpha = \alpha + \widehat{\alpha}$, then $\operatorname{tr}\alpha = 1 + N\alpha - N(1-\alpha) \in \mathbb{Q}$.

Assume $K \neq \mathbb{Q}$, let $\alpha \in K \backslash \mathbb{Q}$. We may replace α by $\alpha - \frac{1}{2}\operatorname{tr}\alpha$ to assume $\operatorname{tr}\alpha = 0$, then $\alpha^2 = -N\alpha < 0 \in \mathbb{Z}$. So $\mathbb{Q}(\alpha)$ is an imaginary quadratic field.

Assume $K \neq \mathbb{Q}(\alpha)$, let $\beta \in K\backslash\mathbb{Q}(\alpha)$. We may replace β by $\beta - \frac{1}{2}\operatorname{tr}\beta - \frac{\operatorname{tr}(\alpha\beta)}{\alpha^2}\alpha$ to assume $\operatorname{tr}(\beta) = \operatorname{tr}(\alpha\beta) = 0$. Hence $\beta^2 = -N\beta < 0 \in \mathbb{Z}$, and $\alpha\beta = -\beta\alpha$. So $\mathbb{Q}(\alpha, \beta)$ is a definite quadratic extension of $\mathbb{Q}$. Then $K = \mathbb{Q}(\alpha, \beta)$ because they are has rank 4 over $\mathbb{Z}$. □

3.7 Lie Algebras

Basic references are [Car05], [Ser87], [Mil13], [Kna96] , [Lie Algebras and Lie Groups Serre], and [Eti21].

Notation (3.7.0.1).
- Let $k \in \texttt{Field}^0$.

⌟

1 Basics

Def. (3.7.1.1) [Lie Algebras]. A **Lie algebra** L is an non-associative algebra over a field k with a bilinear **Lie bracket** operation that satisfies:

$$[x, x] = 0, \quad [x[yz]] = [[xy]z] + [y[xz]](\text{Jacobi Identities}).$$

It is easily deduced that $[xy] = -[yx]$.
Denote $\mathrm{ad}x(y) = [xy]$, then $\mathrm{ad}x$ are all derivatives of L.
An element $x \in \mathfrak{g}$ is called **nilpotent** or **semisimple** if $\mathrm{ad}x$ is nilpotent or semisimple. ⌟

Prop. (3.7.1.2)[Associative Algebra]. For any associative algebra A over k, it can be given naturally a Lie algebra structure by defining $[xy] = xy - yx$. In this way, we get a natural functor $AssAlg_k \to Lie_k : A \mapsto [A]$. ⌟

Prop. (3.7.1.3) [Derivatives form a Lie Algebra]. Given a k-algebra A, the set of derivatives $\mathrm{Der}_k(A) = \mathrm{Der}_k(A, A)$ is a Lie algebra under the associative bracket. ⌟

Proof:

$$\begin{aligned}[D_1, D_2](ab) =& D_1(D_2(a)b + aD_2(b)) - D_2(D_1(a)b + aD_1(b))\\ =& D_1D_2(a)b + D_2(a)D_1(b) + D_1(a)D_2(b) + aD_1D_2(b)\\ &- (D_2D_1(a)b + D_1(a)D_2(b) + D_2(a)D_1(b) + aD_2D_1(b))\\ =& [D_1, D_2](a)b + a[D_1, D_2](b)\end{aligned}$$

□

Prop. (3.7.1.4) [Base Change of Fields]. Let $\mathfrak{a}$ be a subalgebra of a Lie algebra $\mathfrak{g}$ over k, and k'/k a field extension, then $\mathfrak{a}_{k'}$ is a subalgebra of $\mathfrak{g}_{k'}$, and

$$N_{\mathfrak{g}_{k'}}(\mathfrak{a}_{k'}) = N_{\mathfrak{g}}(\mathfrak{a})_{k'}.$$

$$c_{\mathfrak{g}_{k'}}(\mathfrak{a}_{k'}) = c_{\mathfrak{g}}(\mathfrak{a})_{k'}.$$

⌟

Proof: This is because the normalizer and centralizer is defined by linear equations with coefficients in k, thus the vector space is defined over k. □

Prop. (3.7.1.5). Let D be a derivative of a k-algebra A that is nilpotent, then e^D is an automorphism of A(as an algebra). ⌟

Proof: Routine calculation. □

Def. (3.7.1.6) [Semidirect Product of Lie Algebras]. Let $\mathfrak{g}, \mathfrak{h}$ be Lie algebras and $\tau : \mathfrak{g} \to \mathrm{Der}(\mathfrak{h})$, then we can define a **semi-direct product Lie algebra** $\mathfrak{g} \ltimes \mathfrak{h}$ that is isomorphic to $\mathfrak{g} \oplus \mathfrak{h}$ as vector spaces, and $\mathfrak{g}, \mathfrak{h}$ are subalgebras of $\mathfrak{g} \ltimes \mathfrak{h}$, with $[g, h] = \tau(g)(h)$. It can be shown that this is truly a Lie algebra. ┘

Def. (3.7.1.7) [Elementary Automorphisms]. Let $\mathfrak{g}$ be a Lie algebra, a **special automorphism** is an automorphism of $\mathfrak{g}$ of the form $e^{\mathrm{ad}_{\mathfrak{g}} x}$, where x is in the nilpotent radical(3.7.1.34).

The group of **elementary automorphisms** is the subgroup of the automorphism group of $\mathfrak{g}$ generated by the automorphisms of the form $e^{\mathrm{ad}_{\mathfrak{g}}(x)}$ where $\mathrm{ad}(x)$ is nilpotent. ┘

Def. (3.7.1.8) [Ideals]. A subspace $\mathfrak{a} \subset \mathfrak{g}$ is called an **ideal** of $\mathfrak{g}$ iff $[\mathfrak{g}, \mathfrak{a}] \subset \mathfrak{a}$. If I is an ideal of L, then L/I can be made into a Lie algebra by defining $[I + x, I + y] = I + [xy]$. ┘

Def. (3.7.1.9) [Center]. The **center** of a Lie algebra $\mathfrak{g}$ is the elements a that $\mathrm{ad}\, a = 0$. It is an ideal. ┘

Def. (3.7.1.10) [Simple Lie Algebras]. A Lie algebra $\mathfrak{g}$ is called **simple** if it is not 1-dimensional and it has no nontrivial ideal. ┘

Def. (3.7.1.11) [Lie Algebra of Affine Maps]. Let V be a f.d. k-vector space. If we regard V as a commutative algebra, then $\mathrm{Der}_k(V) = \mathrm{gl}_V$. Then $V \rtimes \mathfrak{gl}_V$ is a Lie algebra, denoted by $\mathrm{af}(V)$.

Let $V' = V \oplus k$, and let $\mathfrak{h} = \{w \in \mathfrak{gl}_{V'} | w(V') \subset V\}$, which is a Lie subalgebra of $\mathfrak{gl}_{V'}$. If we define

$$\eta : \mathfrak{h} \to \mathfrak{gl}_V : \eta(w) = w|_V, \quad \zeta : \mathfrak{h} \to V : \zeta(w) = w(0, 1),$$

then (η, ζ) defines a Lie algebra homomorphism from $\mathfrak{h}$ to $\mathfrak{af}(V)$. This map is bijective, with the inverse given by sending $(v, f) \in \mathfrak{af}(V)$ to the morphism

$$(v', c) \mapsto (f(v') + cv, 0).$$

┘

Lemma (3.7.1.12). Let $\lambda, \mu \in k$ and $x, y, z \in \mathfrak{g}$, then we have

$$(\mathrm{ad}(x) - \lambda - \mu)^m [y, z] = \sum_{i=1}^{m} \binom{m}{i} [(\mathrm{ad}(x) - \lambda)^i y, (\mathrm{ad}(x) - \mu)^{m-i} z].$$

┘

Proof:

$$\begin{aligned}(\mathrm{ad}(x) - \lambda - \mu)^m [y, z] &= \sum_{p+q+r+s=m} (-1)^{r+s} \frac{m!}{p!q!r!s!} \lambda^r \mu^s [(\mathrm{ad}\, x)^p (y), (\mathrm{ad}\, x)^q (z)] \\ &= \sum_{k+l=m} \frac{m!}{k!l!} [(\mathrm{ad}(x) - \lambda)^k y, (\mathrm{ad}(x) - \mu)^l z]\end{aligned}$$

□

Def. (3.7.1.13)[Killing Form]. A bilinear form B on $\mathfrak{g}$ is called **invariant** if $B([x,y],z)+B(x,[y,z]) = 0$.

The **Killing form** on a Lie algebra $\mathfrak{g}$ of f.d. is the invariant symmetric bilinear form defined by $B(x,y) = \mathrm{tr}(\mathrm{ad}x \circ \mathrm{ad}y)$.

if $\mathfrak{a}$ is an ideal of a Lie algebra $\mathfrak{g}$, then the Killing form on $\mathfrak{a}$ is that of the Killing form on $\mathfrak{a}$ as a Lie algebra. This is linear algebra. ⌟

Prop. (3.7.1.14). Any invariant symmetric bilinear form on a simple Lie algebra $\mathfrak{g}$ is a multiple of the Killing form. ⌟

Prop. (3.7.1.15). A subalgebra $\mathfrak{h}$ of a Lie algebra $\mathfrak{g}$ is commutative if it consists of semisimple elements. ⌟

Proof: For an element $x \in \mathfrak{h}$, we need to show that $\mathrm{ad}_{\mathfrak{h}}(x) = 0$. If it is not, because $\mathrm{ad}\,\mathfrak{h}(x)$ is semisimple by(3.5.8.8), there is a nonzero eigenvector y at least after a base change, so $[x,y] = cy, y \neq 0 \in \mathfrak{h}$. So $\mathrm{ad}(y)(x) = -cy$, and $\mathrm{ad}(y)^2(x) = 0$, so $\mathrm{ad}(y)$ is non-semisimple on the subspace $\{x,y\}$, which means $\mathrm{ad}(y)$ is non-semisimple on $\mathfrak{g}$, by(3.5.8.8) again. □

Lemma (3.7.1.16). If $\mathfrak{g} \subset \mathfrak{gl}_n$ is a Lie subalgebra, and $a \in \mathfrak{g}$ is a nilpotent matrix, then $\mathrm{ad}(a)$ is also nilpotent. ⌟

Proof: This is because $\mathrm{ad}(a) = l(a) - g(a)$, where $l(a)$ is left multiplication and $r(a)$ is right multiplication. The left and right multiplication commutes, so it is clear $\mathrm{ad}(a)^{2n} = 0$ if $\mathrm{ad}(a)^n = 0$. □

<u>**Nilpotent and Solvable Lie Algebras**</u>

Def. (3.7.1.17)[Nilpotent and Solvable Lie Algebras]. Let $\mathfrak{g}$ be a Lie algebra, the **lower central series** of $\mathfrak{g}$ is the descending sequence of ideals of $\mathfrak{g}$ defined inductively by $C^1\mathfrak{g} = \mathfrak{g}$ and $C^n\mathfrak{g} = [\mathfrak{g}, C^{n-1}\mathfrak{g}]$.

Let $\mathfrak{g}$ be a Lie algebra, the **derived series** of $\mathfrak{g}$ is the descending sequence of ideals of $\mathfrak{g}$ defined inductively by $D^1\mathfrak{g} = \mathfrak{g}$ and $D^n\mathfrak{g} = [D^{n-1}\mathfrak{g}, D^{n-1}\mathfrak{g}]$.

A Lie algebra is called **nilpotent** if there is an n that $C^n\mathfrak{g} = 0$. This is equivalent to $\mathrm{ad}x_1\mathrm{ad}x_2\ldots\mathrm{ad}x_n = 0$ for any n element $x-1,\ldots,x_n$. It is called **solvable** if $D^n = 0$ for some n. It is clear that $D^n \subset C^n$, so nilpotent Lie algebra is solvable. ⌟

Prop. (3.7.1.18). The lower central series satisfies: $[C^n\mathfrak{g}, C^m\mathfrak{g}] \subset C^{m+n}\mathfrak{g}$.

The operation of taking derived series or lower central series commutes with base change of fields. ⌟

Proof: Prove by induction on n: $n = 0,1$ is trivial, and if the assertion is true for $n \geq k$, then for $n = k+1$, $[C^n\mathfrak{g}, C^m\mathfrak{g}] \subset [\mathfrak{g}, [C^{n-1}\mathfrak{g}, C^m\mathfrak{g}]] + [C^{n-1}\mathfrak{g}, C^{m+1}\mathfrak{g}] \subset C^{m+n}\mathfrak{g}$. □

Cor. (3.7.1.19). Let $\mathfrak{g}$ be a Lie algebra over a field k, and k'/k is a field extension, then $\mathfrak{g}$ is solvable/nilpotent iff $\mathfrak{g} \otimes_k k'$ is solvable/nilpotent. ⌟

Prop. (3.7.1.20). If $\mathfrak{g}$ is a nilpotent Lie algebra, then for any subalgebra $\mathfrak{h} \subsetneq \mathfrak{g}$, $N_{\mathfrak{g}}(\mathfrak{h}) \neq \mathfrak{h}$. ⌟

Proof: Because $\mathfrak{g}^n = 0$ for some n, take n to be the maximal one that $\mathfrak{h} \not\subset \mathfrak{g}^n$, the $[\mathfrak{g}^n, \mathfrak{h}] \subset \mathfrak{g}^{n+1} \subset \mathfrak{h}$, so $\mathfrak{g}^n \subset N_{\mathfrak{g}}(\mathfrak{h})$, so $N_{\mathfrak{g}}(\mathfrak{h}) \neq \mathfrak{h}$. □

Prop. (3.7.1.21). Subalgebras, quotient algebras and extension algebras of solvable algebras are solvable. ⌟

Proof: Let $\mathfrak{h} \subset \mathfrak{g}$, then $D^n(\mathfrak{h}) \subset D^n(\mathfrak{g})$, so if $\mathfrak{g}$ is solvable, then so is $\mathfrak{h}$. Also the quotient is clearly solvable. For an extension of Lie algebras

$$0 \to \mathfrak{h} \to \mathfrak{g} \to \mathfrak{r} \to 0,$$

if $\mathfrak{h}, \mathfrak{r}$ are both solvable, let $D^m(\mathfrak{h}) = 0, D^n(\mathfrak{r}) = 0$, then the image of $D^n(\mathfrak{g})$ is 0 in $\mathfrak{r}$, so $D^n(\mathfrak{g}) \subset \mathfrak{h}$, so $D^{m+n}(\mathfrak{g}) = 0$. □

Cor. (3.7.1.22) [Radical]. If $\mathfrak{a}, \mathfrak{b}$ are solvable ideals of a Lie algebra $\mathfrak{g}$, then the ideal $\mathfrak{a} + \mathfrak{b}$ is also solvable, because $0 \to \mathfrak{a} \to \mathfrak{a} + \mathfrak{b} \to \mathfrak{b}/\mathfrak{a} \cap \mathfrak{b}$.

Let $\mathfrak{r} \subset \mathfrak{g}$ be the sum of all solvable ideals of $\mathfrak{g}$, called the **radical** $\mathrm{Rad}(\mathfrak{g})$. When $\mathfrak{g}$ is of f.d., this is the maximal solvable ideal. ⌟

Def. (3.7.1.23) [Semisimple Lie Algebra]. A Lie algebra L is called **semisimple** if $\mathrm{Rad}\ L = 0$, or equivalently $\mathfrak{g}$ has no solvable ideals or no commutative ideals. Notice $L/\mathrm{Rad}(L)$ is semisimple, by(3.7.1.22). ⌟

Prop. (3.7.1.24) [Lie]. Let $\mathfrak{g} \subseteq \mathfrak{gl}(V)$ be a solvable lie algebra over an alg.closed field k of char0, then $\mathfrak{g}$ is upper triangulable. Equivalently, there exists a vector $v \in V$ which is a common eigenvector for all $X \in \mathfrak{g}$, and moreover equivalently, any irreducible representation of $\mathfrak{g}$ is 1-dimensional. ⌟

Proof: Idea is to prove by induction on dimension of $\mathfrak{g}$.

Produce a codimension 1 ideal $\mathfrak{h}$ of $\mathfrak{g}$. Let $\mathfrak{g}$ be generated (as a vector space) by $\mathfrak{h}$ and Y. Being a subalgebra of solvable algebra $\mathfrak{g}$, $\mathfrak{h}$ is itself a solvable lie algebra. Apply induction step on $\mathfrak{h}$ and choose $v \in V$ such that v is an eigenvector for all $X \in \mathfrak{h}$.

The idea is to consider set W all common eigenvectors of elements of $\mathfrak{h}$ and produce an eigenvector of Y from this W. Let

$$W = \{v \in V | X(v) = \lambda(X)v \ \forall\ X \in \mathfrak{h} \text{ for a fixed } \lambda(X) \in \mathbb{C}\}.$$

Suppose W is an invariant subspace of Y, we then have restriction map $Y : W \to W$. As we are in complex vector space (algebraically closed) there exists an eigenvector for Y in W say w_0. Thus, w_0 is common eigenvector for all elements of $\mathfrak{g}$.

It remains to show that W is an invariant subspace of Y i.e., $Y(w) \in W$ for all $w \in W$ i.e., given $X \in \mathfrak{h}$, we need to have $X(Y(w)) = \lambda(X)Y(w)$.

Let $w \in W$, we have

$$\begin{aligned} X(Y(w)) &= Y(X(w)) + [X, Y](w) \\ &= Y(\lambda(X)w) + \lambda([X, Y])\, w \\ &= \lambda(X)Y(w) + \lambda([X, Y])\, w \end{aligned}$$

This is almost the same as what we want but with an extra term $\lambda([X, Y])\, w$. Suppose we prove $\lambda([X, Y]) = 0$ for all $X \in \mathfrak{h}$ then we are done.

Then considers subspace U spanned by elements $\{w, Y(w), Y^2(w), \cdots\}$ and then says that U is invariant subspace of each element of $\mathfrak{h}$ and (assuming n is the smallest integer such that $Y^{n+1}w$ is in the subsapce generated by $\{w, Y(w), \cdots, Y^n(w)\}$) representation of an element Z of $\mathfrak{h}$ with the basis $\{w, Y(w), \cdots, Y^n(w)\}$ is an upper triangular matrix with $\lambda(Z)$ in the diagonal. So, $\mathrm{tr}(Z) = n\lambda(Z)$.

So, $\mathrm{tr}([X, Y]) = n\lambda([X, Y])$. As $[X, Y] = XY - YX$, we have $\mathrm{tr}([X, Y]) = \mathrm{tr}(XY) - \mathrm{tr}(YX) = 0$. Thus, $\lambda([X, Y]) = 0$ and we are done. □

Cor. (3.7.1.25). If $\mathfrak{g}$ is a solvable algebra over an alg.closed field k of char 0, then all irreducible representations of $\mathfrak{g}$ is of dimension 1. ⌟

Cor. (3.7.1.26). $\mathfrak{g}$ is a solvable algebra iff $[\mathfrak{g},\mathfrak{g}]$ is nilpotent. ⌟

Proof: If $[\mathfrak{g},\mathfrak{g}]$ is nilpotent, then clearly $\mathfrak{g}$ is solvable. Conversely, if $\mathfrak{g}$ is solvable, we need to prove $[\mathfrak{g},\mathfrak{g}]$ is nilpotent. For this, we can assume k is alg.closed, and then $\mathrm{ad}(\mathfrak{g})\subset\mathfrak{b}_{\mathfrak{g}}$ for some basis, thus $\mathrm{ad}([\mathfrak{g},\mathfrak{g}])\subset\mathfrak{n}_{\mathfrak{g}}$ is nilpotent, and the kernel of ad is an Abelian subalgebra, so $[\mathfrak{g},\mathfrak{g}]$ is nilpotent. □

Cor. (3.7.1.27). If $\mathfrak{g}$ is a Lie subalgebra of $\mathfrak{gl}_n(k)$ where k is an alg.closed field of char0, then

$$\mathfrak{g}\text{ is solvable }\iff \mathrm{tr}(xy)=0,\ \forall x\in\mathfrak{g},y\in[\mathfrak{g},\mathfrak{g}].$$

⌟

Proof: Firstly if $\mathfrak{g}$ is solvable, then by Lie's theorem, we can assume $\mathfrak{g}\in\mathfrak{b}_V$ the upper-triangular matrices, so $[\mathfrak{g},\mathfrak{g}]\in\mathfrak{n}_V$ is nilpotent, and so $xy\in\mathfrak{n}_V$ is also nilpotent, and $\mathrm{tr}(xy)=0$.

Conversely, if $\mathrm{tr}(xy)=0$ for all $x\in\mathfrak{g},y\in[\mathfrak{g},\mathfrak{g}]$, we only need to prove $[\mathfrak{g},\mathfrak{g}]$ is solvable, so we may change $\mathfrak{g}$ to $[\mathfrak{g},\mathfrak{g}]$ and assume $\mathrm{tr}(xy)=0$ for all $x,y\in\mathfrak{g}$.

Now to show $\mathfrak{g}$ is solvable, it suffices to show $[\mathfrak{g},\mathfrak{g}]$ is nilpotent, or by Engel's theorem(3.7.1.29) all $x\in[\mathfrak{g},\mathfrak{g}]$ defines a nilpotent endomorphism on V. Choose a basis that x is upper-triangular by(3.5.8.3), and let x_s be the semisimple part of x, then it suffices to show $x_s=0$, or equivalently $\mathrm{tr}(\overline{x_s}x)=0$. To show this, notice $x\in[\mathfrak{g},\mathfrak{g}]$, so it suffices to show $\mathrm{tr}(\overline{x_s}[y,z])=0$ for any y,z. But this equals $\mathrm{tr}([\overline{x_s},y],z)$. Finally, this is 0 because of the hypothesis and the fact $\overline{x_s}$ is a polynomial in x(3.5.8.7) so $[\overline{x_s},y]\in\mathfrak{g}$. □

Cor. (3.7.1.28) [Cartan's Criteria for Solvability]. A Lie algebra $\mathfrak{g}$ over a field of characteristic 0 is solvable if $\kappa_{\mathfrak{g}}(x,y)$ for any $x\in\mathfrak{g},y\in[\mathfrak{g},\mathfrak{g}]$, where κ is the Killing form. ⌟

Proof: By(3.7.1.19), it suffices to show for k alg.closed. Because the kernel of the adjoint map is the center of $\mathfrak{g}$, so $\mathfrak{g}$ is solvable iff $\mathrm{ad}(\mathfrak{g})$ is solvable. □

Prop. (3.7.1.29) [Engel]. If (V,ρ) is a representation of a Lie algebra $\mathfrak{g}$ that $\rho(x)$ is nilpotent for all $x\in\mathfrak{g}$, then there is a basis that $\rho(\mathfrak{g})$ is contained in $\mathfrak{n}_V$, in particular $\mathfrak{g}$ is nilpotent. ⌟

Proof: It suffices to show if a sub-Lie algebra of $\mathfrak{gl}_V$ consists of nilpotent elements, then there is a common 0-eigenvector. Use Induction, choose a maximal subalgebra K of L, then notice the normalizer of K in L is strictly containing K, because we can let K acts by adjoint on L/K, and notice $\mathrm{ad}\,x=\lambda_x-\rho_x$ is nilpotent for x a nilpotent matrix, so by induction hypothesis there is an $x\in L$ that $[x,K]\subset K$. But K is maximal, so it must be of codimension 1, and $L=K+Fz$. The 0-eigenvectors for K is a nonzero subspace by induction hypothesis. Now this space is invariant under z: for any $h\in K$,

$$h(z(v))=[h,z](v)+zh(v)=0.$$

So now a 0-eigenvector for z in this space will suffice. □

Cor. (3.7.1.30). If all elements of L are ad-nilpotent(i.e. $\mathrm{ad}x=0$), then L is nilpotent. Equivalently, elements of L has a common 0-eigenvector. ⌟

Proof: Consider $ad:\mathfrak{g}\to\mathfrak{gl}_{\mathfrak{g}}$, then the image is nilpotent by Engel's theorem(3.7.1.29), and the kernel of ad is the center of $\mathfrak{g}$, so $\mathfrak{g}$ is also nilpotent. □

Cor. (3.7.1.31). Let $\mathfrak{a}$ be an ideal of a Lie algebra $\mathfrak{g}$. Then $\mathfrak{a}$ is nilpotent if $\mathrm{ad}_{\mathfrak{g}}(a)$ is nilpotent for any $a \in \mathfrak{a}$. ⌟

Proof: If $\mathrm{ad}_{\mathfrak{g}}(a)$ is nilpotent for any $a \in \mathfrak{a}$, then also $\mathrm{ad}_{\mathfrak{a}}(a)$ is nilpotent, so $\mathfrak{a}$ is nilpotent by Engel's theorem. Conversely, if $\mathfrak{a}$ is nilpotent, then $\mathrm{ad}_{\mathfrak{a}}(a)$ is nilpotent for any $a \in \mathfrak{a}$. And $\mathrm{ad}(a)(\mathfrak{g}) \subset \mathfrak{a}$, so $\mathrm{ad}_{\mathfrak{g}}(a)$ is nilpotent. □

Cor. (3.7.1.32). The sum of two nilpotent ideals of $\mathfrak{g}$ is nilpotent. ⌟

Proof: We need to show for any $a \in \mathfrak{a}, b \in \mathfrak{b}$, $\mathrm{ad}_{\mathfrak{g}}(a+b)$ is nilpotent. For this, we need to factor $\mathfrak{g}$ as Jordan sequence $0 \subset \mathfrak{g}_1 \subset \mathfrak{g}_2 \subset \ldots \subset \mathfrak{g}_n = \mathfrak{g}$ over itself via the adjoint representation, then I claim that $\mathrm{ad}(a)(\mathfrak{g}_k) \subset \mathfrak{g}_{k-1}$: Because $V = \mathfrak{g}_k/\mathfrak{g}_{k-1}$ is simple, let $V' \subset V$ consists of vectors v that $a(v) = 0$ for any $a \in \mathfrak{a}$, then it is non-empty by Engel's theorem, and also it is invariant under action of $\mathfrak{g}$: $a(gv) = [a, g](v) + g(av) = 0$. So it is all of V.

Then, we have $\mathrm{ad}(a+b)(\mathfrak{g}_k) \subset \mathfrak{g}_{k-1}$, thus $\mathrm{ad}(a+b)$ is nilpotent. □

Cor. (3.7.1.33) [Maximal Nilpotent Ideal]. For any Lie algebra $\mathfrak{g}$, there exists a maximal nilpotent ideal, denoted by $\mathfrak{n}$. ⌟

Def. (3.7.1.34) [Nilpotent Radical]. The **nilpotent radical** $\mathfrak{s} = s(\mathfrak{g})$ of a Lie algebra is the intersection of the kernels of simple representations of $\mathfrak{g}$.

$\mathfrak{s}$ is nilpotent for any f.d. representation of $\mathfrak{g}$, in particular the adjoint representation of $\mathfrak{g}$. Thus it is nilpotent, by(3.7.1.31). ⌟

Lemma (3.7.1.35). Let $\mathfrak{g} \subset \mathfrak{gl}_V$ be a subalgebra, and let $\mathfrak{a}$ a commutative ideal of $\mathfrak{g}$. If V is simple as a $\mathfrak{g}$-module, then $[\mathfrak{g}, \mathfrak{g}] \cap \mathfrak{a} = 0$. ⌟

Proof: Cf.[Mil13]P58. □

Prop. (3.7.1.36). Let $\mathfrak{g}$ be a Lie algebra, and $\mathfrak{r}$ its radical, $\mathfrak{s}$ it nilpotent radical, then

$$\mathfrak{s} = D(\mathfrak{g}) \cap \mathfrak{r} = [\mathfrak{g}, \mathfrak{r}].$$

In particular, $[\mathfrak{g}, \mathfrak{r}]$ is nilpotent(3.7.1.34). ⌟

Proof: To show $D(\mathfrak{g}) \cap \mathfrak{r} \subset \mathfrak{s}$, we need to show that $\rho(D(\mathfrak{g}) \cap \mathfrak{r}) = 0$ for any simple representation ρ. Because $\mathfrak{r}$ is solvable, let r be the smallest integer that $\rho(D^{r+1}(\mathfrak{r})) = 0$, then $\mathfrak{a} = \rho(D^r(\mathfrak{r}))$ is a commutative ideal of $\rho(\mathfrak{g})$. Hence by(3.7.1.35) $D(\rho(\mathfrak{g})) \cap \mathfrak{a} = 0$, so $\rho(D(\mathfrak{g}) \cap D^r(\mathfrak{r})) = 0$. Now if $r > 0$, then $\rho(D^r(\mathfrak{r})) = 0$, contradicting the minimality of r, so $\rho(D(\mathfrak{g}) \cap \mathfrak{r}) = 0$.

To show $\mathfrak{s} \subset [\mathfrak{g}, \mathfrak{r}]$, let $\mathfrak{q} = \mathfrak{g}/[\mathfrak{g}, \mathfrak{r}]$, and f the quotient map. Then because the kernel is solvable, $f(\mathfrak{r})$ is the radical of $\mathfrak{q}$(3.7.1.22), but it is also contained in the center of $\mathfrak{q}$, so $\mathfrak{q}$ is reductive, and thus has a faithful semisimple representation(3.7.4.4), then the kernel of this representation is just $[\mathfrak{g}, \mathfrak{r}]$, showing that $\mathfrak{s} \subset [\mathfrak{g}, \mathfrak{r}]$. □

Def. (3.7.1.37) [Levi Subalgebras]. Let $\mathfrak{g}$ be a Lie algebra and $\mathfrak{r}$ its radical, then a Lie subalgebra $\mathfrak{s}$ is called a **Levi subalgebra** if $\mathfrak{g} = \mathfrak{r} \oplus \mathfrak{s}$. ⌟

Prop. (3.7.1.38) [Levi-Malcev]. Every Lie algebra over a field k of char0 has a Levi subalgebra, and any two Levi subalgebras of $\mathfrak{g}$ are conjugate by a special automorphism of $\mathfrak{g}$(3.7.1.7). ⌟

Proof: If $\mathfrak{g}$ is reductive, then Levi subalgebra exists uniquely, by(3.7.4.2) and(3.7.4.3).

if $\mathfrak{r}$ is a minimal ideal of $\mathfrak{g}$, then $[\mathfrak{g},\mathfrak{r}]=\mathfrak{r}$, and $[\mathfrak{r},\mathfrak{r}]=0=Z(\mathfrak{g})$. Consider the adjoint action of $\mathfrak{g}$ on $\mathrm{End}_k(\mathfrak{g})$. Also consider the subspaces V,W of $\mathrm{End}_k(\mathfrak{g})$, where V is the subspace of maps from $\mathfrak{g}$ to $\mathfrak{r}$ that restriction to $\mathfrak{r}$ is a constant multiple of identity, and W is the subspaces of W consisting of maps vanishing on $\mathfrak{r}$. Both of V,W are invariant under action of $\mathfrak{g}$.

Let $\varphi:\mathfrak{r}\to\mathfrak{g}$ be the adjoint action, which is injective and has image $P\subset W$. Also $\mathfrak{P}$ is invariant under action of $\mathfrak{g}$(because $\mathfrak{r}$ is an ideal).

For $x\in\mathfrak{r},y\in\mathfrak{g},\alpha\in V$, $(x\alpha)(y)=[x,\alpha(y)]-\alpha([x,y])=-\lambda(\alpha)[x,y]$, so $x\alpha=\mathrm{ad}(\lambda(\alpha)x)$, which means elements of $\mathfrak{r}$ map V into P. Thus now $\mathfrak{r}$ acts trivially on V/P, and W/P is invariant under the action of $\mathfrak{g}/\mathfrak{r}$, which is a semisimple Lie algebra. Thus by Weyl's theorem(18.8.1.2), there exists a $\mathfrak{g}$-stable line L that $V/P=W/P\oplus L$. But $\mathfrak{g}$ acts trivially on L by(18.8.1.1).

Let α_0 generates L and normalized that $\lambda(\alpha)=1$, then $\mathfrak{g}\alpha_0\in P$, We consider the map $\mathfrak{g}\xrightarrow{g\mapsto g\alpha_0} P\xrightarrow{\varphi^{-1}}\mathfrak{r}$, whose restriction to $\mathfrak{r}$ is the identity map, so its kernel is a Levi subgroup for $\mathfrak{r}$.

Still in this case, let $\mathfrak{s}'$ be a second Levi subgroup for $\mathfrak{r}$. For each $x\in\mathfrak{s}'$, there is a unique $h(x)\in\mathfrak{r}$ that $x+h(x)\in\mathfrak{s}$. Hence this h satisfies $h([x,y])=[h(x),y]+[x,h(y)]$. But then by(18.8.1.3), $h(x)=[a,x]$ for some $a\in\mathfrak{r}$. Then $1+\mathrm{ad}(a)$ maps $\mathfrak{s}$ to $\mathfrak{s}'$, and $\mathrm{ad}(a)^2=0$ because $\mathfrak{r}$ is commutative. And $\mathfrak{r}=[\mathfrak{r},\mathfrak{g}]$, so a is in the nilpotent radical of $\mathfrak{g}$, thus $\mathfrak{s},\mathfrak{s}'$ are conjugate by a special automorphism.

For the general case, we can use induction on the dimension of $\mathfrak{g}$. After the first two cases, we can assume that $[\mathfrak{g},\mathfrak{r}]\neq 0$ and $\mathfrak{r}$ contains a proper non-trivial ideal. As $[\mathfrak{g},\mathfrak{r}]$ is nilpotent(3.7.1.36), its center is non-zero. So we can choose a maximal ideal $\mathfrak{m}$ contained in the center of $[\mathfrak{g},\mathfrak{r}]$, and $\mathfrak{m}\neq\mathfrak{r}$. Now $\mathfrak{g}/\mathfrak{m}$ has radical $\mathfrak{r}/\mathfrak{m}$ because $\mathfrak{m}$ is solvable, so we can apply induction to find a Levi subgroup $\mathfrak{h}'$ for $\mathfrak{g}/\mathfrak{m}$ in $\mathfrak{g}/\mathfrak{m}$, and let $\mathfrak{h}''$ be its preimage in $\mathfrak{g}$. Then $\mathfrak{h}''$ has radical $\mathfrak{m}$, and thus by induction there is a Levi subgroup $\mathfrak{h}$ for $\mathfrak{m}$ in $\mathfrak{h}''$, and this $\mathfrak{h}$ is a Levi subgroup for $\mathfrak{r}$ in $\mathfrak{g}$. Similarly any two such Levi subgroups are conjugate by a special automorphism.

This has another cohomological proof in [Etingof, Section48].? □

2 Semisimple Lie Algebra

Prop. (3.7.2.1) [Cartan-Killing Criteria for Semisimplicity]. A f.d. Lie algebra $\mathfrak{g}$ is semisimple iff its Killing form(3.7.1.13) is non-degenerate. ⌟

Proof: If $\mathfrak{g}$ is semisimple, then the adjoint representation is faithful, thus by(3.7.9.6) the Killing form is non-degenerate. Conversely, if the Killing form is non-degenerate and $\mathfrak{a}$ is a commutative ideal of $\mathfrak{g}$ and $a\in\mathfrak{a},g\in\mathfrak{g}$, then $(\mathrm{ad}\,a\circ\mathrm{ad}\,g)^2=0$, so $\mathrm{ad}\,a\circ\mathrm{ad}\,g$ is nilpotent and has trace 0. so $a\in\mathfrak{g}^\perp$, which is 0 because the Killing form is non-degenerate. □

Cor. (3.7.2.2). Let $\mathfrak{a}$ be a semisimple ideal of a Lie algebra $\mathfrak{g}$, then the orthogonal space $\mathfrak{a}'$ w.r.t the Killing form is an ideal and is a complement for $\mathfrak{a}$ in $\mathfrak{g}$, and $\mathfrak{g}\cong\mathfrak{a}\times\mathfrak{a}'$. ⌟

Proof: $\mathfrak{a}^\perp$ is an ideal because the Killing form is invariant. The Killing form of $\mathfrak{a}$ is the restriction of the Killing form of $\mathfrak{g}$(3.7.1.13), so $\mathfrak{a}\cap\mathfrak{a}'=0$ because $\kappa_{\mathfrak{a}}$ is non-degenerate. □

Cor. (3.7.2.3). A Lie algebra is semisimple iff it is isomorphic to a product of simple algebras $\mathfrak{g}=\mathfrak{a}_1\times\cdots\times\mathfrak{a}_r$, and these $\mathfrak{a}_i$ are all its minimal ideals, (Not only up to isomorphism). ⌟

Proof: The Killing form of $\mathfrak{a}\cap\mathfrak{a}^\perp$ is 0, thus it is solvable, by(3.7.1.28), and then 0, so we can continue the decomposition.

For any minimal nonzero ideal $\mathfrak{a} \subset \mathfrak{g}$, then $[\mathfrak{g}, \mathfrak{a}]$ is an ideal contained in $\mathfrak{a}$. which is nonzero because $\mathfrak{g}$ has trivial center. Then
$$\mathfrak{a} = [\mathfrak{g}, \mathfrak{a}] = \oplus_i [\mathfrak{a}, \mathfrak{a}_i]$$
so $\mathfrak{a} \subset [\mathfrak{a}, \mathfrak{a}_i] \subset \mathfrak{a}_i$, and then $\mathfrak{a} = \mathfrak{a}_i$ by simplicity. □

Cor. (3.7.2.4). If $\mathfrak{g}$ is semisimple, then $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{g}$. ⌟

Cor. (3.7.2.5). Let $\mathfrak{g}$ be a Lie algebra over a field k and k'/k is a field extension, then $\mathfrak{g}$ is semisimple iff $\mathfrak{g} \otimes_k k'$ is semisimple. ⌟

Prop. (3.7.2.6) [Examples of Semisimple Lie Algebras].
- The subalgebra $\mathfrak{sl}(V)$ of all elements of $\mathrm{End}(V)$ of trace 0 is semisimple.

⌟

Prop. (3.7.2.7). If L is semisimple, then every derivative of L is inner. ⌟

Proof: This is a special case of(18.8.1.3) applied to the adjoint representation. □

Prop. (3.7.2.8). If $\mathfrak{g}$ is a semisimple algebra of $\mathfrak{gl}_n(k)$ where k is a field of char0, then it contains the semisimple and nilpotent parts of each of its elements under the Jordan decomposition(3.5.8.7). ⌟

Proof: We may assume k is alg.closed, because the Jordan decomposition is invariant of the field that contains $\mathfrak{g}$, and an element is contained is a vector space can be checked after base change to a larger field. For any subspace $W \subset V$, let $\mathfrak{g}_W = \{\alpha \in \mathfrak{gl}_V | \alpha(W) \subset W, \mathrm{tr}(\alpha|_W) = 0\}$, then if $\mathfrak{g}W \subset W$, then $\mathfrak{g} \subset \mathfrak{g}_W$, because every element of $\mathfrak{g}$ is a sum of brackets by(3.7.2.4), thus have zero trace. Now consider
$$\mathfrak{g}' = \mathfrak{n}_{\mathfrak{gl}_V}(\mathfrak{g}) \bigcap_{\mathfrak{g}W \subset W} \mathfrak{g}_W.$$

If $x \in \mathfrak{g}'$, then so does x_s and x_n, because they are polynomials in x without constant terms, and $\mathrm{ad}(x)_s = \mathrm{ad}(x_s), \mathrm{ad}(x)_n = \mathrm{ad}(x_n)$.

So it suffices to show that $\mathfrak{g} = \mathfrak{g}'$. We claim that $\mathfrak{g}' = \mathfrak{g}$: As $\mathfrak{g}$ is a semisimple ideal of $\mathfrak{g}'$, by(3.7.2.2), we have a decomposition
$$\mathfrak{g}' = \mathfrak{g} \oplus \mathfrak{g}^{\perp}.$$

Let $\alpha \in \mathfrak{g}^{\perp}$ and W a simple $\mathfrak{g}$-module of V, then α acts on W as a scalar, which must be 0 because $\alpha \in \mathfrak{g}_W$ and k has char 0. As W is a sum of simple $\mathfrak{g}$-modules by Weyl's theorem(18.8.1.2), we get the desired conclusion. □

Prop. (3.7.2.9) [Abstract Jordan Decomposition]. A **semisimple/nilpotent element** x in a Lie algebra $\mathfrak{g}$ is an element that $\rho(x)$ is semisimple/nilpotent for any representation (V, ρ) of $\mathfrak{g}$. And $x = x_s + x_n$ is called a **Jordan decomposition** iff $\rho(x) = \rho(x_s) + \rho(x_n)$ is a Jordan decomposition(3.5.8.7) for any representation ρ of $\mathfrak{g}$.

Every element of a semisimple Lie algebra $\mathfrak{g}$ over a field of characteristic 0 has a unique Jordan decomposition, and $x = x_s + x_n$ is a Jordan decomposition if $\rho(x) = \rho(x_s) + \rho(x_n)$ is a Jordan decomposition for one faithful representation ρ of $\mathfrak{g}$. In particular, this is holds for the adjoint representation ad. ⌟

Proof: Let $x \in \mathfrak{g}$ and (V, ρ) a faithful representation of $\mathfrak{g}$(for example the adjoint representation), then there is at most one $x = x_s + x_n$ that $\rho(x) = \rho(x_s) + \rho(x_n)$ is the Jordan decomposition, which proves the uniqueness.

Now for any $x \in \mathfrak{g}$, as(3.7.2.8) shows, there do exist these two elements that $\rho(x) = \rho(x_s) + \rho(x_n)$. But then it can be checked directly $\mathrm{ad}(x) = \mathrm{ad}(x_s) + \mathrm{ad}(x_n)$ is the Jordan decomposition of $\mathrm{ad}(x)$ as an endomorphism of $\mathfrak{g}$, by(3.7.1.16). As the adjoint representation is faithful, this shows the Jordan decomposition is independent of the faithful representation chosen.

Now every representation is a subrepresentation of a faithful representation, so we can prove the existence. □

Simple Lie Algebras

Main references are [Car05]Chap8 and [Kna96], more data about simple Lie algebras can be found in [Kna96]P508.

Def. (3.7.2.10) [Lie Algebras of Type A_n: $\mathfrak{sl}(n+1, \mathbb{C})$]. ⌟

Def. (3.7.2.11) [Lie Algebras of Type A_1]. A_1 is also called $\mathfrak{sl}_2(\mathbb{C})$. It has a basis f, h, e with

$$[he] = 2e, \quad [hf] = -2f, \quad [ef] = h.$$

In matrix form,

$$h = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad e = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad f = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

It can also be realized by

$$H = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad R = \frac{1}{2}\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}, \quad L = \frac{1}{2}\begin{bmatrix} 1 & -i \\ -i & -1 \end{bmatrix}.$$

These two representation differ by a conjugation by the Cayley transformation $C = -\frac{1+i}{2}\begin{bmatrix} i & 1 \\ i & -1 \end{bmatrix}$.

It is simple by?. The subalgebra $\mathfrak{b}$ generated by X and H is solvable, called the canonical Borel subalgebra of $\mathfrak{sl}_2$. ⌟

Proof: □

Prop. (3.7.2.12) [Lie Algebras of Type B_n: $\mathfrak{so}(2n+1, \mathbb{C})$]. ⌟

Prop. (3.7.2.13) [Lie Algebras of Type C_n: $\mathfrak{sp}(n, \mathbb{C})$]. ⌟

Prop. (3.7.2.14) [Lie Algebras of Type D_n: $\mathfrak{so}(2n, \mathbb{C})$]. ⌟

Prop. (3.7.2.15) [Lie Algebras of Type G_2]. ⌟

Prop. (3.7.2.16) [Lie Algebras of Type F_4]. ⌟

Prop. (3.7.2.17) [Lie Algebras of Type E_8]. ⌟

Prop. (3.7.2.18) [Classification of F.D. Complex Simple Lie Algebras]. ⌟

Prop. (3.7.2.19) [Group Automorphisms of Simple Lie Algebras]. Cf.[Carter, P184]. ⌟

Prop. (3.7.2.20). $\mathfrak{sl}_2(k)$ is simple if k has characteristic$\neq 2$. ⌟

Def. (3.7.2.21) [Exponent]. Let $\mathfrak{g}$ be a simple Lie algebra,

$$e=\sum e_i,\quad h=2\rho^\vee=\sum_i(2\rho^\vee,\omega_i)h_i,\quad f=\sum_i(2\rho^\vee,\omega_i)f_i,$$

then by definition, $[h,e]=2e,[e,f]=h$, and

$$\begin{aligned}[h,f]&=\sum_i\sum_j(2\rho^\vee,\omega_i)\alpha_i^\vee(\alpha_j)(2\rho^\vee,\omega_j)f_j\\&=\sum_j[(\sum_i(2\rho^\vee,\omega_i)\alpha_i^\vee,\alpha_j)](2\rho^\vee,\omega_j)f_j\\&=\sum_j(2\rho^\vee,\alpha_j)(2\rho^\vee,\omega_j)f_j\\&=-2f\end{aligned}$$

So $\{h,e,f\}$ is a $\mathfrak{sl}_2$-tuple, called the **principal $\mathfrak{sl}_2$-subalgebra** of $\mathfrak{g}$. The highest weights of subrepresentation of the adjoint action of this subalgebra on $\mathfrak{g}$ is called the **exponents of** $\mathfrak{g}$, counted with multiplicity.

Equivalently, as $h|_{\mathfrak{g}^\alpha}=\mathrm{ht}(\alpha)\,\mathrm{id}$, if r_m is the number of roots of $\mathfrak{g}$ of height m, the exponents of $\mathfrak{g}$ is the numbers m that $r_m>r_{m+1}$. ⌟

Cor. (3.7.2.22). While $r_m=0$ for m large and $r_1=r(\mathfrak{g})$, there are r exponents of $\mathfrak{g}$. Since the roots of height 2 are all $\alpha_i+\alpha_j$ where i,j are connected by an edge in the Dynkin diagram, thus $r_2=r-1$, thus $1=m_1\le\ldots\le m_r$, $\sum_{i=1}^r=|R^+|$. And $\mathfrak{g}\cong\oplus_{r=1}^r L_{2m_i+1}$ as a representation of the principal $\mathfrak{sl}_2$-subalgebra. ⌟

Prop. (3.7.2.23) [Exponents of Simple Lie Algebras]. Let $\mathfrak{g}$ be a Lie algebra, the exponents are.

- $A_n:1,2,\ldots,n$.
- $B_n:1,3,\ldots,2n-1$.
- $C_n:1,3,\ldots,2n-1$.
- $D_n:1,3,\ldots,2n-3$ and n.
- $G_2:1,5$.
- $F_4:1,5,7,11$.
- $E_8:1,7,11,13,17,19,23,29$.
- $E_7:1,5,7,9,11,13,17$.
- $E_6:1,4,5,7,8,11$.

⌟

3 Cartan Subalgebras

Lie algebras in this subsection are assumed to be of f.d..

Def. (3.7.3.1) [Cartan Subalgebras]. A **Cartan subalgebra** of a Lie algebra $\mathfrak{g}$ is a nilpotent subalgebra $\mathfrak{h}$ that equals to its own normalizer in $\mathfrak{g}$. ⌟

Remark (3.7.3.2). As a proper subalgebra of a nilpotent algebra is never its own normalizer(3.7.1.20), a Cartan subalgebra is a maximal nilpotent subalgebra, but a maximal nilpotent subalgebra may not be a Cartan subalgebra.

If k'/k is a field extension, then $\mathfrak{h}$ is a Cartan subalgebra of $\mathfrak{g}$ iff $\mathfrak{h}_{\mathfrak{k}'}$ is a Cartan subalgebra of $\mathfrak{g}_{k'}$. This is because being nilpotent and the normalizer is also compatible with base change(3.7.1.4). ⌟

Prop. (3.7.3.3) [Diagonal Cartan Algebra]. Let $\mathfrak{g} \subset \mathfrak{gl}_V$ be a subalgebra containing a diagonal matrix $a = \mathrm{diag}(a_1, \ldots, a_n)$ with distinct a_i, and let $\mathfrak{h}$ be the subspace of all diagonal matrices in $\mathfrak{g}$, then $\mathfrak{h}$ is a Cartan subalgebra of $\mathfrak{g}$. ⌟

Proof: Firstly $\mathfrak{h}$ is Abelian, and if $b = \sum b_{ij} eij \in N_{\mathfrak{g}}(\mathfrak{h})$, then $[a, b] \in \mathfrak{h}$. But

$$[a, b] = \sum_{ij} (a_{ii} - a_{jj}) b_{ij} e_{ij}$$

is in $\mathfrak{h}$ iff $\mathfrak{b}$ is diagonal, or $b \in \mathfrak{h}$, so $\mathfrak{h} = N_{\mathfrak{g}}(\mathfrak{h})$ and $\mathfrak{h}$ is a Cartan subalgebra. □

Def. (3.7.3.4) [Regular Elements]. Let $\mathfrak{g}$ be a f.d. Lie algebra, for any $x \in \mathfrak{g}$, let $P_x(T)$ be the characteristic polynomial of $\mathrm{ad}(x)$:

$$P_x(T) = \det(T - \mathrm{ad}(x)) = T^m + a_{m-1}(x) T^{m-1} + \ldots + a_0(x).$$

Then the **rank of** $\mathfrak{g}$ is the minimal n that $n(x) \neq 0$ for some $x \in \mathfrak{g}$. A **regular element** is an element $x \in \mathfrak{g}$ that $a_n(x) \neq 0$. ⌟

Prop. (3.7.3.5) [Regular Elements and Cartan Subalgebras]. For any regular element $x \in \mathfrak{g}$, the nilspace $\mathfrak{g}_x^0$ is a Cartan subalgebra of $\mathfrak{g}$. ⌟

Proof: Let

$$U_1 = \{y \in \mathfrak{g}_x^0 | \mathrm{ad}_{\mathfrak{g}}(y)|_{\mathfrak{g}_x^0} \text{ is not nilpotent}\},$$

$$U_2 = \{y \in \mathfrak{g}_x^0 | \mathrm{ad}_{\mathfrak{g}}(y)|_{(\mathfrak{g}/\mathfrak{g}_x^0)} \text{ is invertible}\}.$$

They are both Zariski open subsets of $\mathfrak{g}_x^0$. According to Engel's theorem(3.7.1.29), to show $\mathfrak{g}$ is nilpotent, it suffices to show that U_1 is empty. U_2 is non-empty because it contains x, so if U_1 is non-empty, $U_1 \cap U_2$ is non-empty and there is a $y \in U_1 \cap U_2$. For this y, $n(y) < \dim \mathfrak{g}_x^0 = n(x)$, contradicting the regularity of x.

It remains to show that $\mathfrak{g}_x^0$ is its own normalizer. If z normalizes $\mathfrak{g}_x^0$, then $[z, x] \in \mathfrak{g}_x^0$, which means $(\mathrm{ad}(x))^n [z, x] = 0$, so $\mathrm{ad}(x)^{n+1}(z) = 0$, thus $z \in \mathfrak{g}_x^0$. □

Cor. (3.7.3.6) [Cartan Subalgebras Exist]. Let $\mathfrak{g}$ be a Lie algebra over an infinity field k contains some Cartan subalgebra, and when k is alg.closed, all Cartan subalgebras come from some regular element, by(3.7.3.13). ⌟

Proof: Regular elements exist because k is infinite. □

Cor. (3.7.3.7). Every Lie algebra over an infinite field is a sum of Cartan subalgebras. ⌟

Proof: This is because the sum of Cartan subalgebras is a vector space thus Zariski closed but it contains all regular elements, which is a Zariski open subset. □

Cor. (3.7.3.8). Let $\mathfrak{a}$ be a subalgebra of a Lie algebra $\mathfrak{g}$ that $\mathrm{ad}_{\mathfrak{g}}(a)$ is semisimple for any $a \in \mathfrak{a}$, then $\mathfrak{a}$ is contained in a Cartan subalgebra of $\mathfrak{g}$. ⌟

Proof: Cf.[Mil13]P81.**?** □

Prop. (3.7.3.9). Let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$ over an alg.closed field k. Consider the generalized eigenvalue decomposition(3.7.3.12), if $x \in \mathfrak{g}^\alpha$, then $\mathrm{ad}(x)(\mathfrak{g}^\beta) \in \mathfrak{g}^{\alpha+\beta}$(3.7.1.12), and thus $\mathrm{ad}(x)$ is nilpotent. Let $E(\mathfrak{h})$ be the subgroup of the group of elementary automorphisms(3.7.1.7) of $\mathfrak{g}$ generated by the set of all the automorphisms $e^{\mathrm{ad}_{\mathfrak{g}}(x)}$, where $x \in \mathfrak{g}^\alpha$ for some $\alpha \in \mathfrak{h}^*\backslash 0$.

Now let $\mathfrak{h}, \mathfrak{h}'$ be two Cartan subalgebras of $\mathfrak{g}$, then there exists $u \in E(\mathfrak{h}), u' \in E(\mathfrak{h}')$ that $u(\mathfrak{h}) = u'(\mathfrak{h}')$. ⌟

Proof: Number the elements of $\mathfrak{h}^*\backslash 0$ as $\alpha_1, \ldots, \alpha_n$, and consider the map

$$f : \mathfrak{g}^{\alpha_1} \times \ldots \times \mathfrak{g}^{\alpha_n} \times \mathfrak{h} \to \mathfrak{g} : (x_1, \ldots, x_n, h) \mapsto e^{\mathrm{ad}(x_1)} \ldots e^{\mathrm{ad}(x_n)} h.$$

Given a $h_0 \in \mathfrak{h}$, it can be shown that

$$(df)|_{(0,\ldots,0,h_0)} : (x_1, \ldots, x_n, h) \mapsto h + \sum_i [x_i, h_0].$$

Thus if we choose a regular $h_0 \in \mathfrak{h}$, then $(df)|_{(0,\ldots,0,h_0)}$ is surjective from $\mathfrak{g}$ to $\mathfrak{g}$. Thus $E(\mathfrak{h})\mathfrak{h}_r$ contains a dense open subset of $\mathfrak{g}$**?**. Similarly, $E(\mathfrak{h}')\mathfrak{h}'_r$ contains a dense open subset of $\mathfrak{g}$. So their intersection is not empty, i.e. $u(h) = u'(h')$ for some u, u', h, h'. Now

$$u(\mathfrak{h}) = u(\mathfrak{g}^0_h) = \mathfrak{g}^0_{u(h)} = \mathfrak{g}^0_{u'(h')} = u'(\mathfrak{g}^0_{h'}) = u'(\mathfrak{h}')$$

□

Cor. (3.7.3.10). All Cartan subalgebras in a Lie algebra have the same dimension, which is the rank of $\mathfrak{g}$(3.7.3.4). ⌟

Proof: Because we can take a base change to an alg.closed field, under which a Cartan subalgebra is also a Cartan subalgebra by(3.7.3.2), then they have the same rank. □

Cor. (3.7.3.11) [Cartan Subalgebras are Conjugate]. Any two Cartan subalgebras of a f.d. Lie algebra over an alg.closed field k are conjugate by an elementary automorphism(3.7.1.7). ⌟

Cartan Subalgebra of Semisimple Lie Algebras

Lemma (3.7.3.12) [Decomposition w.r.t. a Cartan Subalgebra]. Let $\mathfrak{h}$ be a Cartan subalgebra of a semisimple Lie algebra $\mathfrak{g}$, and assume that

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \mathfrak{h}^\vee \backslash 0} \mathfrak{g}^\alpha.$$

where $R = R(\mathfrak{g}, \mathfrak{h})$ is called the **root system associated to** $(\mathfrak{g}, \mathfrak{h})$. This is true, for example, when k is alg.closed, by(3.7.9.10).(See(3.7.3.21) for when this decomposition is possible). ⌟

Cor. (3.7.3.13). If k is alg.closed, the set $\mathfrak{h}_r$ of regular elements h in $\mathfrak{h}$ that $\mathfrak{g}^0_h = \mathfrak{h}$ is open and dense in $\mathfrak{h}$ in the Zariski topology. ⌟

Proof: The condition is equivalent to $\prod_{\alpha \in \mathfrak{h}^\vee \backslash 0} \alpha(h) \neq 0$, which is an open condition. □

Lemma (3.7.3.14). In the decomposition above, if $\alpha + \beta \neq 0$, then $\mathfrak{g}^\alpha$ and $\mathfrak{g}^\beta$ is orthogonal w.r.t. the Killing form. ⌟

Proof: $\operatorname{ad}(x)\operatorname{ad}(y)\mathfrak{g}^\gamma \subset \mathfrak{g}^{\alpha+\beta+\gamma}$, so if $\alpha+\beta\neq 0$, then $\operatorname{ad}(x)\operatorname{ad}(y)$ is nilpotent, thus $\kappa(x,y)=0$. □

Prop. (3.7.3.15)[Cartan Subalgebras of Semisimple Lie Algebras]. Let $\mathfrak{h}$ be a Cartan subalgebra of a semisimple Lie algebra $\mathfrak{g}$, then

- Every element of $\mathfrak{h}$ is semisimple. In particular, $\mathfrak{h}$ is commutative(3.7.1.15).
- The centralizer of $\mathfrak{h}$ in $\mathfrak{g}$ is $\mathfrak{h}$.
- The restriction of the Killing form to $\mathfrak{h}$ is non-degenerate.

⌟

Proof: By(3.7.3.2), it suffices to prove this after k is replaced by its alg.closure, so the generalized eigenvalue decomposition(3.7.3.12) holds. We prove 3 first: by(3.7.3.14), $\mathfrak{h}$ is orthogonal to all $[\mathfrak{h},x]$ for any x. But if $x\in\mathfrak{g}^\alpha$, we can see that $[\mathfrak{h},x]=\mathfrak{g}^\alpha$, so $\mathfrak{h}$ is orthogonal to all $\bigoplus\mathfrak{g}^\alpha$, so κ must be non-degenerate on $\mathfrak{h}$.

Because $\mathfrak{g}$ has trivial center, the adjoint representation realizes $\mathfrak{h}$ as a subalgebra of $\mathfrak{gl}_\mathfrak{g}$, and Lie's theorem(3.7.1.24) shows there is a basis that $\mathfrak{h}\subset\mathfrak{b}_\mathfrak{g}$, hence $\operatorname{ad}([\mathfrak{h},\mathfrak{h}])\subset\mathfrak{n}_\mathfrak{g}$, and so $\operatorname{tr}(\mathfrak{h},[\mathfrak{h},\mathfrak{h}])=0$. As κ is non-degenerate on $\mathfrak{h}$, $[\mathfrak{h},\mathfrak{h}]=0$, thus $\mathfrak{h}$ is commutative. Now $\mathfrak{h}\subset c_\mathfrak{g}(\mathfrak{h})\subset N_\mathfrak{g}(\mathfrak{h})$, thus $\mathfrak{h}=c_\mathfrak{g}(\mathfrak{h})$.

If $x\in\mathfrak{h}$, and $x=x_s+x_n$ is the Jordan decomposition(3.7.2.9), then $\operatorname{ad}(x_n)$ are polynomials of $\operatorname{ad}(x)$ thus lies in $\mathfrak{h}$. Now $\operatorname{ad}(x_n)$ commutes with all $\operatorname{ad}(y)$ for $y\in\mathfrak{h}$, thus $\operatorname{ad}(y)\operatorname{ad}(x_n)$ is nilpotent, thus $\kappa(y,x_n)=0$. Thus $x_n=0$ as κ is non-degenerate on $\mathfrak{h}$. □

Cor. (3.7.3.16) [Cartan Subalgebra Maximal Abelian]. The Cartan subalgebras of a semisimple Lie algebra are the maximal subalgebras consisting of semisimple elements(3.7.2.9), and they are maximal Abelian subalgebras.

WARNING: maximal Abelian subalgebra may not by Cartan subalgebras, as they may contain non-semisimple elements. ⌟

Proof: A subalgebra consisting of semisimple elements is contained in a Cartan subalgebra, by(3.7.3.8).

Conversely, if $\mathfrak{h}\subset\mathfrak{h}'$ and $\mathfrak{h}$ is a Cartan subalgebra and $\mathfrak{h}'$ consists of semisimple elements, then by(3.7.1.15), $\mathfrak{h}'$ is commutative, and thus $\mathfrak{h}'\subset c_\mathfrak{g}(\mathfrak{h})$, so $\mathfrak{h}=\mathfrak{h}'$.

Cartan subalgebras are Abelian by(3.7.3.15), and the are maximal Abelian because they are self-centralizing. □

Cor. (3.7.3.17). Every regular element is semisimple, because it is contained in a Cartan subalgebra by(3.7.3.5). ⌟

Split Semisimple Lie Algebras

Def. (3.7.3.18) [Split Semisimple Lie Algebras]. A **split Cartan subalgebra** of a semisimple Lie algebra $\mathfrak{g}$ over a field k is a Cartan subalgebra that all the eigenvalues of the linear maps $\operatorname{ad}(h)$ lies in k for all $h\in\mathfrak{h}$. A **split semisimple Lie algebra** is a pair $(\mathfrak{g},\mathfrak{h})$ where $\mathfrak{g}$ is semisimple and $\mathfrak{h}$ is a split Cartan subalgebra. ⌟

Remark (3.7.3.19). For example, the diagonal matrices in $\mathfrak{sl}_n$ is a splitting Cartan subalgebra over any field.

$\mathfrak{sl}_2(\mathbb{R})$ has a non-split Cartan subalgebra $\{\begin{bmatrix}0 & -a\\ a & 0\end{bmatrix}|a\in\mathbb{R}\}$. ⌟

Prop. (3.7.3.20). Let α be a root of the split semisimple Lie algebra $(\mathfrak{g},\mathfrak{h})$, then

- The subspaces $\mathfrak{g}^\alpha$ and $\mathfrak{h}_\alpha = [\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}]$ are both 1-dimensional.
- There is a unique element $h_\alpha \in \mathfrak{h}_\alpha$ such that $\alpha(h_\alpha) = 2$, and $(h_\alpha, h_\alpha) \neq 0$.
- For each nonzero $x_\alpha \in \mathfrak{g}^\alpha$, there is a $y_\alpha \in \mathfrak{g}^{-\alpha}$ such that

$$[x_\alpha, y_\alpha] = h_\alpha, \quad [h_\alpha, x_\alpha] = 2x_\alpha, \quad [h_\alpha, y_\alpha] = -2y_\alpha.$$

  i.e. $\mathfrak{s}_\alpha = \{x_\alpha, y_\alpha, h_\alpha\} \cong \mathfrak{sl}_2$.
- $k\alpha$ is a root iff $k = 0, \pm 1$.

⌟

Proof: Define $\mathfrak{h}_\alpha = [\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}] \subset \mathfrak{h}$. Because the Killing form is non-degenerate on $\mathfrak{h}$, we can define for each $\alpha \in R$ a unique element $h^\alpha \in \mathfrak{h}$ that $\alpha(h) = \kappa(h, h^\alpha)$ for all $h \in \mathfrak{h}$. Then $\mathfrak{h}_\alpha$ is the subspace spanned by h^α: This is because for $x \in \mathfrak{g}^\alpha, y \in \mathfrak{g}^{-\alpha}$,

$$\kappa(h, [x, y]) = \kappa([h, x], y) = \alpha(x)\kappa(x, y)$$

so $[x, y] = \kappa(x, y)h^\alpha$. Combine this with the fact $\kappa(\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}) \neq 0$, we get the fact $\mathfrak{h}_\alpha = kh^\alpha$ is 1-dimensional.

Next, there is a unique element $h_\alpha \in \mathfrak{h}_\alpha$ that $\alpha(h_\alpha) = 2$. For this, it suffices to show that α doesn't vanish on $\mathfrak{h}_\alpha$: Otherwise let $x \in \mathfrak{g}^\alpha$ and $y \in \mathfrak{g}^{-\alpha}$ that $[x, y] = h \neq 0$, then $[h, x] = \alpha(h)x = 0 = [h, y]$. So $\{x, y, h\}$ spans a solvable subalgebra $\mathfrak{a}$ of $\mathfrak{g}$. As $h \in [\mathfrak{a}, \mathfrak{a}]$. By Lie's theorem, $\rho(h)$ is nilpotent for any representation ρ of $\mathfrak{a}$. But h is in the Cartan subalgebra so $\mathrm{ad}_{\mathfrak{g}}(h)$ is semisimple(3.7.3.15), so $h = 0$, contradiction.

If $(h_\alpha, h_\alpha) = 0$, let $h_\alpha = [x_\alpha, y_\alpha]$ for $x_\alpha \in \mathfrak{g}^\alpha, y_\alpha \in \mathfrak{g}^{-\alpha}$, then $\{x_\alpha, y_\alpha, h_\alpha\}$ is solvable, so by Lie's theorem, there is a basis of $\mathfrak{g}$ that the adjoint action is upper-triangular(when pass to the alg.closure). But then $\mathrm{ad}(h_\alpha)$ is nilpotent, but it is also semisimple, so $h_\alpha = 0$, contradiction.

Because $x_\alpha \neq 0$, there exists a unique $y_\alpha \in \mathfrak{g}^{-\alpha}$ that $[x_\alpha, y_\alpha] = h_\alpha$. Now $[h_\alpha, x_\alpha] = \alpha(h_\alpha)x_\alpha = 2x_\alpha, [h_\alpha, y_\alpha] = -\alpha(h_\alpha)y_\alpha = -2y_\alpha$.

Finally, $\mathfrak{h}_\alpha \bigoplus \oplus_{k\neq 0 \in \mathbb{Z}} \mathfrak{g}^{k\alpha}$ is a subrepresentation of $x_\alpha, y_\alpha, h_\alpha \cong \mathfrak{sl}_2$, so if $\mathfrak{g}^{2\alpha} \neq 0$, then $\mathrm{ad}(x_\alpha)$ induces an isomorphism $\mathfrak{g}^\alpha \cong \mathfrak{g}^{2\alpha}$ by the representation theory of $\mathfrak{sl}_2$(18.8.1.11). But $\mathfrak{g}^\alpha$ is generated by x_α, contradiction. So $\mathfrak{g}^{k\alpha} \neq 0$ only for $k = 0, \pm 1$. □

Prop. (3.7.3.21)[Root Decompositions]. If $\mathfrak{h}$ is a split Cartan subalgebra, then $\mathrm{ad}(\mathfrak{h})$ is a commuting family of semisimple endomorphisms with eigenvalues in k(3.7.3.15). so the decomposition

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}^\alpha$$

holds as in(3.7.3.12). And it is in fact an eigenvalue decomposition, not only generalized eigenvalue decomposition, by(3.7.3.20).

Then R is a reduced root system(3.9.2.2) in $\mathfrak{h}^\vee$, with $s_\alpha(\beta) = \beta - \beta(h_\alpha)\alpha$. In particular, $\alpha^\vee = h_\alpha$.
⌟

Proof: Firstly R spans $\mathfrak{h}^\vee$: if $h \in \mathfrak{h}$ lies in the center of all $\alpha \in R$, then $[h, \mathfrak{g}^\alpha] = 0$ for all $\alpha \in R$, and as $[h, \mathfrak{h}] = 0$, this means h is in the center of $\mathfrak{g}$, which is trivial, so $h = 0$. So R spans $\mathfrak{h}^\vee$.

We need to prove that if $\alpha, \beta \in R$, then $\beta(h_\alpha) \in \mathbb{Z}$ and $\beta - \beta(h_\alpha)\alpha \in R$. For this, regard $\mathfrak{g}$ as a $\mathfrak{s}_\alpha$-module(3.7.3.20) under the adjoint action, then the assertion follows from the representation theory of $\mathfrak{sl}_2$(18.8.1.11): h_α acts on $\mathfrak{g}^\beta$ by $\beta(h_\alpha)$, and y_α^n induces an isomorphism $\mathfrak{g}^\beta \cong \mathfrak{g}^{\beta - n\alpha}$.

Finally, R is reduced by(3.7.3.20). □

Prop. (3.7.3.22) [Splitting Cartan Subalgebras are Conjugate]. The group of elementary automorphisms of $\mathfrak{g}$(3.7.1.7) acts transitively on the set of pairs $(\mathfrak{b},\mathfrak{h})$ consisting of a Borel subalgebra(3.7.4.7) and a splitting Cartan subalgebra of $\mathfrak{g}$. ⌟

Proof: Cf.[Mil13]P98. □

Prop. (3.7.3.23)[Jacobson-Morozov]. Let $\mathfrak{g}$ be a semisimple Lie algebra and $e\in\mathfrak{g}$ is nilpotent, then there exists a homomorphism $\mathfrak{sl}_2\to\mathfrak{g}$ mapping X to e. ⌟

Proof: Cf.https://people.math.harvard.edu/~ana/part1.pdf. □

Recovering Split Semisimple Lie Algebras from Dynkin Diagrams

Main references are [Car05]Chap7.

Def. (3.7.3.24) [Cartan Matrix]. Let $(\mathfrak{g},\mathfrak{h})$ be a split semisimple Lie algebra with root system R, with notations in(3.7.3.20), define the Cartan matrix of $\mathfrak{g}$ to be the Cartan matrix A of R, $A=(a_{ij})$, where $a_{ij}=\alpha_j(h_{\alpha_i})$, where $\{\alpha_1,\ldots,\alpha_n\}$ is a base S of R. ⌟

Prop. (3.7.3.25) [Serre Relations]. Let $(\mathfrak{g},\mathfrak{h})$ be a split semisimple Lie algebra with root system R and a base S, and Cartan matrix $A=(a_{ij})$. Denote $\mathfrak{n}_\pm=\oplus_{\alpha\in R^\pm}\mathfrak{g}^\alpha$, then $\mathfrak{g}=\mathfrak{n}_-\oplus\mathfrak{h}\oplus\mathfrak{n}_+$. Take $e_i\in\mathfrak{g}^{\alpha_i}, f_i\in\mathfrak{g}^{-\alpha_i}$ s.t. $\{e_i,f_i,h_i=[e_i,f_i]\}=\mathfrak{s}_i$ is a $\mathfrak{sl}_2$-triple(3.7.3.20). Then

- e_i,f_i,h_i generate $\mathfrak{g}$.
- (Serre Relations):

$$[h_i,h_j]=0,\quad [h_i,e_j]=a_{ij},\quad [h_i,f_j]=-a_{ij}f_j,\quad [e_i,f_j]=\delta_{ij}h_i,$$

$$(\mathrm{ad}(e_i))^{1-a_{ij}}e_j=0,\quad (\mathrm{ad}(f_i))^{1-a_{ij}}f_j=0,\quad i\neq j$$

⌟

Proof: 1: Because $\mathfrak{h}_i$ generate $\mathfrak{h}$, it suffices to show e_i generate $\mathfrak{n}_+$, then dually f_i generate $\mathfrak{n}_-$. We prove any $\mathfrak{g}^\alpha$ is in the span by induction on the height of α. If $\alpha=\sum n_i\alpha_i$, where $n_i>0$, then $0<(\alpha,\alpha)=\sum n_i(\alpha,\alpha_i)$, thus $(\alpha,\alpha_i)>0$ for some i, thus by(3.9.2.21) $\alpha-\alpha_i$ is a root, and the representation theory of $\mathfrak{s}_i$ shows e_i induces an isomorphism $\mathfrak{g}^{\alpha-\alpha_i}\cong\mathfrak{g}^\alpha$. So we are done.

2: Only the last two assertions need a proof. The irreducible $\mathfrak{s}_i$ representation generated by e_j satisfies $[f_i,e_j]=0,[h_i,e_j]=a_{ij}$, thus this submodule is isomorphic to $W_{a_{ij}}$, and $(\mathrm{ad}(e_i))^{1-a_{ij}}e_j=0$. The f_i case is similar. □

Prop. (3.7.3.26) [Criterion of Semisimplicity]. Let $\mathfrak{g}$ be a Lie algebra and $\mathfrak{h}$ a commutative Lie subalgebra. If

- there is a decomposition
$$\mathfrak{g}=\mathfrak{h}\oplus\bigoplus_{\alpha\in R}\mathfrak{g}^\alpha,$$
where $R\in\mathfrak{h}^\vee$ is the finite set of $\alpha\in\mathfrak{h}^\vee\backslash\{0\}$ that $\mathfrak{g}^\alpha\neq 0$, and $\dim\mathfrak{g}^\alpha=1$ for all $\alpha\in R$.
- R generates $\mathfrak{h}^\vee$.
- If $\alpha\in R$, then $-\alpha\in R$, and $[[\mathfrak{g}^\alpha,\mathfrak{g}^{-\alpha}],\mathfrak{g}^\alpha]\neq 0$.

Then $\mathfrak{g}$ is semisimple and $\mathfrak{h}$ is a split Cartan subalgebra of $\mathfrak{g}$ with root system R. ⌟

Proof: If I is a commutative ideal of $\mathfrak{g}$, by action of $\mathfrak{h}$, we can assume that $\mathfrak{g}^\alpha \subset I$ for some α. If $\alpha \neq 0$, then $\mathfrak{g}^\alpha$ and $[\mathfrak{g}^{-\alpha}, \mathfrak{g}^\alpha] \subset I$, so $[[\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}], \mathfrak{g}^\alpha] = 0$, contradiction. If $I \subset \mathfrak{h}$, then by the hypothesis some $\alpha(I) \neq 0$, so $\mathfrak{g}^\alpha = [I, \mathfrak{g}^\alpha] \subset \mathfrak{g}^\alpha$, contradiction. So $I = 0$.

$\mathfrak{h}$ consists of semisimple elements and it is its own centralizer, so it is a Cartan subalgebra by(3.7.3.16). It is clearly split. □

Cor. (3.7.3.27) [Criterion of Simplicity]. Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebra. A decomposition $\mathfrak{g} = \mathfrak{g}_1 \oplus \mathfrak{g}_2$ of Lie algebras defines a decomposition $(\mathfrak{g}, \mathfrak{h}) = (\mathfrak{g}_1, \mathfrak{h}_1) \oplus (\mathfrak{g}_2, \mathfrak{h}_2)$, and hence a decomposition of the root system $R(\mathfrak{g}, \mathfrak{h})$.

In particular, if the root system $R(\mathfrak{g}, \mathfrak{h})$ is indecomposable, then $\mathfrak{g}$ is simple. ⌟

Proof: Let

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}^\alpha, \quad \mathfrak{g}_1 = \mathfrak{h}_1 \oplus \bigoplus_{\alpha \in R_1} \mathfrak{g}_1^\alpha, \quad \mathfrak{g}_2 = \mathfrak{h}_2 \oplus \bigoplus_{\alpha \in R_2} \mathfrak{g}_2^\alpha$$

be the eigenvalue decomposition of $\mathfrak{g}, \mathfrak{g}_1, \mathfrak{g}_2$ w.r.t. the adjoint action of $\mathfrak{h}$, then $\mathfrak{h} = \mathfrak{h}_1 \oplus \mathfrak{h}_2$, and $R = R_1 \coprod R_2$. □

Prop. (3.7.3.28)[Serre Presentations]. Let $\mathfrak{g}(R)$ be the Lie algebra generated by e_i, f_i, h_i with defining relations as in(3.7.3.25), then

- The Lie subalgebra $\mathfrak{n}_+$ generated by e_i has $(\mathrm{ad}(e_i))^{1-a_{ij}}(e_j) = 0$ as defining relations. The Lie subalgebra $\mathfrak{n}_-$ generated by f_i has $(\mathrm{ad}(f_i))^{1-a_{ij}}(f_j) = 0$ as defining relations. And h_i are linearly independent.
- $\mathfrak{g}(R)$ is a sum of f.d. modules over every $\mathfrak{sl}_2$-triple $\mathfrak{s}_i$.
- $\mathfrak{g}(R)$ is of f.d..
- $\mathfrak{g}(R)$ is semisimple and has root system R.
- $\mathfrak{g}(R_1 \oplus R_2) \cong \mathfrak{g}(R_1) \oplus \mathfrak{g}(R_2)$. In particular, by(3.7.3.27), $\mathfrak{g}(R)$ is simple iff R is indecomposable. ⌟

Proof: It suffices to prove for indecomposable root systems. Consider $\widetilde{\mathfrak{g}(R)}$ the Lie algebra generated by elements e_i, f_i, h_i with the defining relations in(3.7.3.25) without the final two Serre relations, then it is $\mathbb{Z}$-grated, with $\deg(e_i) = 1, \deg(f_i) = -1, \deg(h_i) = 0$. Thus we have a decomposition

$$\widetilde{g(R)} = \widetilde{\mathfrak{n}_+} \oplus \widetilde{\mathfrak{h}} \oplus \widetilde{\mathfrak{n}_-}$$

by degree, and clearly $\widetilde{\mathfrak{n}_+}$ is generated by e_i, $\widetilde{\mathfrak{h}}$ is generated by h_i and $\widetilde{\mathfrak{n}_-}$ is generated by f_i.

Now I claim that $\widetilde{\mathfrak{n}_+}$ is a free Lie algebra on generators e_i, $\widetilde{\mathfrak{n}_-}$ is a free Lie algebra on generators f_i and h_i are linearly independent. It suffices to prove for e_i, and f_i is true with the dual polarization. For this, let $\mathfrak{h}'$ be a vector space with basis h_i', and consider the Lie algebra $\mathfrak{a} = FL_r \rtimes \mathfrak{h}'$, where FL_r is the free Lie algebra generated by f_i', and $\mathfrak{h}'$ acts on FL_r by $[h_i', f_j'] = -a_{ij} f_j'$, then $U = U(\mathfrak{a}) = k\langle f_1', \ldots, f_n' \rangle \rtimes k[h_1', \ldots, h_n']$, and there is an action of $\widetilde{\mathfrak{g}(R)}$ on U that is defined on the generators as follows: if $w = f_{j_1}' \ldots f_{j_s}'$ is a word in f_i' of weight α and $P \in k[h_1', \ldots, h_n']$, then

$$h_i(w \otimes P) = w \otimes (h_i' - \alpha(h_i))P$$

$$f_i(w \otimes P) = fw \otimes P$$

$$e_i(f_{j_1}' \ldots f_{j_s}' \otimes P) = \sum_{k | j_k = i} f_{j_1}' \ldots \widehat{f_{j_k}'} \ldots f_{j_s}' (h_i' - (\alpha_{j_{k+1}} + \ldots + \alpha_{j_s})(h_i'))P.$$

It can be shown that this is truly a representation, and then it induces a map $\widetilde{g(R)} \to U : x \mapsto x(1)$, and this maps Lie polynomials of f_i in $\widetilde{\mathfrak{n}_+}$ to Lie polynomials of f_i', and h_i to h_i', so the assertions are true.

1: Now consider the elements $S_{ij}^+ = (\mathrm{ad}\, e_i)^{1-a_{ij}} e_j \in \widetilde{\mathfrak{n}_+}$ and $S_{ij}^- = (\mathrm{ad}\, f_i)^{1-a_{ij}} f_j \in \widetilde{\mathfrak{n}_-}$. Then $[f_k, S_{ij}^+] = 0$: If $k \neq i, j$, then this is true, and if $k = j$, then $[f_j[e_i e_j]] = [e_i[f_j e_j]] = [h_j e_i] = a_{ji} e_i$, thus $[f_j(\mathrm{ad}\, e_i)^r(e_j)] = 0$ for $r \geq 2$. If $a_{ij} \geq -1$, then this is true, and if $a_{ij} = 0$, then $a_{ji} = 0$ too, so the assertion is also true. If $k = i$, then we can prove by induction that $[f_i(\mathrm{ad}\, e_i)^r(e_j)] = -r(a_{ij} + r - 1)(\mathrm{ad}\, e_i)^{r-1}(e_j)$. Thus $[f_i(\mathrm{ad}\, e_i)^{1-a_{ij}}(e_j)] = 0$, too.

So by induction we see that the ideals $I^{\pm} \in \widetilde{\mathfrak{n}_{\pm}}$ generated by such $S_{ij}^{\pm}$ is ideals $I_{\pm}$ of $\widetilde{g(R)}$. Then the ideal generated by the the Serre relations is the graded ideal $I = I_+ \oplus I_-$, which implies the assertion.

2: The Serre relations shows that e_j generates the representation $W_{-a_{ij}}$ of $\mathfrak{s}_i$ for $j \geq i$, and so does f_j. Also e_i, f_i, h_i generate W_2, and h_j generates W_0 or $W_0 \oplus W_2$, so $\mathfrak{g}(R)$ is a sum of f.d. modules over $\mathfrak{s}_i$, as the module generated by $[a, b]$ is a subquotient of $V \otimes W$ the modules generated by $\{a\}$ and $\{b\}$.

3: $\mathfrak{g}(R) = \oplus_{\alpha \in Q} \mathfrak{g}_\alpha$, where $\mathfrak{g}_\alpha$ is the subspace of $\mathfrak{g}(R)$ of weight α. Then $\mathfrak{g}_\alpha \neq 0$ only if $\alpha \in Q_+$ or Q_-, and each $\mathfrak{g}_\alpha$ is of f.d.. Now we show that $\mathfrak{g}_R \neq 0$ only if $\alpha \in R \cup \{0\}$, which will suffice. We prove by induction on the height of α: the height 1 case is trivial, and if $\alpha = k e_i$, then the statement is clear as $\mathfrak{g}^{k\alpha_i} = 0$ for $k \geq 2$, because $\mathfrak{n}_+$ is generated by e_i. If it is not of the form $\alpha = k e_i$, $(\alpha, \alpha_i) > 0$ for some i, so by the representation theory of $\mathfrak{s}_i \cong \mathfrak{sl}_2$, $\mathfrak{g}^{s_i \alpha} \neq 0$, where $s_i \alpha = \alpha - \alpha_i^\vee(\alpha)\alpha_i \notin Q_-$, thus $s_i \alpha \in Q_+$, and then by induction hypothesis $s_i \alpha \in R$, so $\alpha \in R$.

4: $\widetilde{\mathfrak{g}(R)}^\alpha$ is 1-dimensional for any α, so this is also true for $\mathfrak{g}(R)^\alpha$. Then $\mathfrak{g}(R)$ is semisimple with root system R by(3.7.3.26). □

Cor. (3.7.3.29) [Classification of Split Simple Lie Algebras]. By2, split simple Lie algebras over k are in bijection with Dynkin diagrams $A_l, l \geq 1, B_l, l \geq 2, C_l, l \geq 3, D_l, l \geq 4$ and E_6, E_7, E_8, F_4, G_2, by(3.9.3.5). ⌟

Notations for Split Semisimple Lie algebras

Def. (3.7.3.30) [Notations for a Split Semisimple Lie Algebra]. Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebra, then

- Its (positive/negative) root system is denoted by $(R^+/R^-)R$.
- Notation for root system is the same as in(3.9.4.1).
- $\mathfrak{g}$ has a weight decomposition $\mathfrak{g} = \mathfrak{h} \oplus_{\alpha \in R} \mathfrak{g}^\alpha$.
- $x_\alpha \in \mathfrak{g}^\alpha, y_\alpha \in \mathfrak{g}^{-\alpha}$, where $\alpha \in R^+$.
- $\mathfrak{s}_i = \{x_i, y_i, h_i\}$ is a $\mathfrak{sl}_2$-triple, where $x_i \in \mathfrak{g}^{\alpha_i}, y_i \in \mathfrak{g}^{-\alpha_i}$(3.7.3.20).
- $\alpha_i^\vee = h_i$(3.7.3.21).

⌟

4 Reductive Lie Algebra

Def. (3.7.4.1) [Reductive Lie Algebra]. A Lie algebra is called **reductive** if $\mathrm{rad}(L) = Z(L)$, or equivalently $Z(L) \subset \mathrm{rad}(L)$. ⌟

Prop. (3.7.4.2). The following conditions on a Lie algebra $\mathfrak{g}$ are equivalent:

- $\mathfrak{g}$ is reductive.
- The adjoint representation of $\mathfrak{g}$ is semisimple.
- $\mathfrak{g}$ is a product of a commutative Lie algebra $\mathfrak{c}$ and a semisimple Lie algebra $\mathfrak{b}$.

⌟

Proof: $1 \to 2$: The adjoint representation factors through the center of $\mathfrak{g}$, which is also the radical of $\mathfrak{g}$, so it is a representation of $\mathfrak{g}/\operatorname{rad}(\mathfrak{g})$, which is semisimple(3.7.1.23), so Weyl's theorem(18.8.1.2) shows the adjoint representation is semisimple.

$2 \to 3$: If the adjoint representation is semisimple, then $\mathfrak{g}$ decomposes as a sum of minimal nonzero ideals $\mathfrak{a}_i$ of $\mathfrak{g}$, and then $\mathfrak{g}$ is a product of these $\mathfrak{a}_i$. Let $\mathfrak{c}$ be the product of the one-dimensional ideals, then $\mathfrak{c}$ is in the center thus commutative, and $\mathfrak{b}$ the product of the remaining ideals, then $\mathfrak{b}$ is semisimple because it has no solvable ideals.

$3 \to 1$ is trivial. □

Cor. (3.7.4.3). The decomposition of $\mathfrak{g}$ into a product of commutative Lie algebra and a semisimple Lie algebra is unique: in fact $\mathfrak{c}$ is the center of $\mathfrak{g}$, and $\mathfrak{b} = [\mathfrak{g}, \mathfrak{g}]$, by(3.7.2.4). ⌟

Prop. (3.7.4.4). A Lie algebra $\mathfrak{g}$ is reductive iff it has a faithful semisimple representation iff it has a trivial nilpotent radical(3.7.1.34). ⌟

Proof: If $\mathfrak{g}$ has a faithful semisimple representation, then the nilpotent radical $\mathfrak{s} = 0$, thus by(3.7.1.36), $\mathfrak{r}$ is in the center of $\mathfrak{g}$, thus $\mathfrak{g}$ is reductive.

Conversely, if $\mathfrak{g}$ is reductive, then we need to show $\mathfrak{g}$ has a faithful semisimple representation: For this, we can take the tensor product of the trivial representation of the commutative part and the adjoint representation of the semisimple part(3.7.2.3).

The last assertion is clear from(3.7.1.36). □

Cor. (3.7.4.5) [Trace Form Criterion for Reductiveness]. If the trace form B_ρ(3.7.9.5) is non-degenerate for some representation (ρ, V) of $\mathfrak{g}$, then $\mathfrak{g}$ is reductive. ⌟

Proof: If $x \in \mathfrak{s}$, then $\rho(x) = 0$, thus $B_\rho(x, y) = 0$ for any y, thus $x = 0$. So $\mathfrak{s} = 0$, and $\mathfrak{g}$ is reductive. □

Cor. (3.7.4.6) [Classical Lie Algebras are Reductive]. All classical Lie groups over $\mathbb{R}$ or $\mathbb{C}$ are reductive. ⌟

Proof: Apply(3.7.4.5) their standard representations. □

Def. (3.7.4.7) [Borel Subalgebras]. Let $\mathfrak{g}$ be a split reductive Lie algebra and $\mathfrak{h}$ a Cartan subalgebra with a system of positive roots Π, and consider the corresponding triangular decomposition $\mathfrak{g} = \mathfrak{n}_- \oplus \mathfrak{h} \oplus \mathfrak{n}_+$(3.7.3.21). Denote $\mathfrak{b}_+ = \mathfrak{h} \oplus n_+$, and call any Lie subalgebra of $\mathfrak{g}$ conjugate to $\mathfrak{b}_+$ a **borel subalgebra** of $\mathfrak{g}$. The definition is independent of the choice of the Cartan subalgebra $\mathfrak{h}$, by(3.7.3.22). ⌟

5 Compact Lie Algebras

Main references are [李群讲义, 项武义] and [Kna96].

Def. (3.7.5.1) [Compact Lie Algebras]. A **compact Lie algebra** is Lie algebra that is the Lie algebra of a compact Lie group. ⌟

Prop. (3.7.5.2) [Killing Form of Compact Lie Algberas]. The Killing form of a compact Lie algebra $\mathfrak{g}$ is negatively semi-definite, with the kernel the center of $\mathfrak{g}$. ⌟

Proof: Choose an invariant inner product on $\mathfrak{g}$ w.r.t. the adjoint representation of G by(11.10.4.1). Take derivative w.r.t the equation $(\mathrm{Ad}(g)Y, \mathrm{Ad}(g)Z) = (Y, Z)$, we get by(12.11.1.12),

$$(\mathrm{ad}(X)Y, Z) + (Y, \mathrm{ad}(X)Z) = 0.$$

so $\mathrm{ad}(X)$ is skew-symmetric w.r.t. this inner product, thus the eigenvalues are all purely imaginary. Then $B(x, x) = \mathrm{tr}(\mathrm{ad}(x)\,\mathrm{ad}(x)) \leq 0$. □

Cor. (3.7.5.3) [Compact Lie Algebra is Reductive]. A compact Lie algebra $\mathfrak{g}$ is reductive. ⌟

Proof: Because of the invariant inner form, any ideal $\mathfrak{a}$ of $\mathfrak{g}$ has a complement $\mathfrak{a}^\perp$, thus the adjoint representation of $\mathfrak{g}$ is semisimple, thus $\mathfrak{g}$ is reductive(3.7.4.2). □

Cor. (3.7.5.4) [Compact Lie algebra Elements Semisimple]. For a compact Lie algebra $\mathfrak{g}$, every element is semisimple, and the eigenvalues of any adjoint operator $\mathrm{ad}(x)$ is purely imaginary. ⌟

Proof: Because the Killing form is negative definite, thus its negation is an inner product on $\mathfrak{g}$, and $\mathrm{ad}(x)$ acts by skew-Hermitian matrices, thus has purely imaginary eigenvalues. □

Prop. (3.7.5.5). If $\mathfrak{g}$ is reductive and the Killing form is negative definite on $[\mathfrak{g}, \mathfrak{g}]$, then $\mathfrak{g}$ is compact. ⌟

Proof: For the commutative part we can take the torus $(S^1)^n$, so it suffices to prove the semisimple case: for this, we consider $\mathrm{Int}(\mathfrak{g})^0 \subset GL(\mathfrak{g})$, it is contained in $O(\mathfrak{g})$ with the inner product defined by the negation of the Killing form, thus it is compact. And the Lie algebra of it is $\mathrm{Der}(\mathfrak{g}) = \mathrm{ad}(\mathfrak{g})$(3.7.2.7). □

Prop. (3.7.5.6) [Representation of Compact Lie Algebras]. Let $\mathfrak{g}$ be a compact Lie algebra that is the Lie algebra of a simply-connected compact Lie group, then $\mathrm{Rep}(\mathfrak{g})$ is semisimple. ⌟

Proof: □

6 Singular element

Introduction

Singular element in $\mathfrak{g}$ is a linear space and is defined by some homogenous ideal in $S(\mathfrak{g})$.

The paper [Singular element] of Kostant tells in fact it is defined by some r-homogenous functions M^r in $S(\mathfrak{g})$,and further describes the properties of this ideal such as the G-module decomposition and as span of determinant minors.

Preliminary

Let complex simple Lie algebra $\mathfrak{g} = \mathrm{Lie}\ G$,$n = l + 2r$.The non-degenerate Killing form $\mathcal{B} \triangleq (x, y)$ on $\mathfrak{g}$ generate a nonsingular pair on $S(\mathfrak{g})$ and $\wedge(g)$ by

$$(x_1 \cdots x_k, y_1 \cdots y_k) = \sum_{\sigma \in \Sigma_k} (x_1, y_{\sigma(1)}) \cdots (x_k, y_{\sigma(k)})$$

$$(x_1 \wedge \cdots \wedge x_k, y_1 \wedge \cdots y_k) = \sum_{\sigma \in \Sigma_k} sg(\sigma)(x_1, y_{\sigma(1)}) \cdots (x_k, y_{\sigma(k)})$$

So $\mathfrak{g} \longleftrightarrow \mathfrak{g}'$,$S(\mathfrak{g}) \longleftrightarrow S(\mathfrak{g}') \longleftrightarrow$ polynomial functions on $\mathfrak{g}$; and $S(\mathfrak{g})$ and $\wedge(g)$ are $\mathfrak{g}$ thus G modules extending the adjoint representation.

recall that δ and ∂ are called $\mathcal{B}$-dual if $(\delta x, y) = (x, \partial y)$.Set antiderivation $-d$ $\mathcal{B}$-dual to the operator

$$\partial(x_1 \wedge \cdots \wedge x_p) = \sum_{i<j} (-1)^{i+j+1} [x_i, x_j] \wedge x_1 \wedge \cdots \widehat{x}_i \wedge \cdots \widehat{x}_j \wedge \cdots \wedge x_p$$

on $\wedge(\mathfrak{g})$ and antiderivation $\iota(u)$ $\mathcal{B}$-dual to the operator $\epsilon(u)v = u \wedge v$ on $\wedge(\mathfrak{g})$.

Element v of $S(\mathfrak{g})$ are called **invarient** iff $gv = v, \forall g \in G$ and element u of $S(\mathfrak{g})$ are called **harmonic** iff $(u, v) = 0,\ \forall v$ invariant and no constant term.

Denote by J, H respectively the graded subspace of invariant and harmonic elements, then:

Prop. (3.7.6.1) [Separation of Variables (in [Kos63])]. $S(\mathfrak{g}) \cong J \otimes H$. ⌟

the Ideal of Sing $\mathfrak{g}$

In the projection $\tau : T(\mathfrak{g}) \longrightarrow U(\mathfrak{g})$, PBW theorem asserts that $S(\mathfrak{g}) \longrightarrow U(\mathfrak{g})$ is an isomorphism. Denote:

$$\Gamma = \tau|_{S(\mathfrak{g})}^{-1} \circ \tau$$

Γ is a G-map (as a consequence of the next prop).

Denote by $\Gamma_{2r,2}$ the subgroup of permutation that preserves the set of unordered pairs $\{(1,2), (3,4), \ldots, (2r-1, 2r)\}$ and let Π_r be a left coset representative of $\Gamma_{2r,2}$ in Γ_{2r} that $sg(\Pi_r) = 1$

In [Amitsur-Levitski],Kostant proved:

Prop. (3.7.6.2) [in [Kos81]].

$$\Gamma(\wedge^{2k}(\mathfrak{g})) = R^k \in S^k(\mathfrak{g})$$

$$\Gamma(x_1 \wedge \cdots \wedge x_k) \longrightarrow \sum_{v \in \Pi_k} [x_{v(1)}, x_{v(2)}] \cdots [x_{v(2k-1)}, x_{v(2k)}]$$

⌟

Prop. (3.7.6.3) [in [Kos81]].

$$M = R^r \in H^r$$

so it consists of harmonic functions. ⌟

Let $w \in \wedge^2 \mathfrak{g}$ of rank k standardized as $v_1 \wedge v_2 + \cdots + v_{2k-1} \wedge v_{2k}$.Let

$$\mathrm{Rad} w = \{y \in \mathfrak{g} | \iota(y) w = 0\} = \{y \in \mathfrak{g} | (w, \epsilon(y) z) = 0, \forall z\}$$

then w of rank $2k \iff w^k \neq 0$ & $w^{k+1} = 0 \iff \dim \mathrm{Rad} w = n - 2k$.

Lemma (3.7.6.4).

$$\iota(y) dx = [y, x]$$

Thus

$$\mathrm{Rad} dx = \mathfrak{g}^x,\ \mathrm{Sing}\mathfrak{g} = \{x \in \mathfrak{g} | (dx)^r = 0\}.$$

⌟

Proof: $(\iota(y)dx, z) = (dx, y \wedge z) = (x, -[y, z]) = ([y, x], z)$ □

So in order to find the module M,it's the best to find the dual of

$$\gamma : S(\mathfrak{g}) \longrightarrow \wedge^{\text{even}}\mathfrak{g} : x \longrightarrow -dx$$

Luckily:

Prop. (3.7.6.5) [in [Kos81]]. γ is $\mathcal{B}$ dual to Γ,in particular,

$$(\Gamma(\zeta), x) = \frac{(-1)^r}{r!}(\zeta, (dx)^r) \ (\forall \zeta \in \wedge^{2r}\mathfrak{g} \text{ and } x \in \mathfrak{g})$$

⌟

So: $f(x) = 0, \forall f \in M \iff x \in \text{Sing}\mathfrak{g}$.

Cor. (3.7.6.6). Let $\mathfrak{a}$ be a CSA of $\mathfrak{g}$,$\Delta_+(\mathfrak{a})$ be the positive roots, then

$$f|\mathfrak{a} = C_f \cdot \prod_{\beta \in \Delta_+(\mathfrak{a})} \beta \qquad (\forall f \in M)$$

⌟

Proof: This is because that an element in a CSA is singular iff it commutes with an element outside this CSA, and taking root decomposition, this is equivalent to annihilated by a root, and by counting degree, the cor follows. □

By propositions of [[Kos59]] a **regular nilpotent** element e is **uniquely** in a nilpotent radical $\mathfrak{n}$ of a Borel subalgebra and that $\mathfrak{g}^e \cap [\mathfrak{n}, \mathfrak{n}] = (\text{Sing}\mathfrak{g}) \cap \mathfrak{g}^e$.So there is a linear function ξ on $\mathfrak{g}^e$ that $\ker \xi = (\text{Sing}\mathfrak{g}) \cap \mathfrak{g}^e$.Thus:

Cor. (3.7.6.7). $f|\mathfrak{g}^e = C_f \cdot \xi^r \qquad (\forall f \in M)$. ⌟

Proof: By counting degree, the same reason as before. □

Now we think of a natural question:Can singular elements be defined be functions of even lower degree? The answer is NO.

Prop. (3.7.6.8). Assume $0 \neq f$ homogenous vanishes on $\text{Sing}\mathfrak{g}$,then $\deg f \geq r$ ⌟

Proof: By the last cor, if f has degree less than r then f vanish on any CSA, but semisimple regular element, thus CSAs are Zariski dense in $\mathfrak{g}$ (this is because semisimple element are defined by a polynomial), so $f = 0$. □

Thus we have established that $\text{Sing}\mathfrak{g}$ is an algebraic set defined by a set of harmonic r-homogenous functions on $\mathfrak{g}$ and not by functions of degree lower than r.

Next we offer a different formation of M.

M as minors of determinants

for a $\mathcal{B}$ dual basis y_i, w_j,define a derivation

$$d_W(f \otimes u) = \sum_i^n \partial_{y_i} f \otimes \epsilon(w_i)u \qquad \text{on } S(\mathfrak{g}) \otimes \wedge\mathfrak{g}.$$

Here $\partial_{\sum a_i x_i}$ is defined as $\sum a_i \frac{\partial}{\partial x_1}$ for a standard basis x_i of $\mathfrak{g}$. It's easy to verify that d_W is well defined and is a G-map(Take a different basis Aw_i and Bz_i,then $AB^t = I$,substitute into the formula of d_W,it doesn't change).

Chevalley Thm tells us J is a polynomial ring $\mathbb{C}[p_1, \ldots, p_l]$, where p_i are homogenous polynomials of fixed degree d_i and $\sum_{j=i}^{l}(d_j - 1) = r$.So:

$$d_W p_1(x) \wedge \cdots \wedge d_W p_l(x) = \sum_{1 \le i_1 < \ldots < i_l \le n} \phi(y_{i_1}, \ldots, y_{i_l})(x) w_{i_1} \wedge \cdots \wedge w_{i_l}$$

Where $\phi(y_{i_1}, \ldots, y_{i_l}) = \det \partial_{y_i} p_j$ is homogenous of degree r.(counting degree).

To see this, notice that $f \otimes u$ acts as a function from $\mathfrak{g}$ to $\wedge \mathfrak{g}$: $f \otimes u(x) = f(x)u$.So:

$$d_W p_j(x) = \sum_{i=1}^{n} \partial_{z_i} p_j(x) w_i.$$

Prop. (3.7.6.9). for any CSA $\mathfrak{h}$ of $\mathfrak{g}$ and a basis $\{v_i\}$ of $\mathfrak{h}$,$\forall x \in \mathfrak{h}$,

$$d_W p_1(x) \wedge \cdots \wedge d_W p_l(x) = \kappa \cdot \prod_{\phi \in \Delta_+} \phi(y) v_1 \wedge \ldots \wedge v_l$$

⌟

Lemma (3.7.6.10) [in [Kos63]]. $\{d_W p_1(x), \cdots, d_W p_l(x)\}$ is linearly independant iff $x \in \mathrm{Reg}\mathfrak{g}$. ⌟

Proof: Notice that $d_W p_j$ is a $\mathfrak{g}$-map,ad$y \cdot d_W p_j = d_W p_j([y, x])$ so $d_W p_j(x)$ commutes with $\mathfrak{g}^x$; so $\in \mathfrak{g}^x$.Then the lm tells us when y is regular, $d_W p_j(y)$ forms a basis of $\mathfrak{g}^y$.Considering in $\mathfrak{g}^y, x$ is regular iff $\prod_{\phi \in \Delta_+} \phi(x) \neq 0$,the prop follows. □

Next we give an explicit expression for γ_r.

It can be verified (taking a z_i basis) that $dx = \frac{1}{2} \sum_{i=1}^{n} w_i \wedge [z_i, x]$.

Now $x \in \mathfrak{h}$,

$$dx = \sum_{\phi \in \Delta_+} \phi(x) e_\phi \wedge f_{-\phi}$$

(just take the basis w_i and z_i as a standard basis of $\mathfrak{g}$ consisting of $\{h_i, \ldots, h_l, e_\phi, f_\phi\}$)

So

$$\gamma_r(x^r) = r!(-1)^r \prod_{\phi \in \Delta_+} \phi(x) e_\phi \wedge f_{-\phi}$$

Let $\mu = i^r v_1 \wedge \cdots \wedge v_l \wedge \prod_{\phi \in \Delta_+} e_\phi \wedge f_{-\phi}$ then $(\mu, \mu) = 1$.

Denote $v^* = \iota(v)\mu$ for $v \in \wedge \mathfrak{g}$, then

$$(v_1 \wedge \cdots \wedge v_l)^* = i^r \prod_{\phi \in \Delta_+} e_\phi \wedge f_{-\phi} = C_o \gamma_r(x^r)$$

(notice that $\iota(u)\iota(v) = \iota(v \wedge u)$ and use lm 1)

Prop. (3.7.6.11). $(d_W p_1(x) \wedge \cdots \wedge d_W p_l(x))^* = \kappa_o \gamma_r(\frac{x^r}{r!}) \neq 0$. ⌟

Proof: For $y \in \mathfrak{h}$ regular, this follows from previous calculations, and notice both side are G-maps, and semisimple regular elements are Zariski open, conclusion follows. □

Lemma (3.7.6.12). $(s, t) = (s^*, t^*)$,so that $-^*$ is a $\mathcal{B}$-isomorphism. ⌟

Prop. (3.7.6.13). Let $\{w_1,\dots,w_{2r}\}$ be linearly independent and $\{u_1,\dots,u_l\}$ be a basis of $\{w_1,\dots,w_{2r}\}^{\perp}$,then

$$\Gamma(w_1\wedge\dots\wedge w_{2r})=\kappa_1\det\partial_{u_i}p_j\neq 0$$

Thus,M is the span of all the minors $\det\partial_{u_i}p_j$. ⌟

Proof: By the preceding props,

$$\begin{aligned}\det\partial_{u_i}p_j &= \phi(u_1,\dots,u_l)(x)\\ &= (d_W p_1(x)\wedge\dots\wedge d_W p_l(x),u_1\wedge\dots\wedge u_l)\\ &= ((d_W p_1(x)\wedge\dots\wedge d_W p_l(x))^*,(u_1\wedge\dots\wedge u_l)^*)\\ &= \kappa_o\kappa_2(\phi_r(\frac{x^r}{r!}),w_1\wedge\dots\wedge w_{2r})\\ &= \kappa^{-1}\Gamma(w_1\wedge\dots\wedge w_{2r})(x).\end{aligned}$$

□

G-module structure of M

Now we show the G-module structure of M.

Let θ be the derivative that $\theta(x)(y)=[x,y]$ on $\mathfrak{g}$. Cas $=\sum_{i=1}^n\theta(z_i)\theta(w_i)$.

It's in fact just the action of the Casimir element in center of $U(\mathfrak{g})$.Let m_l and M_l be the maximal eigenvalue and eigenspace of Cas.

For a commutative Lie subalgebra $\mathfrak{c}$ of rank l, denote by $[\mathfrak{c}]$ the line it defines on $\wedge^l\mathfrak{g}$.The span of these $[\mathfrak{c}]$ is denoted A_l.Notice that $[g^y]\subset A_l$ for a regular y,and A_l is a G-submodule.

Prop. (3.7.6.14) [in [Kos65]].

$$A_l=M_l;\qquad m_l=l.$$

⌟

An ideal in a Borel subalgebra of $\mathfrak{g}$ is necessarily spanned by root vectors and a prop of [[K-W09]] says any ideal of dim l is (denoted by $\mathcal{I}$) in fact abelian.

A prop in [[Kos65]] asserts that for two different ideals Φ_1,Φ_2,sum of their weight vectors $\langle\Phi\rangle$ is distinct.

So $G[\Phi_i]$ is an irreducible G-module V_Φ with highest weight $\langle\Phi\rangle$ and V_Φ are inequivalent G-modules(because an irreducible representation have only one highest vector).

Prop. (3.7.6.15) [in [Kos65]].

$$M_l=\oplus_{\Phi\in\mathcal{I}}V_\Phi.$$

⌟

Now denote M_{2r} image of M_l under the isomorphism $u\longrightarrow u^*$, then

Prop. (3.7.6.16) [in [K-W09]]. M_l is the span of $G\cdot[\mathfrak{g}^x]$ for x regular. ⌟

but by precious prop,

$$[\mathfrak{g}^x]=\mathbb{C}d_W p_1(x)\wedge\ldots\wedge p_l(x).$$

thus M_{2r} is the span of $G\cdot(\gamma_r(\frac{x^r}{r!})),x$ regular.

Prop. (3.7.6.17) [Final]. $\Gamma|_{M_{2r}} : M_{2r} \longrightarrow M$ is an isomorphism and $M \cong M_{2r} \cong M_l = A_l$ as G-module.

So M is a multiplicity one module with $|\mathcal{I}|$ irreducible components. ⌟

Proof: Notice that $\Gamma(\zeta)(x) = (\zeta, \gamma_r(\frac{x^r}{r!}))$ and M_{2r} is the span of $G \cdot (\gamma_r(\frac{x^r}{r!}))$,the first part follows, and the rest is a recapitulation of previous props. □

7 Real Lie Algebra

Prop. (3.7.7.1) [Passage from Real to Complex]. If $\mathfrak{g}_0$ is a Lie algebra over $\mathbb{R}$ and $\mathfrak{g} = \mathfrak{g}_0 \otimes \mathbb{C}$ its complexification, then $\mathfrak{g}_0$ is Abelian/nilpotent/solvable/semisimple iff $\mathfrak{g}$ does. ⌟

Def. (3.7.7.2). A **compact real form** is a real subalgebra $\mathfrak{l}$ of $\mathfrak{g}$ s.t. $\mathfrak{g}$ is the complexification of $\mathfrak{l}$ and $\mathfrak{l}$ is the lie algebra of a compact simply-connected Lie group. ⌟

Prop. (3.7.7.3). A real Lie algebra is compact iff there exists an invariant inner product iff the Killing form is negative definite. ⌟

Proof: One direction is easy, just use the average method to find a G-invariant inner product and then take derivative. For the other direction, the identity shows that a complement of an ideal is an ideal so $\mathfrak{g}$ is decomposed into simple lie groups and reduce to the case that $\mathfrak{g}$ is simple. The ideal is to show that $\mathfrak{g} \cong \mathrm{ad}(\mathfrak{g})$ is the whole outer derivative group $\partial(\mathfrak{g})$(the following lm). So $\mathfrak{g}$ equals to the identity component of $\mathrm{Aut}(\mathfrak{g})$ which is a closed subgroup thus closed but it is also a subgroup of the compact group $O(\mathfrak{g})$ thus it is compact. □

Lemma (3.7.7.4). If a real semisimple Lie algebra X has an invariant inner product, then every outer derivative is inner.(In fact, this is true by Cartan Criterion for semisimplicity (3.7.2.7)). ⌟

Proof: since $\mathrm{ad}(X)$ is skew-symmetric, it's diagonalizable and its eigenvalue is pure imaginary, so the Killing form of X is negative definite. Now choose the complement $\mathfrak{a}$ of $\mathrm{ad}(X)$ in $\partial(X)$, then $\mathfrak{a} \cap X = 0$. Thus for $D \in \mathfrak{a}$, $\mathrm{ad}(D(g)) = [D, \mathrm{ad}(g)] = 0$ for all g in X, so $D = 0$, thus $\mathrm{ad}(X) = \partial(X)$. □

Prop. (3.7.7.5). -

1. The complexification of the Lie algebra of a connected compact Lie group is reductive.
2. A complex Lie algebra is semisimple iff it is isomorphic to the complexification of the Lie algebra of a simply-connected compact Lie group. i.e. every complex semisimple Lie algebra has a compact real form.

⌟

Proof: 1: Because a connected compact Lie group is completely reducible so the does the Lie algebra and so does the complexification. So it is reductive by (3.7.4.1)4.

2: Cf.[Varadarajan Lie Groups Lie algebras and Their Representations]. The idea is to find a real form whose corresponding simply-connected group is compact. □

Prop. (3.7.7.6). If $\mathfrak{g}$ is the Lie algebra of a matrix Lie group G, then:

1. every Cartan subalgebra comes from a maximal commutative subalgebra of a compact real form and any two Cartan subalgebras are conjugate under the Ad-action of G.
2. any two compact real form is conjugate under the Ad-action of G.

3. any two maximal commutative subalgebra of a compact real form is conjugate under the Ad-action of the corresponding compact compact subgroup.

⌟

Prop. (3.7.7.7). A real Lie algebra is semisimple iff its complexification is semisimple. Cf.[Varadarajan]. ⌟

Cor. (3.7.7.8). The real Lie algebra of a compact simply-connected group is semisimple. ⌟

Note: For the classification of real semisimple Lie algebras, Cf.[李群讲义项武义 §6]

Prop. (3.7.7.9). If a complex representation of a Lie group admits an invariant bilinear form, then it is non-degenerate and unique. In fact, this is equivalent to a G-map from V to V^*. Thus there is unique invariant inner product in a compact real form by the preceding proposition. ⌟

8 Universal Constructions

In this subsection k can be a field of any characteristics.

Def. (3.7.8.1) [Universal Enveloping Algebra]. The **universal enveloping algebra** of a Lie algebra $\mathfrak{g}$ is defined to be

$$U(g) = T(\mathfrak{g})/J, \quad T(\mathfrak{g}) = \bigoplus_{n=0}^{\infty} \mathfrak{g}^{\otimes n}$$

which is a graded algebra $T(\mathfrak{g})$ quotients the ideal $J = (\{x \otimes y - y \otimes x - [xy]\})$.

There is a natural linear map $\sigma : \mathfrak{g} \to U(\mathfrak{g})$. ⌟

Prop. (3.7.8.2). The universal enveloping algebra $U : \mathfrak{g} \mapsto U(\mathfrak{g})$ defines a functor $\mathtt{LieAlg} \to \mathcal{A}\mathrm{lg}^{\mathrm{asso}}$ that is left adjoint to the canonical functor ${\mathcal{A}\mathrm{lg}^{\mathrm{asso}}}_k \to \mathtt{LieAlg}_k$(3.7.1.2). ⌟

Proof: For any associative algebra A and a morphism of Lie algebras $\mathfrak{g} \to [A]$, there is easily seen a morphism $U(\mathfrak{g}) \to A$, and it is unique. □

Cor. (3.7.8.3) [Representation as Modules]. A representation of $\mathfrak{g}$(3.7.12.4) is he same as a representation of $U(\mathfrak{g})$. ⌟

Prop. (3.7.8.4) [Poincaré-Birkhoff-Witt]. Let $\mathfrak{g}$ be a Lie algebra, define a filtration on $U(\mathfrak{g})$ by assigning $F_nU(\mathfrak{g})$ = the image of $\bigoplus_{i=0}^n \mathfrak{g}^{\otimes i}$ in $U(\mathfrak{g})$. We have $[F_iU(\mathfrak{g}), F_jU(\mathfrak{g})] \subset F_{i+j-1}U(\mathfrak{g})$, thus $grU(\mathfrak{g})$ has a graded commutative ring structure. Thus there is an algebra homomorphism $S(\mathfrak{g}) \to grU(\mathfrak{g})$, and this homomorphism is an isomorphism.

If $\mathfrak{g}$ has a basis $\{x_i\}, i \in I$ and $<$ is an order on I, then $U(\mathfrak{g})$ has a basis consisting of elements $\{x_{i_1}^{r_1} \cdots x_{i_k}^{r_k}\}$ where $i_1 < i_2 < \ldots < i_r$. ⌟

Proof: We assign any monomial $a_{i_1} \ldots a_{i_n}$ in a_is a pair (k, N) where k is the number of factors in a monomial and N is the number of inversions(meaning the number of pairs $1 \le r, s \le n$ that $i_r > i_s$), pairs (k, N) are lexicographical ordered. Let $T^{(k,N)}$ be the space of $T(\mathfrak{g})$ generated by monomials of index (k, N), $T^k = \cup_{N=1}^{\infty} T^{(k,N)}$, and $\mathcal{U}^{(k,N)}, \mathcal{U}^k$ the space of $T(\mathfrak{g})$ the image of $T^{(k,N)}, T^k$ in $\mathcal{U}(\mathfrak{g})$. We will use induction on (k, N). Notice for any k, $T^k = T^{(k,N)}$ for N large.

To show that the monomials in $(\star)$ generates $\mathcal{U}(\mathfrak{g})$, if we have a monomial $a_{i_1}a_{i_2} \ldots a_{i_s}a_{i_{s+1}} \ldots a_{i_k}$ that $i_s > i_{s+1}$, then

$$a_{i_1}a_{i_2} \ldots a_{i_s}a_{i_{s+1}} \ldots a_{i_k} = a_{i_1}a_{i_2} \ldots (a_{i_{s+1}}a_{i_s} + [a_{i_s}, a_{i_{s+1}}]) \ldots a_{i_k},$$

which is in $\cup_{(k',N')<(k,N)}\mathcal{U}^{(k',N')}$. So we can use induction on (k,N) to show that any element of $\mathcal{U}(\mathfrak{g})$ is in $\cup_{k=1}^{\infty}T^{(k,0)}$.

From now on, we write $a_{i_1}a_{i_2}\dots a_{i_n}$ as $a_{i_1}a_{i_2}\dots a_{i_n}$ for simplicity.

To show that the monomials are linearly independent, we first show that there is a linear map

$$\theta : T(\mathfrak{g}) \to R = \mathbb{C}[z_i]_{i\in I}$$

satisfying the following conditions:

$$\theta(a_{i_1}\dots a_{i_n}) = z_{i_1}\dots z_{i_n}, \text{if } i_1 \le i_2 \dots \le i_n, \qquad (\star\star)$$

$$\theta(a_1\dots a_{i_k}a_{i_{k+1}}\dots a_{i_n})$$
$$= \theta(a_1\dots a_{i_{k+1}}a_{i_k}\dots a_{i_n}) + \theta(a_1\dots[a_{i_k}a_{i_{k+1}}]\dots a_{i_n}). \qquad (\star\star\star)$$

We construct this map by construction on $\cup_{(k',N')\le(k,N)}\mathcal{U}^{(k',N')}$ and use induction on (kN). For $k=0$, let $\theta(1)=1$. If θ is defined for any monomials of index (k,N) that $k<n$, define θ on $T^{n,0}$ by $\theta(a_{i_1}\dots a_{i_n}) = z_{i_1}\dots z_{i_n}$, then it satisfies $(\star\star)$.

And if θ is already defined for any $T^{n,k}$ that $k<i$, suppose that the monomial $a_{i_1}\dots a_{i_n}$ has index (n,i), then there is a smallest k that $a_{i_1}\dots a_{i_{k+1}}a_{i_k}\dots a_{i_n}$ has index $i-1$. Then we define

$$\theta(a_{i_1}\dots a_{i_n}) = \theta(a_{i_1}\dots a_{i_{k+1}}a_{i_k}\dots a_{i_n}) + \theta(a_{i_1}\dots[a_{i_k},a_{i_{k+1}}]\dots a_{i_n}).$$

Now we need to check that this definition satisfies $(\star\star\star)$:

If there is another k' that $i_{k'} > i_{k'+1}$, then $k<k'$. Suppose first that $k+1<k'$, let $a_{i_k} = a, a_{i_{k+1}} = b, a_{i_{k'}} = c, a_{i_{k'+1}} = d$, then

$$\begin{aligned}\theta(\dots ab\dots cd\dots) &= \theta(\dots ba\dots cd\dots) + \theta(\dots[a,b]\dots cd\dots)\\ &= \theta(\dots ba\dots dc\dots) + \theta(\dots ba\dots[cd]\dots) + \theta(\dots[ab]\dots dc\dots) + \theta(\dots[ab]\dots[cd]\dots)\\ &= \theta(\dots ab\dots dc\dots) + \theta(\dots ab\dots[cd]\dots)\end{aligned}$$

where the terms except the first one are all in $\cup_{(k',N')<(k,N)}T^{(k',N')}$ so the equalities come from induction hypothesis. So it satisfies $(\star\star\star)$.

Suppose next that $k'=k+1$, let $a_{i_k}=a, a_{i_{k+1}}=b, a_{i_{k+2}}=c$, then

$$\begin{aligned}\theta(\dots abc\dots) &= \theta(\dots bac\dots) + \theta(\dots[ab]c\dots)\\ &= \theta(\dots bca\dots) + \theta(\dots b[ac]\dots) + \theta(\dots c[ab]\dots) + \theta(\dots[[ab]c]\dots)\\ &= \theta(\dots cba\dots) + \theta(\dots[bc]a\dots) + \theta(\dots b[ac]\dots) + \theta(\dots c[ab]\dots) + \theta(\dots[[ac]b]\dots) + \theta(\dots[a[bc]]\dots)\\ &= \theta(\dots cab\dots) + \theta(\dots[ac]b\dots) + \theta(\dots a[bc]\dots)\\ &= \theta(\dots acb\dots) + \theta(\dots a[bc]\dots)\end{aligned}$$

where the terms except the first one are all in $\cup_{(k',N')<(k,N)}T^{(k',N')}$ so the equalities come from induction hypothesis, and in the third equality we used the Jacobi identity. So it satisfies $(\star\star\star)$.

Now all elements in J is a linear combination of elements of the form

$$a_1\dots a_{i_k}a_{i_{k+1}}\dots a_{i_n} - a_1\dots a_{i_{k+1}}a_{i_k}\dots a_{i_n} - a_1\dots[a_{i_k}a_{i_{k+1}}]\dots a_{i_n},$$

so the map θ factors through $T(\mathfrak{g})\to\mathcal{U}(\mathfrak{g})$ to a map $\overline{\theta}:\mathcal{U}(\mathfrak{g})\to R$, and the elements $a_{i_1}a_{i_2}\dots a_{i_k}, i_1 \le i_2 \le \dots \le i_k$ are mapped to $z_{i_1}\dots z_{i_n}$, which are linearly independent in R, so the elements $a_{i_1}a_{i_2}\dots a_{i_k}, i_1\le i_2\le\dots\le i_k$ are also linearly independent in $\mathcal{U}(\mathfrak{g})$. □

Cor. (3.7.8.5). The map $\mathfrak{g} \to U(\mathfrak{g})$ is injective. ⌟

Cor. (3.7.8.6). $U(\mathfrak{g})$ has no zero-divisors. ⌟

Proof: We can use the identities $x \otimes y - y \otimes x = [xy]$ to make any element in their right representations under the PBW prop(3.7.8.4), so it is clear that the product of two nonzero elements cannot be 0. □

Cor. (3.7.8.7). If $\mathfrak{h} \subset \mathfrak{g}$, then the subalgebra of $U(\mathfrak{g})$ generated by $\mathfrak{h}$ is isomorphic to $U(\mathfrak{h})$. ⌟

Proof: There is a natural map $U(\mathfrak{h}) \to U(\mathfrak{g})$, and the image is just the subgroup generated by $\mathfrak{h}$. The PBW theorem shows this map is injective. □

Cor. (3.7.8.8). If $\mathfrak{g} = \mathfrak{a} \times \mathfrak{b}$, then $U(\mathfrak{g}) = U(\mathfrak{a}) \otimes U(\mathfrak{b})$. ⌟

Def. (3.7.8.9) [Coproduct of $U(\mathfrak{g})$]. Let $\mathfrak{g}$ be a Lie algebra, there is a coproduct Δ on $T(\mathfrak{g})$ defined by $\Delta(g) = g \otimes 1 + 1 \otimes g$. This coproduct descends to a coproduct $\Delta : U(\mathfrak{g}) \to U(\mathfrak{g}) \otimes U(\mathfrak{g})$. ⌟

Proof: It suffices to check that $\Delta(J) \subset J \otimes T(\mathfrak{g}) + T(\mathfrak{g}) \otimes J$, and this is because

$$\begin{aligned}\Delta(x \otimes y - y \otimes x - [xy]) &= (x \otimes 1 + 1 \otimes x)(y \otimes 1 + 1 \otimes y) - (y \otimes 1 + 1 \otimes y)(x \otimes 1 + 1 \otimes x) - ([xy] \otimes 1 + 1 \otimes [xy]) \\ &= (x \otimes y - y \otimes x - [xy]) \otimes 1 + 1 \otimes (x \otimes y - y \otimes x - [xy])\end{aligned}$$

□

Prop. (3.7.8.10) [$\mathfrak{g}$-Module Structure]. Let $\mathfrak{g}$ be a Lie algebra, then $T(\mathfrak{g})$ is a $\mathfrak{g}$-module, and this action descends to a $\mathfrak{g}$-module structure on $U(\mathfrak{g})$. ⌟

Proof: It suffices to show that $\mathfrak{g}J \subset J$ and $\mathfrak{g}I \subset I$:

$$\begin{aligned}y(a \otimes b - b \otimes a - [ab]) &= [ya] \otimes b + a \otimes [yb] - [yb] \otimes a - b \otimes [ya] - [y[ab]] \\ &= [ya] \otimes b - b \otimes [ya] - [[ya]b] + a \otimes [yb] - [yb] \otimes a - [a[yb]]\end{aligned}$$

□

Prop. (3.7.8.11) [Transpose]. There is an anti-automorphism $u \mapsto u^t$ of $U(\mathfrak{g})$ that $X^t = -X$ for $X \in \mathfrak{g}$. ⌟

Proof: We first extend this t to an automorphism of $T(\mathfrak{g})$, then we compose with the obvious anti-automorphism $T(\mathfrak{g}) \to T(\mathfrak{g})$. Then we check that this map descends to $U(\mathfrak{g})$: $(X \otimes Y - Y \otimes X - [X,Y])^t = Y \otimes X - X \otimes Y - [Y,X] \in J$, so $J^t \in J$. □

Prop. (3.7.8.12) [Graded Algebra of $U(\mathfrak{g})$]. Let L be a Lie algebra, if we let $S(L) = T(L)/(x \otimes y - y \otimes x)$ be the universal symmetric algebra of L, then it is a graded algebra. There is a filtered structure on $U(L)$ given by $U_i = \{\text{subalgebra generated by } a_1 a_2 \ldots a_j, j \leq i\}$, then the associated graded algebra of $U(L)$ is isomorphic to $S(L)$ by PBW theorem. ⌟

Cor. (3.7.8.13). If W is a subspace of $T^n(L)$ that is sent isomorphically onto $S^n(L)$, then the image of W is a complement of $U_n(L)$ complementary to $U_{n-1}(L)$. ⌟

Cor. (3.7.8.14) [Symmetrization Map]. Over a field of characteristic 0, the symmetrization map $\sigma : S(\mathfrak{g}) \to T(\mathfrak{g}) \to U(\mathfrak{g})$(3.5.5.2) is an isomorphism of $\mathfrak{g}$-modules that

$$U^n(\mathfrak{g}) = \sigma(S^n(\mathfrak{g})) \oplus U^{n-1}(\mathfrak{g}).$$

⌟

Proof: It is clearly an isomorphism of vector spaces. It suffices to show the map is compatible with $\mathfrak{g}$-actions: Because

$$\sigma(y_1 \dots y_n) = \frac{1}{n!}\sum_{\sigma\in\Sigma_n} y_{\sigma(1)}\cdots y_{\sigma(n)},$$

$$\begin{aligned}\sigma(g(y_1\dots y_n)) &= \sigma([gy_1]\dots y_n + \dots + y_1\dots[gy_n])\\ &= \frac{1}{n!}\sum_{\sigma\in\Sigma_n}([gy_{\sigma(1)}]\dots y_{\sigma(n)} + \dots + y_{\sigma(1)}\dots[gy_{\sigma(n)}])\\ &= g(\frac{1}{n!}\sum_{\sigma\in\Sigma_n} y_{\sigma(1)}\cdots y_{\sigma(n)})\end{aligned}$$

□

Prop. (3.7.8.15). If $\mathfrak{g}$ is a Lie algebra over a field k of characteristic 0, then the set of primitive elements(3.11.2.4) are just $\mathfrak{g}$. ⌟

Proof: If f is primitive, then the leading term f_0 of f is also primitive in $grU(\mathfrak{g}) \cong S(\mathfrak{g})$. Now consider $S(\mathfrak{g}) \xrightarrow{\Delta} S(\mathfrak{g})\otimes S(\mathfrak{g}) \xrightarrow{\mu} S(\mathfrak{g})$, then if f is of degree n, then $2^n f_0 = 2f_0$, which means $n = 1$. So $f = c + f_0$, and $c = 0$. □

Prop. (3.7.8.16) [$U(\mathfrak{g})$ is Notherian]. For a f.d. Lie algebra $\mathfrak{g}$, $U(\mathfrak{g})$ is left Noetherian. ⌟

Proof: This is because the graded stricture on $U(\mathfrak{g})$ satisfies $\mathrm{gr}U(\mathfrak{g}) \cong S(\mathfrak{g}) \cong \mathbb{C}[X_1,\dots,X_n]$ is Noetherian, so $U(\mathfrak{g})$ is Noetherian itself. □

Free Lie Algebras

Def. (3.7.8.17) [Free Lie Algebra]. Let X be a set, then we define the **free Lie algebra** $FL(X)$ to be the intersection of Lie subalgebras in $[F(X)]$ containing $\sigma(X)$, where $F(X)$ is the free algebra generated by X.

Then the free Lie algebra $FL : X \mapsto FL(X)$ defines a functor $Set \to LieAlg$ that is left adjoint to the forgetful functor. ⌟

Proof: We need to show that for any Lie algebra L and a map fo sets $\theta : X \to L$, there is a unique φ completing the upper left triangular diagram:

$$\begin{array}{ccccc} X & \xrightarrow{i} & FL(X) & \longrightarrow & F(X) \\ \downarrow\theta & \swarrow\varphi & & \searrow\overline{\varphi} & \downarrow\overline{\theta} \\ L & & \xrightarrow{\sigma} & & U(L) \end{array}$$

Notice $\overline{\varphi}^{-1}(\sigma(L))$ is a Lie algebra containing X thus containing $FL(X)$, so it induces a φ.

And for the uniqueness, if there are two φ_1,φ_2, then the element that they coincide is a Lie algebra containing X, thus containing $FL(X)$, so $\varphi_1 = \varphi_2$. □

Cor. (3.7.8.18). $U(FL(X)) \cong FX$ for any set X. ⌟

Proof: Because $U\circ FL$ and F are both left adjoint to the forgetful functor $AssAlg \to Set$. □

Center of $U(\mathfrak{g})$

Prop. (3.7.8.19) [$\mathfrak{g}$ Action on $U(\mathfrak{g})$]. $\mathfrak{g}$ acts on $T(\mathfrak{g})$ by adjoint(3.7.9.2), and notice

$$\mathrm{ad}(z)(x\otimes y - y\otimes x - [xy]) = [zx]\otimes y + x\otimes [zy] - [zy]\otimes x - y\otimes [zx] - [z[xy]] \in J,$$

so the action of $\mathfrak{g}$ descends to an action on $U(\mathfrak{g})$.

In fact, this action is inner: $\mathrm{ad}(g)(z) = gz - zg$ for $z\in U(\mathfrak{g})$. In particular,

$$Z(U(\mathfrak{g})) = U(\mathfrak{g})^{\mathrm{ad}(\mathfrak{g})}.$$

⌟

Invariant Polynomials

Prop. (3.7.8.20) [Chevalley]. The center of the universal enveloping algebra is isomorphic to the polynomial ring over $\mathbb{C}$ of l elements, where L is a semisimple lie algebra of rank l. In particular, The center for $\mathfrak{sl}_2$ is the algebra generated by the Casimir element $1/2h^2 + ef + fe$. ⌟

Proof: Because there is a commutative diagram of isomorphisms of algebras:

$$\begin{array}{ccc} S(L)^G & \xrightarrow{\alpha} & P(L)^G \\ \downarrow{\scriptstyle\eta} & & \downarrow{\scriptstyle\phi} \\ S(H)^W & \xrightarrow{\beta} & P(H)^W \end{array}$$

Where P is the polynomial ring$\cong S(L^*)$, the horizontal is Killing isomorphisms and vertical is the restriction maps. Cf.[Carter prop 13.32]**?**.

The twisted Harish-Chandra map gives an isomorphism of algebras $Z(L)\to S(H)^W$ (It just maps $z\in Z(L)$ to its pure H part and transform every indeterminants h_i to $h_i - 1$). e.g. $z = h^2 + 2h + 1 + 4fe \in Z(\mathfrak{sl}_2)$ is maped to h^2 in $S(H)$. And $P(H)^W$ is isomorphic to a polynomial ring in l generators over $\mathbb{C}$. □

Def. (3.7.8.21) [Casimir Element]. If L is semisimple Lie algebra, by(3.7.2.1) the Killing form is non-degenerate, thus we choose a basis x_i of L and a dual basis y_i, then $c = \sum x_i y_i$ is independent of x_i chosen by(3.5.10.24), and is called the **Casimir element** of $U(L)$. ⌟

Prop. (3.7.8.22). The Casimir element lies in the center of $U(L)$. ⌟

Proof: □

Prop. (3.7.8.23) [Quillen's lm]. If K is an alg.closed field of char 0 that $\mathfrak{g}$ is a f.d. Lie algebra over K. If $U = U(\mathfrak{g})$ is its universal enveloping algebra, then for any irreducible U-module M, $\mathrm{End}_U(M) = K$. ⌟

Miscellaneous

Prop. (3.7.8.24) [Grading on $U(\mathfrak{sl}_2(\mathbb{C}))$]. Let H, R, L be a basis of $\mathfrak{sl}_2(\mathbb{C})$(3.7.2.11), if we define a grading as $\deg R = 1, \deg H = 0, \deg L = -1$, then this is descends to a grading on $U(\mathfrak{g})$, and the degree 0 part is the ring $\mathcal{R} = \mathbb{C}[\Delta, H]$. Also, there is a decomposition:

$$U(\mathfrak{g}) = \bigoplus_{i\geq 0} L^i\mathcal{R} \oplus \bigoplus_{i>0} R^i\mathcal{R}.$$

⌟

9 Representations

Def. (3.7.9.1) [Representations]. A **representation of a Lie algebra** $\mathfrak{g}$ over a vector space V is a Lie homomorphism $\mathfrak{g} \to \mathfrak{gl}_V$. ⌟

Def. (3.7.9.2) [Tensor Product of Representations]. Let $(V_1, \pi_1), (V_2, \pi_2)$ be two representations of a Lie algebra $\mathfrak{g}$, then $(V_1 \otimes V_2, \pi_1 \otimes \pi_2)$ is a representation of $\mathfrak{g}$ given by

$$(\pi_1 \otimes \pi_2)(g)(v_1 \otimes v_2) = \pi_1(g)v_1 \otimes v_2 + v_1 \otimes \pi_2(g)v_2.$$

⌟

Def. (3.7.9.3) [Representation on Tensor Algebras]. If (V, ρ) is a representation of $\mathfrak{g}$, then $\mathfrak{g}$ acts on $T(V)$ via(3.7.9.2). Also, the ideals I, J are invariant under action of $\mathfrak{g}$, thus the representation extends to $\mathrm{Sym}(V)$ and $\wedge(V)$. Also it preserves degree, thus it induces representations on $\mathrm{Sym}^k(V)$ and $\wedge^k(V)$. ⌟

Proof:

$$g(a \otimes a) = g(a) \otimes a + a \otimes g(a) = (a + g(a)) \otimes (a + g(a)) - a \otimes a - g(a) \otimes g(a)$$

and

$$g(a \otimes b - b \otimes a) = g(a) \otimes b + a \otimes g(b) - g(b) \otimes a - b \otimes g(a) = g(a) \otimes b - b \otimes g(a) + a \otimes g(b) - g(b) \otimes a$$

□

Def. (3.7.9.4) [dual representation]. If (φ, V) is a representation of $\mathfrak{g}$, we define the **dual representation** $(\varphi^*, V^\vee)$ as

$$(\varphi^(g)(v^*), v) = (v^*, \varphi(g)v).$$

⌟

Def. (3.7.9.5) [Trace Form]. The **trace form** of a representation (V, ρ) of a Lie algebra $\mathfrak{g}$ is an invariant symmetric form β_ρ defined by $(x, y) \mapsto \mathrm{tr}(\rho(x) \circ \rho(y))$. ⌟

Proof: It is invariant because

$$\begin{aligned}\mathrm{tr}(\rho([x, y]) \circ \rho(z)) &= \mathrm{tr}(\rho(x)\rho(y)\rho(z)) - \mathrm{tr}(\rho(y)\rho(x)\rho(z)) \\ &= \mathrm{tr}(\rho(x)\rho(y)\rho(z)) - \mathrm{tr}(\rho(x)\rho(z)\rho(y)) \\ &= \mathrm{tr}(\rho(x)\rho([y, z])).\end{aligned}$$

□

Prop. (3.7.9.6). If ρ is a faithful representation of $\mathfrak{g}$ and $\mathfrak{g}$ is semisimple, then β_ρ is non-degenerate. ⌟

Proof: The Cartan's criteria(3.7.1.27) shows $\mathfrak{g}^\perp$ is a solvable sub-Lie algebra, so it must be 0 as $\mathfrak{g}$ is semisimple(3.7.1.23). □

Prop. (3.7.9.7). Let L be a simple lie algebra, then any two non-degenerate symmetric invariant bilinear forms on L is proportional. Because any of this form corresponds to a L-morphism from L to L^*. In particular, when $L \subset \mathfrak{gl}_n$, the usual trace is proportional to the Killing form. ⌟

Remark (3.7.9.8) [Rep($\mathfrak{g}$)]. Let $\mathfrak{g}$ be a Lie algebra over a field k, let $\mathrm{Rep}(\mathfrak{g})$ denote the category of f.d. representations of $\mathfrak{g}$. ⌟

Prop. (3.7.9.9) [Schur's Lemma]. Let $\mathfrak{g}$ be a finite Lie algebra, M be an irreducible $\mathfrak{g}$-module, then $\dim M$ is countable. In particular, Shur's lemma holds by(18.1.1.10). ⌟

Proof: It is of countable dimensional because $\dim U(\mathfrak{g})$ is countable. □

Prop. (3.7.9.10) [Generalized Eigenspace Decomposition for Nilpotent Lie Algebras]. Assume k is alg.closed, and $\mathfrak{g}$ is a nilpotent algebra, and (V,ρ) is a representation of $\mathfrak{g}$, then there is a generalized eigenspace decomposition

$$V=\oplus_{\lambda\in\mathfrak{g}^*}V^\lambda,$$

where V^λ are the generalized eigenspaces, and they are stable under action of $\mathfrak{g}$. ⌟

Proof: We use an induction argument:

If each $a\in\mathfrak{h}$ has only one eigenvalue, then V is the generalized eigenspace V_λ for some function λ on $\mathfrak{h}$. Then it suffices to show that λ is linear. But this is because by Lie's theorem elements of $\mathfrak{h}$ has a common eigenvector.

If for some a_0, $\mathrm{ad}(a_0)$ has two eigenvalues. Now $\mathfrak{h}$ is nilpotent, so $\mathfrak{h}\subset\mathfrak{h}_0^{a_0}$, and hence $\pi(h)V_\lambda^{a_0}\subset V_\lambda^{a_0}$ for any λ by(3.7.1.12).

As k is alg.closed, V can be written as a sum of generalized eigenspaces of a_0, and each generalized eigenspace is a subrepresentation of $\mathfrak{h}$, thus we can use induction. □

Def. (3.7.9.11)[Casimir Operator]. Let $\mathfrak{g}$ be a semisimple Lie algebra of dimension n, and $\beta:\mathfrak{g}\times\mathfrak{g}\to k$ a non-degenerate invariant bilinear form on $\mathfrak{g}$. Let e_i be a basis of $\mathfrak{g}$ and e_i' be the dual basis under β, then $c=\sum e_ie_i'\in U(\mathfrak{g})$ is independent of the basis, and lies in the center of $U(\mathfrak{g})$.

Now the trace form β_V for a faithful representation $\mathfrak{g}\to\mathfrak{gl}_V$ of $\mathfrak{g}$ is non-degenerate and invariant(3.7.9.6), then the corresponding elements c_ρ is called the **Casimir element** of (V,ρ), and the action c_V of c_ρ on V is called the **Casimir operator** of (V,ρ).

The Casimir operator c_V is a $\mathfrak{g}$-module homomorphism, and has trace n. ⌟

Proof: The independence of basis is by(3.5.10.24). To show it is in the center of $\mathcal{U}(\mathfrak{g})$, Cf.[Mil13].P50**?**.

Casimir operator c_V is a $\mathfrak{g}$-module homomorphism follows from the fact c_ρ is in the center of $U(\mathfrak{g})$, and its trace is

$$\mathrm{tr}(c_V)=\sum_i\mathrm{tr}(e_ie_i')=\sum_i(\beta_V(e_i,e_i'))=n$$

□

Def. (3.7.9.12) [Unimodular Lie Algebras]. A f.d Lie algebra $\mathfrak{g}$ is called **unimodular** if $\wedge\,\mathrm{ad}$ is a trivial representation of $\mathfrak{g}$. ⌟

Prop. (3.7.9.13).

- If $\mathfrak{g}=[\mathfrak{g},\mathfrak{g}]$, then $\mathfrak{g}$ is unimodular.
- If $\mathfrak{g}$ is nilpotent, then $\mathfrak{g}$ is unimodular.
- If $\mathfrak{g}_1,\mathfrak{g}_2$ is nilpotent, then $\mathfrak{g}_1\oplus\mathfrak{g}_2$ is unimodular.
- If $\mathfrak{g}$ is reductive, then $\mathfrak{g}$ is unimodular.

⌟

Lemma (3.7.9.14) [Zassenhaus]. Let $\mathfrak{g}$ be a Lie algebra and $\mathfrak{g}'$ an ideal of $\mathfrak{g}$. A representation ρ' of $\mathfrak{g}'$ extends to a representation ρ of $\mathfrak{g}$ that $\mathfrak{n}_{\rho'}(\mathfrak{g}')\subset\mathfrak{n}_\rho(\mathfrak{g})$ if there exists a Lie subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ that $\mathfrak{g}=\mathfrak{g}'\oplus\mathfrak{h}$ and $[\mathfrak{h},\mathfrak{g}']\subset\mathfrak{n}_{\rho'}(\mathfrak{g}')$. If moreover $\mathrm{ad}_{\mathfrak{g}}(x)|_{\mathfrak{g}'}$ is nilpotent for all $x\in\mathfrak{h}$, then ρ can be chosen that $\mathfrak{h}\subset\mathfrak{n}_\rho(g)$. ⌟

Proof: Cf.[Mil13]P65. □

Prop. (3.7.9.15)[Nilpotent Representation Extension]. Let $\mathfrak{g}$ be a Lie algebra, $\mathfrak{a}$ a nilpotent ideal of $\mathfrak{g}$, and ρ a representation of $\mathfrak{a}$ that $\rho(x)$ is nilpotent for all $x \in \mathfrak{a}$. Then ρ extends to a representation ρ' of $\mathfrak{g}$ that $\rho'(x)$ is nilpotent for all $x \in \mathfrak{n}$ the largest nilpotent ideal of $\mathfrak{g}$. ⌟

Proof: □

Thm. (3.7.9.16) [Ado]. Let $\mathfrak{g}$ be a Lie algebra over a field k of char0, then there exists a faithful representation ρ of $\mathfrak{g}$ that $\rho(\mathfrak{n})$ consists of nilpotent endomorphisms, where $\mathfrak{n}$ is the largest nilpotent radical. If $\mathfrak{g}$ is of f.d., then this representation can be chosen to be of f.d.. In particular, any finite dimensional Lie algebra can be embedded in some $\mathfrak{gl}(n, k)$. ⌟

Proof: This is true for any commutative Lie algebras, for example we can use tensor products of $c \mapsto \begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix}$. Choose a faithful representation of the center $\mathfrak{c}$ of $\mathfrak{g}$ that every element is mapped to a nilpotent endomorphism, and then extend it to a representation ρ_1 of $\mathfrak{g}$ by(3.7.9.15). Let ρ_2 be the adjoint representation of $\mathfrak{g}$, and $\rho = \rho_1 \oplus \rho_2$. Then $\ker(\rho) = \ker(\rho_1) \cap \ker(\rho_2) = \ker(\rho_1) \cap \mathfrak{c} = 0$, so this is faithful. And it sends an element in $\mathfrak{n}$ to a nilpotent endomorphism because each ρ_1 and ρ_2 do. □

Remark (3.7.9.17). In fact, this is true for Lie algebras over a field of char p, too, Cf.[JACOBSON, N. 1962. Lie algebras.]Chap 6.3. ⌟

Semisimple Representations

For representations of a semisimple Lie algebra, See18.8.

10 Lie Algebra Cohomology

Main references are [Wei94] and [Eti21].

Prop. (3.7.10.1) [Chevalley-Eilenberg resolution]. ⌟

11 Amitsur-Levitski

Preliminary

Notice that in this paper, Kostant considers **reductive** lie groups. But in the range of this paper, the abelian part makes no contribution in the alternative part because they commutes with all elements. So We well just consider a **semisimple** Lie algebra in order to get a non-degenerate Killing form.

Prop. (3.7.11.1).

$$\Gamma(\wedge^{2k}(\mathfrak{g})) = R^k \in S^k(\mathfrak{g})$$

$$\Gamma(x_1 \wedge \cdots \wedge x_k) = \sum_{v \in \Pi_k} [x_{v(1)}, x_{v(2)}] \cdots [x_{v(2k-1)}, x_{v(2k)}]$$

⌟

Proof: The proof is in fact simple, just notice that for every $v \in \Pi_k$ a representative of the subgroup $\Sigma_{2k,2}$ permuting the unordered pairs $\{(1,2),(3,4),\dots,(2k-1,2k)\}$,the element in $v\Sigma_{2k,2}$ in fact combine in pairs to $[x_{v(2i-1)}, x_{v(2i)}]$ and together the $k!$ permutation of them compose a $[x_{v(1)}, x_{v(2)}]\cdots[x_{v(2k-1)}, x_{v(2k)}]$. □

Later he finds the dual of Γ,that is:

Prop. (3.7.11.2). γ is $\mathcal{B}$ dual to Γ,

$$(\Gamma(\zeta), y_1 \cdots y_r) = (-1)^r(\zeta, dy_1 \wedge \cdots \wedge dy_r) \qquad \forall \zeta \in \wedge^{2r}\mathfrak{g} \text{ and } y_i \in \mathfrak{g}.$$

In particular,

$$\Gamma(\zeta)(x) = \frac{(-1)^r}{r!}(\zeta, (dx)^r) \qquad \forall \zeta \in \wedge^{2r}\mathfrak{g} \text{ and } x \in \mathfrak{g}.$$

⌟

For the proof just notice that $(-dw, x_i \wedge x_j) = (w_i, [x_i, x_j])$ and

$$(x_1 \otimes \cdots \otimes x_r, y_1 \otimes \cdots \otimes y_r) = \sum_\sigma (x_1, y_{\sigma(1)}) \cdots (x_r, y_{\sigma(r)})$$

So dim of R^k equals the dim of image of γ_r,that is, spanned by $(dx)^k$(because they are dual).

We say that a representation of $\mathfrak{g}$ satisfies m-fold standard identity if the alternating sum of any m elements of image of $\mathfrak{g}$ is 0.Obviously, this is equivalent to:

$$\tau(R^k(\mathfrak{g})) \subset \ker \pi_V$$

Now let $o(\mathfrak{g})$ be the maximum rank of $dw, w \in \mathfrak{g}$,then by the discussion of the first paper, when $\mathfrak{g}$ is semisimple,$o(\mathfrak{g}) = r$.So the $2r$-identity is satisfied by any representation of $\mathfrak{g}$.

Furthermore a prop of [Harish-Chandra] assert for any nonzero element $u \in U(\mathfrak{g})$,there is a representation such that $\pi(U) \neq 0$.So this is a sharp bound for general representations.

But one might naturally ask:Can we find the specific bound for a particular representation of a specific $\mathfrak{g}$?The answer is YES.

Prop. (3.7.11.3). γ vanishes on the ideal $J'_+ \cdot S(\mathfrak{g})$. ⌟

Proof: The proof comes from the observation π is a G-map and by **Cartan-Koszul** theory, invariant elements in $\wedge\mathfrak{g}$ are naturally isomorphic to the cohomology of $\mathfrak{g}$ and $\gamma(w) = -dw$ is clearly exact,Thus $\gamma(w_1 w_2 \dots w_i) = (-1)^i dw_1 \wedge \cdots \wedge dw_i$ is exact too. So $\gamma(w) = 0$.

□

Cor. (3.7.11.4). $M = R^r \in H^r$, so it consists of harmonic functions. ⌟

Proof: $(u, \Gamma(y)) = (\gamma(u), y) = 0$ $\forall u$ invariant, by Thm; so R^k =Image Γ is harmonic. □

Generalized Amitsur-Levitski

Let $E^k \subset U(\mathfrak{g})$ be spanned be y^k, y nilpotent in $\mathfrak{g}$,and Z the center.

in [Kos97] Kostant proved that the PBW isomorphism $\delta : S(\mathfrak{g}) \longrightarrow U(\mathfrak{g})$ induces $\delta(J) = Z$,$\delta(H) = E$.

so $\tau : T(\mathfrak{g}) \longrightarrow U(\mathfrak{g})$ induces

$$\tau(A^{2k}(\mathfrak{g})) = \delta(R^k(\mathfrak{g})) \subset E^k.$$

Define $\epsilon(\pi)$ the minimum integer k that $\pi(y)^k = 0, \forall y$ nilpotent in $\mathfrak{g}$.Then clearly:

Prop. (3.7.11.5) [Generalized Amitsur-Levitski]. π satisfies the $2\epsilon(\pi)$-fold standard identity. ⌟

Prop. (3.7.11.6). If π satisfies the m-identity, it satisfies the $m+1$-identity(By taking a summation on a fixed first element $\sigma(1)$). ⌟

Prop. (3.7.11.7).

- Let π be the natural representation of $\mathfrak{gl}_n$ on $\mathbb{C}^n$ then $\epsilon(\pi) = n$.
- If n even and π the natural representation of skew-symmtric matrixs on $\mathbb{C}^n$ then $\epsilon(\pi) = n-1$.

From this one derives the **classical Amitsur-Levitski prop** that $GL_n(\mathbb{C})$ satisfies the n-fold standard identity. ⌟

Proof: 1: the **abstract Jordan decomposition** which assures x is nilpotent in $\mathfrak{gl}_n$ if $\pi(x)$ is nilpotent.

2: comes from the **Lacobson-Morosov** Thm that any nilpotent element of $\mathfrak{g}$ is contained in a $\mathfrak{sl}_2$-triple. Thus we only need to show that W is reducible considered as this $\mathfrak{sl}_2$-triple-module.

But then an irreducible representation of $\mathfrak{sl}_2$ preserves a non-degenerate bilinear form it must be odd dimensional cause a non-degenerate bilinear form is equivalent to a $\mathfrak{g}$-map from V to V^*.

And there can be constructed an anti-symmetric form defined on the $\mathfrak{sl}_2$-representation on $\mathrm{Sym}_{2k}[x,y]$ by(3.7.11.9), so there can't exist symmetric $\mathfrak{g}$-invariant form. So this representation must be reducible. □

Cor. (3.7.11.8) [Classical Amitsur-Levitski]. By(3.7.11.5),

$$[[x_1, x_2, \ldots, x_n]] = \sum_\sigma \mathrm{sgn}(\sigma) x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(k)} = 0 \qquad \forall x_i \in \mathfrak{gl}_n$$

called n-fold **standard identity**.
⌟

Prop. (3.7.11.9). For a construction of the anti-symmetric form, notice

$$\pi(g) f(x_1, x_2) = f(g_{11}x_1 + g_{12}x_2, g_{21}x_1 + g_{22}x_2).$$

Set

$$v_k = \binom{m}{k} x_1^{m-k} x_2^k, \quad \Omega(v_k, v_{m-k}) = (-1)^k \binom{m}{k}. \quad \Omega(v_k, v_p) = 0, \qquad k+p \neq m.$$

One verifies:

$$\Omega(g \cdot u, g \cdot v) = (\det g)^m \Omega(u, v) \qquad \forall g \in \mathrm{GL}(2, \mathbb{C})$$

So when $m = n-1$ is odd, this is a symplectic form preserved by $\mathfrak{sl}_2$. ⌟

A computable Formula

Finally, Kostant gave a computable formula for determining $\epsilon(\pi)$.Clearly we just need to consider irreducible representation.

Let π_λ be the irreducible representation of highest weight λ,then the dual representation $\pi_{\lambda'}$ has highest weight the negative of the lowest weight of π_λ,that is, $-w_o(\gamma)$.

But then $\lambda + \lambda'$ is a sum of simple positive roots.$\lambda + \lambda' = \sum_{i=1}^n m_i \alpha_i$.Put $\epsilon(\lambda) = 1 + \sum_{i=1}^n m_i$.then:

Prop. (3.7.11.10). $\epsilon(\pi_\lambda) = \epsilon(\lambda)$. ⌟

Proof: Just choose a $\mathfrak{sl}_2$-triple $\{e, x, f\}$ with $\alpha(x) = 2\ \forall \alpha$ simple root.Then $\lambda(x)$ and $-\lambda'(x)$ are respectively the maximal and minimal eigenvalues of $\pi(x)$. $(\lambda + \lambda')(x) = 2(\epsilon(\lambda) - 1)$. Thus f has nilpotent degree $\epsilon(\lambda)$.And any nilpotent element action increases the eigenvalue of a eigenvector of x by at lest 2, the prop follows. □

Further Work

(cf. [Pro76]) Another different proof of the Amitsur-Levitski theorem is given by Kostant using techniques related to **trace identities**. It turns out that method sheds more light. Later is studied the polynomial of matrices invariant under the conjugation action.

Artin conjectured that all the invariants is polynomials of the Trace polynomial $Tr(A_1A_2\cdots A_n)$(Proved)

And further, the relations among these invariant all turned out to be consequences of the prop of Hamilton-Cayley. All this is made into the **Invariant Theory**.

Prop. (3.7.11.11) [Interesting results].

1. If an algebra over a field of characteristic 0 satisfies the identity $X^n=0$,then it satisfies all the identities of $n\times n$ matrices.
2. The space of multilinear identities of degree m of $n\times n$ matrices can be described completely in terms of Young diagrams.

⌟

12 Lie p-Algebras

Remark (3.7.12.1). In this subsection, let k be a field of characteristic p. ⌟

Def. (3.7.12.2) [Lie p-Algebras]. Let x_0,x_1 be elements of a Lie algebra over k of characteristic p, then for $0<r<p$, let $s_r(x_0,x_1)$ denote $\frac{1}{r}$ times coefficient of t^{r-1} in the expression of $\mathrm{ad}^{p-1}_{tx+y}(x)$.

Then a **Lie p-algebra** is a Lie algebra $\mathfrak{g}$ over k equipped with a map $x\mapsto x^{[p]}:\mathfrak{g}\to\mathfrak{g}$ such that

- $(cx)^{[p]}=c^px^{[p]}$ where $c\in k$.
- $\mathrm{ad}(x^{[p]})=(\mathrm{ad}(x))^p$.
- $(x+y)^{[p]}=x^{[p]}+y^{[p]}+\sum_{r=1}^{p-1}s_r(x,y)$.

⌟

Example (3.7.12.3). If L is an Abelian Lie algebra, then it can be regarded as a Lie p-algebra by assigning $x^{[p]}=0$.

If A is an associative algebra, then it can be given a Lie p-algebra structure by assigning $x^{[p]}=x^p$. ⌟

Proof: To show A is a Lie p-algebra, we check $\mathrm{ad}(x)^p(y)=(l_x-r_x)^p(y)=l_x^p-r_x^p(y)=\mathrm{ad}(x^p)(y)$. For the third formula, notice

$$\mathrm{ad}(tx+y)^{p-1}(x)=\sum_{i=0}^{p-1}(-i)^i\binom{p-1}{i}(tx+y)^{p-1-i}x(tx+y)^i$$

Notice that $(-i)^i\binom{p-1}{i}\equiv 1\mod p$, so $s_r(x,y)$ is equivalent to the sum of words of x,y with r xs. So the third formula clearly holds. □

Def. (3.7.12.4) [Representations]. A **representation of a Lie p-algebra** $\mathfrak{g}$ over a k-vector space V is a homomorphism $\mathfrak{g}\to\mathfrak{gl}_V$ of Lie p-algebras. ⌟

Def. (3.7.12.5) [Universal Enveloping p-Algebra]. The **universal enveloping p-algebra** of a Lie p-algebra $\mathfrak{g}$ is defined to be

$$U^{[p]}(g) = T(\mathfrak{g})/J^{[p]}, \quad T(\mathfrak{g}) = \bigoplus_{n=0}^{\infty} \mathfrak{g}^{\otimes n}$$

which is a graded algebra $T(\mathfrak{g})$ quotients the ideal $J = (\{x \otimes y - y \otimes x - [xy], x^{\otimes p} - x^{[p]}\})$.
There is a natural linear map $\sigma : \mathfrak{g} \to U^{[p]}(\mathfrak{g})$. ⌟

Prop. (3.7.12.6). The universal enveloping p-algebra $U^{[p]} : \mathfrak{g} \mapsto U^{[p]}(\mathfrak{g})$ defines a functor $LiepAlg \to AssAlg$ that is left adjoint to the canonical functor $AssAlg_k \to LiepAlg_k$(3.7.12.3). ⌟

Proof: For any associative algebra A and a morphism of Lie p-algebras $\mathfrak{g} \to [A]$, there is easily seen a morphism $U^{[p]}(\mathfrak{g}) \to A$, and it is unique. □

Cor. (3.7.12.7) [Representation as Modules]. A representation of a Lie-p-algebra $\mathfrak{g}$(3.7.12.4) is the same as a representation of $U^{[p]}(\mathfrak{g})$. ⌟

Prop. (3.7.12.8). Let e_i be a k-vector space basis of $\mathfrak{g}$, then the monomials

$$\{e_{i_1}^{n_{i_1}} e_{i_2}^{n_{i_2}} \ldots e_{i_r}^{n_{i_r}} | i_1 < i_2 < \ldots < i_r, 0 < n_{i_k} < p\}$$

for different r form a basis of $U^{[p]}(\mathfrak{g})$. ⌟

Proof: This is a consequence of PBW theorem(3.7.8.4). □

Cor. (3.7.12.9). If $\mathfrak{g}$ is of finite dimensional over k, then so does $U^{[p]}(\mathfrak{g})$, and the map $i : \mathfrak{g} \to U^{[p]}(\mathfrak{g})$ is injective. ⌟

3.8 Infinite Dimensional Lie Algebras

References are [What is moonshine?], [Vertex Operator Algebras and the Monster], [Infinite-Dimensional Lie Algebras, Kac], [Car05].

1 Kac-Moody Algebras

2 Vertex Operator Algebras

3 Moonshine Conjectures

Thm. (3.8.3.1) [Monstrous Moonshine]. There is a naturally defined graded infinite dimensional module, called the **Monstrous module** $V=\oplus_{n\in\mathbb{Z}}V_n$ of the monster group $\mathbb{M}$ s.t. for any $g\in\mathbb{M}$, the Mckay-Thompson series

$$T_g(\tau)=\sum_{n\geq -1}\mathrm{tr}(g|V_n)e^{2\pi inr}$$

is a Hauptmodul for a discrete subgroup $\Gamma\subset SL(2,\mathbb{Z})$ of genus 0 and period r at the cusp. ⌟

Proof: Cf.[Borcherds, 1992] □

Prop. (3.8.3.2) [Duncan-Mertens-Ono, 2017]. There exists an infinite dimensional module $V=\oplus_{n>0,n\equiv 0,3 \mod 4}V_n$ of the O'Nan group(3.1.12.5) $\mathbb{O}\mathbb{N}$ s.t. for any $g\in\mathbb{O}\mathbb{N}$, the Mckay-Thompson series

$$F_g(\tau)=q^{-4}+2+\sum_{n>0}\mathrm{tr}(g|V_n)e^{2piin\tau}$$

is a meromorphic modular form of weight $\frac{3}{2}$ on $\Gamma_0(4N)$, where N is the order of g. ⌟

Proof: □

3.9 Reflection Groups and Coxeter Groups

Main references are [Hum90], [Ser87], [Kna96].

Notation (3.9.0.1).

- Let $k \in \texttt{Field}, \operatorname{char} k = 0, V \in \mathcal{V}\mathrm{ect}/k$.

⌟

1 Reflection Groups

Def. (3.9.1.1) [Reflections]. Let $V \in \mathcal{V}\mathrm{ect}^d/k$, a **reflection** on V is a linear transformation $s \in \operatorname{End}(V)$ that has $d-1$ eigenvalues 1 and one eigenvalue -1. ⌟

Prop. (3.9.1.2). Let $\alpha \in V$ and $\alpha^\vee \in V^\vee$ that $(\alpha, \alpha^\vee) = 2$, then

$$s_\alpha : x \mapsto x - (x, \alpha^\vee)\alpha$$

is a reflection, and every reflection with vector α is of this form. ⌟

Proof: Clearly s_α is a reflection, and if s is any reflection, then $\alpha^\vee$ is the composition of the quotient map $V \to V/H$ with the map $V/H \to \mathbb{F}$ sending $\alpha + H$ to 1. □

Lemma (3.9.1.3). Let $R \subset V$ be a set s.t. $\operatorname{span}\{R\} = V$, then for any $\alpha \in V$, there exists at most one reflection s with vector α that $s(R) \subset R$. ⌟

Proof: Let s, s' be two such reflections, then $t = ss'$ is an automorphism that is identity on both $\mathbb{F}\alpha$ and $V/\mathbb{F}\alpha$. So $(t-1)^2 = 0$ on V. So the minimal polynomial of T divides $(T-1)^2$. Also because R is finite there exists an m that $t^m = 1$ on R thus on V, so $t = 1$ as the greatest divisor of $(T-1)^2$ and $T^m - 1$ is $T - 1$. □

Lemma (3.9.1.4). Let V be an inner product space, then for any vector α, there exists a unique reflection s_α that respects the inner product, which is

$$s_\alpha(x) = x - 2\frac{(x,\alpha)}{(\alpha,\alpha)}\alpha.$$

⌟

Def. (3.9.1.5) [Reflection Groups]. $\Gamma \leq GL(n,k)$ is called a **reflection group** if it is generated by reflections. ⌟

Thm. (3.9.1.6) [Shephard-Todd-Chevalley]. Let $\Gamma \leq GL(n,k)$, then Γ is a reflection group iff $k[X_1, \ldots, X_n]^\Gamma$ is a polynomial ring. And in this case,

- There are homogenous alg.ind polynomials $p_1, \ldots, p_r$, $d_i = \deg(p_i)$, $d_1 \leq d_2 \leq \ldots \leq d_r$ s.t. $k[X_1, \ldots, X_n]^\Gamma = k[p_1, \ldots, p_r]$.
- $$\frac{1}{\#\Gamma}\sum_{\gamma\in\Gamma}\frac{\operatorname{tr}(\gamma)}{\det(1-\gamma T)} = \prod_{i=1}^r \frac{1}{1-T^{d_i}} \in k(T).$$
- $(d_1, \ldots, d_r)$ are determined by Γ.
- $\#\Gamma = \prod_i d_i$, and Γ contains $\sum_i (d_i - 1)$ reflections.
- If Γ is an irreducible subgroup of $GL(n,k)$, then it is an abstractly irreducible group, and $Z(\Gamma)$ is cyclic of order $pgcd(d_1, \ldots, d_r)$.

⌟

Proof: □

2 Root Systems

Def. (3.9.2.1) [Root System]. A subset R of a vector space V over $\mathbb{F}$ is called a **root system** if

- R spans V and doesn't contain 0.
- For each $\alpha \in R$, there exists a unique reflection $s_\alpha = \mathrm{id} - \alpha^\vee \otimes \alpha$ with vector α that $s_\alpha(R) \subset R$.
- For any $\alpha, \beta \in R$, $s_\alpha(\beta) - \beta$ is a multiple of α, or equivalently $\alpha^\vee(\beta) \in \mathbb{Z}$.

Elements of R are called the **roots** of R, and dimension of V is called the dimension of the root system. And the subgroup of $GL(V)$ generated by all s_α is called the **Weyl group** of R. The Weyl subgroup is a finite group, as a subgroup of the group of permutations of R.

A root system is called indecomposable iff it cannot be written as a direct sum of two root systems. ⌟

Def. (3.9.2.2) [Reduced Root System]. Let α, β be roots that are multiples of each other, then $\beta = c\alpha$ for some $c \in \mathbb{F}$, then $2(\beta, \alpha^\vee) = 2c \in \mathbb{Z}$, also $2c^{-1} \in \mathbb{Z}$, so $c \in \{-1, -1/2, 1/2, 1\}$. A **reduced root system** is a root system that there are no roots α, β that $\alpha = 2\beta$. ⌟

Prop. (3.9.2.3) [Invariant Quadratic Form]. Let R be a root system in V, then there is a positive bilinear form in V that is invariant under the action of the Weyl group of R.

Notice that for such a bilinear form, the reflection must be of the form given in(3.9.1.4), or in other words, $\alpha^\vee(\beta) = (\frac{2\alpha}{(\alpha,\alpha)}, \beta)$. ⌟

Proof: This follows entirely because the Weyl group of R is finite, as we can take the average of any positive bilinear form under the action of reflections. □

Def. (3.9.2.4) [Dual Root System]. Let R be a root system in V, the set of dual vectors $\alpha^\vee$ for $\alpha \in R$ is also a root system in $V^\vee$, called the **dual system** of R. And it has the same Weyl group as R.

Moreover, $R^{\vee\vee} \cong R$. ⌟

Proof: Take an invariant quadratic form on V(3.9.2.3), then it gives an isomorphism $V \to V^\vee$. Then $\alpha^\vee$ corresponds to $\frac{2\alpha}{(\alpha,\alpha)}$ under this isomorphism, and there obviously generates V. If $\alpha^\vee \in R^\vee$, we can take the corresponding reflection to be $s_{\alpha^\vee} = 1 - \alpha \otimes \alpha^\vee$. Then

$$\begin{aligned} s_{\alpha^\vee}(\beta^\vee)(x) &= (\beta^\vee - \beta^\vee(\alpha)\alpha^\vee)(x) \\ &= (x, 2\beta/(\beta,\beta)) - \frac{(\alpha,\beta)}{(\beta,\beta)}(x, 2\alpha/(\alpha,\alpha)) \\ &= (x, \frac{2(\beta - \alpha(\alpha,\beta)/(\alpha,\alpha))}{(\beta,\beta)}) \\ &= (x, \frac{2s_\alpha(\beta)}{(\beta,\beta)}) = (s_\alpha(\beta))^\vee(x). \end{aligned}$$

So $s_{\alpha^\vee}(\beta^\vee) = (s_\alpha(\beta))^\vee \in R^\vee$. In this way, we see $\alpha^{\vee\vee} = \alpha$, and $s_{\alpha^\vee}(\beta^\vee) - \beta^\vee = \beta^\vee(\alpha)\alpha^\vee$ is an integral multiple of $\alpha^\vee$. Also it can be seen easily from the formula above that the Weyl group is the same as the Weyl group of R. □

Prop. (3.9.2.5) [Real Root Systems]. Let R be a roots system in a vector space V over a field $\mathbb{F}$, and let V_0 be the $\mathbb{Q}$-vector space spanned by R, then R is a root system in V_0 and $V_0 \otimes_{\mathbb{Q}} \mathbb{F} \cong V$.

So from now on we focus on a real root system. ⌟

Proof: The non-trivial part is that the isomorphism $V_0 \otimes_{\mathbb{Q}} \mathbb{F} \cong V$. The natural map $i : V_0 \otimes_{\mathbb{Q}} \mathbb{F} \to V$ is surjective because R generates V, and consider its transpose

$$i^* : V^\vee \to V_0^\vee \otimes_{\mathbb{Q}} \mathbb{F},$$

then we can see that this maps $\alpha^\vee$ to $\alpha_0^\vee$, and $R_0^\vee$ is a root system in $V_0^\vee$(3.9.2.4), thus $\alpha_0^\vee$ generates $V_0^\vee$, and i^* is surjective, showing i is injective. □

Def. (3.9.2.6) [Base]. A subset $S \subset R$ is called a **base** of R if the every elements of R can be written uniquely as a linear integral combination of elements of S with the same sign.

If S is a base of R, then we let R^+ denote the set of R that is non-negative integral combinations of elements of S, called the **positive roots of** R, and R^- the set of R that is non-positive integral combinations of elements of S, called the **negative roots of** R. $R = R^+ \coprod R^-$. ⌟

Prop. (3.9.2.7) [Base exists]. Let $t \in V^\vee$ be an element that $t(\alpha) \neq 0$ for all $\alpha \in R$. Let $R_t^+ (R_t^-)$ be the set of all $\alpha \in R$ that $t(\alpha) > 0 (< 0)$, then $R = R_t^+ \cup R_t^-$. An element of R_t^+ is called **indecomposable** if it cannot be written as the sum of two elements in R_t^+. Let S_t be the set of indecomposable elements of R_t^+, then S_t is a base of R.

In particular, every root system (R, V) contains a base. And if S is a base and $t \in V^\vee$ that $t(S) > 0$, then $S = S_t$. ⌟

Proof: Cf.[Ser87]P38. □

Cor. (3.9.2.8). If $t \in V^\vee$ and S_t is a basis of V contained in R_t^+ that attains the minimal value of t in R_t^+, then S_t is a base of R. ⌟

Prop. (3.9.2.9). Let S be a base of a root system (R, V), then every positive root β can be written as

$$\beta = \alpha_1 + \ldots + \alpha_k$$

in such a way that all the partial sums are roots. ⌟

Proof: Cf.[Ser87]P40. □

Prop. (3.9.2.10). Let R be a reduced root system and S a base, then for any $\alpha \in S$,

$$s_\alpha(R^+ \backslash \{\alpha\}) = R^+ \backslash \{\alpha\}.$$

In particular if $\rho = \frac{1}{2}(\sum_{\alpha \in R^+} \alpha)$, then $s_\alpha \rho = \rho - \alpha$. ⌟

Proof: If $\beta \in R^+$, then $s_\alpha(\beta) = \beta - c\alpha$ for some $c > 0$, Thus $s_\alpha(\beta) \in R^-$ iff $\beta = \alpha$. □

Prop. (3.9.2.11) [Base and Dual System]. Let R be a reduced system and S a base, then $S^\vee$ is a base of $R^\vee$. ⌟

Proof: By the isomorphism between V and $V^\vee$, it suffices to show the vectors $\{\alpha^\vee, \alpha \in S\}$ is a base for $R^* = \{\alpha^\vee, \alpha \in R\}$. But it is clear if S is a base corresponding to a vector $t \in V^*$, then $\{\alpha^\vee, \alpha \in S\}$ is the extremal vectors corresponding to t too, so it is a base by(3.9.2.7). □

Property of the Weyl Group

Prop. (3.9.2.12) [Weyl Group and Bases]. Let W be the Weyl group of a reduced root system R and S a base of R, then

1. For any $t \in V^*$, there exists $w \in W$ that $(w(t), \alpha) \geq 0$ for all $\alpha \in S$.
2. W acts transitively on the set of bases of R.
3. For each $\beta \in R$, there exists some $w \in W$ that $w(\beta) \in S$.
4. The group W is generated by s_α where $\alpha \in S$.
5. W acts simply transitively on the set of bases of R.

⌟

Proof: We can in fact prove this for W_S the group generated by s_α where $\alpha \in S$.

1: Let ρ be defined in(3.9.2.10), and choose an element $w \in W_S$ that $w(t)(\rho)$ is maximal, then $w(t)(\rho) \geq w(t)s_\alpha(\rho) = w(t)(\rho) - w(t)(\alpha)$. So $(w(t), \alpha) \geq 0$.

2: Let S' be a base and $t' \in V^\vee$ that $t'(S') > 0$(3.9.2.7), Also by 1 we can find $w \in W$ that $w(t)(\alpha) \geq 0$ for all $\alpha \in S$. And in fact $w(t)(\alpha) > 0$ for all $\alpha \in S$. So $S = S_t, S' = S_{w(t)}$. Thus w sends S' to S.

4: Finally we prove that $W_S = W$: because for any $\beta \in R$, there exists $w \in W_S$ that $w(\beta) \in S$, so $s_\beta = w^{-1} s_{w(\beta)} w \in W_S$.

5: See [Ser87]P70.**?** □

Def. (3.9.2.13) [Length]. Let $w \in W$, define the **length** of w to be the minimal number m that w can be written as a product of m simple reflections s_i. ⌟

Prop. (3.9.2.14). Let R be a root system with Weyl group W, $w \in W$.

- Let $n(w)$ be the number of elements α in R^+ that $w(\alpha) \in R^-$, then $n(w) = l(w)$.
- There is a unique element $w_0 \in W$ with length $|R^+|$.
- $w_0(R^+) = R^-$, and $w_0^2 = \mathrm{id}$.

⌟

Proof: 1: Cf.[Carter, P63]**?**.

2: By(3.9.2.12) there is a unique element $w_0 \in W$ mapping S to $-S$, and it has maximal length $|R^+|$ by item1.

3: $w_0^2(R^+) = R^+$, thus $l(w_0^2) = 0$ and $w_0^2 = \mathrm{id}$. □

Def. (3.9.2.15) [Weyl Chambers]. Let (V, R) be a real root system, then a **Weyl chamber** is a connected component of $V \backslash \bigcup_{\alpha \in R} H_\alpha$, where H_α is the fixed hyperplane of vectors fixed by s_α. ⌟

Prop. (3.9.2.16). The Weyl group W acts transitively on the set of Weyl chambers of R. ⌟

Proof: To show the action is transitive, if two Weyl chambers C, C' are adjacent with a common face $F \subset H_\alpha$, then clearly $s_\alpha(C) = C'$. In general, choose two generic vector in C, C' and connect them, then C, C' can be connected by adjacent chambers.

If $w \in W$ satisfies $w(C) = C$, we may assume C is the fundamental Weyl chamber, then $w(S) = S$, so by(3.9.2.14), $l(w) = 0$, so $w = \mathrm{id}$. □

Def. (3.9.2.17) [Height of Weights]. Let $\alpha = \sum n_i \alpha_i \in R$, then the **height of roots** α is denoted by $\mathrm{ht}(\alpha) = \sum n_i$. ⌟

Prop. (3.9.2.18) [Highest Root]. Let (R, V) be a root system and S a base. If S is indecomposable, then there exists a root $\widetilde{\alpha} = \sum_{\alpha\in S} n_\alpha \alpha$ that for any other root $\sum_{\alpha\in S} m_\alpha\alpha$, $n_\alpha \geq m_\alpha$. ⌟

Proof: □

Def. (3.9.2.19) [Kostant's Partition Function]. Let R be a root system, the **Kostant's partition function** $\mathfrak{P}$ is a function on $Q(R)$ that $\mathfrak{P}(\alpha)$ equals the number of ways to write α as an unordered sum of positive roots in R^+. ⌟

Cartan Matrix and Dynkin Diagrams

Prop. (3.9.2.20) [Angles Between Roots]. Let α, β be two non-propositional roots in a root system R, then we can put $n(\alpha, \beta) = \alpha^\vee(\beta) = 2(\alpha, \beta)/(\alpha, \alpha)$. Then $n(\alpha, \beta)$ are integers(3.9.2.1), and $n(\alpha, \beta)n(\beta, \alpha) = 4\cos^2 \varphi_{\alpha,\beta}$, where $\varphi_{\alpha,\beta}$ is the angle between these two vectors. Then because $4\cos^2 \varphi_{\alpha,\beta}$ is an integer, it can only take values $0, 1, 2, 3$. Then there are only 7 possibilities of the angles between α, β, and if α, β are not orthogonal, their ration of lengths are determined also by the angle. ⌟

Prop. (3.9.2.21) [String of Roots]. If α, β are not proportional and $n(\beta, \alpha) > 0$, then $\alpha - \beta$ is a root. In particular, for $\alpha, \beta \in S$ where S is a base of R, $n(\alpha, \beta) \leq 0$. ⌟

Proof: (3.9.2.20) shows $n(\beta, \alpha) = 1$ or $n(\alpha, \beta) = 1$. Now $\alpha - \beta = s_\beta(\alpha)$ or $-s_\alpha(\beta)$ is a root of R. □

Def. (3.9.2.22) [Cartan Matrix]. Let R be a root system with a base S. Then the **Cartan matrix** is $(n(\alpha, \beta))_{\alpha,\beta\in S}$(3.9.2.20). ⌟

Prop. (3.9.2.23). The Cartan matrix depends only on (V, R) and not on S, and if R is reduced, R is determined by its Cartan matrix up to isomorphisms. ⌟

Proof: The first assertion follows from(3.9.2.12) as every two bases are conjugate. The Cartan matrix determines R because it determined the inner product between roots in a basis of V. □

Prop. (3.9.2.24). Let E be the group of automorphisms of S that leaves that Cartan matrix invariant, then it can be identified with the set of automorphisms of R that leave the base S invariant. Then the group $\mathrm{Aut}(R)$ is isomorphic to the semi-product $E \ltimes W$. ⌟

Proof: Let W is generated by s_α so invariant under $\mathrm{Aut}(R)$. Now if $u \in \mathrm{Aut}(R)$, then $u(S)$ is a base of R, so there exists some $w \in W$ that $w(u(S)) = S$, thus $u \in EW$. Also if $w \in W \cap E$, then □

Def. (3.9.2.25) [Coxeter graph]. A **coxeter graph** is a finite graph that each pair of distinct vertices are connected by $0, 1, 2$ or 3 vertices. ⌟

Def. (3.9.2.26) [Coxeter Graph associated to a Root System]. Let (R, V) be a root system and S a base of R, then the associated **coxeter graph** is a graph whose nodes are indexed by the elements of S, and two distinct nodes α, β are connected by $a(\beta, \alpha)a(\alpha, \beta) = 4\cos^2 \varphi_{\alpha,\beta}$ edges(3.9.2.20). This is independent of the choice of S, by(3.9.2.23). ⌟

Prop. (3.9.2.27). R is indecomposable iff the Coxeter graph is connected. ⌟

Proof: By the formula in(3.9.1.4), R is decomposable iff $R = R_1 \coprod R_2$ where R_1, R_2 are orthogonal to each other. Then this is equivalent to $\varphi_{\alpha,\beta} = \pi/2$ for any $\alpha \in R_1, \beta \in R_2$. □

3 Simple Root System

Lemma (3.9.3.1) [Listing of Indecomposable Root Systems]. The coxeter graphs Γ arising from indecomposable root systems are exactly the graphs $A_n(n \geq 1), B_n(n \geq 2), D_n(n \geq 4), E_6, E_7, E_8, F_4, G_2$. (graphs are given in [Etingod, Lie algebras]P109.) ⌟

Proof: The existence is these types are given by(3.9.3.2).

For the converse, notice first that for a graph with vertices v_i and v_i, v_j are connected with A_{ij} edges, the quadratic form

$$Q(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^2 - \sum_{1 \leq i < j \leq n} \sqrt{A_{ij}} x_i x_j = || \sum x_i v_i ||^2$$

is positive definite.

Next we show some constraints on the graph:

- Any subgraph of the coxeter graph, it can be shown that the corresponding quadratic form is also positive definite, in particular non-degenerate.
- : It is a tree: If it contains a circle, consider the subgraph of the circle, then the corresponding quadratic form vanishes on $(1, 1, \ldots, 1)$, contradiction.
- It doesn't contains subgraphs listed in P77 of[Car05].

Now if Γ contains a triple edge, then it must be G_2, otherwise it must contain a $\widehat{G}_2$. If Γ contains no triple edges, then it contains at most one double edge, otherwise it contains some $\widehat{C}_l$, $l \geq 2$. If it contains only one double edge, then it contains no branch points, otherwise it contains some $\widehat{B}_l, l \geq 3$, so it is a chain with an edge added. If the double edge is in one end, then it is B_l for some $l \geq 3$, otherwise it must by F_4, in order not to contain $\widehat{F}_4$.

Now we assume Γ contains only simple edges. If it contains no branch point, then it is A_l for some $l \geq 1$. But Γ contains at most one branch point, and only 3 edges, otherwise it contains some $\widehat{D}_l, l \geq 4$. If Γ has only one branch point, then the graph is a center with three branches. One of the branch must be a single vertex, otherwise it contains a $\widehat{E}_6$. Then a second branch must has≤ 2 vertices, otherwise it contains a $\widehat{E}_7$. If the second branch has a single vertex, then $\Gamma \cong D_l$ for some $l \geq 4$. If the second branch has two vertices, then the third branch has≤ 4 vertices, otherwise it contains some $\widehat{E}_8$. So $\Gamma \cong E_6, E_7$ or E_8. □

Prop. (3.9.3.2) [Listing of Indecomposable Root Systems]. Let e_n be the standard basis of $\mathbb{R}^n$ with the standard bilinear form, and let L_n be the subgroup generated by e_n. Then

- A_n: Let V be the hyperplane of $\mathbb{R}^{n+1}$ orthogonal to the vector $e_1 + \ldots + e_{n+1}$, and R be the subset of $L_{n+1} \cap V$ consisting of vectors of length $\sqrt{2}$. Then (R, V) is a root system, and the Weyl group is the permutation group S_n of $e_1, \ldots, e_{n+1}$. The polarization with $t(e_i) = n+1-i$ gives a base consisting of $\{e_i - e_{i+1},\ i = 1, \ldots, n\}$ by(3.9.2.8).
- B_n: Let $V = \mathbb{R}^n$ and R be the subset of L_n consisting of vectors of length 1 or $\sqrt{2}$. Then (R, V) is a root system, and the Weyl group is the permutation and sign changes of the vectors e_i, isomorphic to $\mathbb{Z}_2^n \rtimes S_n$. The polarization with $t(e_i) = n + 1 - i$ gives a base consisting of $\{e_1 - e_2, \ldots, e_{n-1} - e_n, e_n\}$ by(3.9.2.8).
- C_n: Let C_n be the dual system of B_n(3.9.2.4), which by the invariant form isomorphic to the set of $\mathbb{R}^n$ consisting of vectors $\pm e_i \pm e_j, \pm 2e_i$. It has the same Weyl group as B_n. It has a base consisting of $\{e_1 - e_2, \ldots, e_{n-1} - e_n, 2e_n\}$ by(3.9.2.8).

- D_n: Let $V = \mathbb{R}^n$ and R be the set of all vectors of L_n of length $\sqrt{2}$. The Weyl group consists of permutations and sign changes of an even number of the vectors e_i. The polarization with $t(e_i) = n - i$ gives a base consisting of $\{e_1 - e_2, \ldots, e_{n-1} - e_n, e_{n-1} + e_n\}$.
- G_2: Let $V = \mathbb{R}[\omega]$ and R be the subset of $\mathbb{Z}[\omega]$ of norm 1 or 3. The Weyl group is isomorphic to the dihedral group. It clearly has a base consisting of $\{1, \omega - 1\}$.
- F_4: Let $V = \mathbb{R}^4$, and let R be the set of vectors $\{\pm e_i, \pm e_i \pm e_j, \frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4)\}$. It can be shown this is a root system. The polarization with

$$t(\varepsilon_1) = 8, t(\varepsilon_2) = 3, t(\varepsilon_3) = 2, t(\varepsilon_3) = 1,$$

gives a base consisting of $\{e_2 - e_3, e_3 - e_4, e_4, \frac{1}{2}(e_1 - e_2 - e_3 - e_4)\}$.
- E_8: Let $V = \mathbb{R}^8$ and

$$R_{E_8} = \{\pm e_i \pm e_j, i \neq j\} \cup \{\frac{1}{2}(\sum_{i=1}^{8} \pm e_i) \text{ with even number of minus signs}\}.$$

The polarization with

$$t(e_1) = 23, t(e_2) = 6, t(e_3) = 5, \ldots, t(e_8) = 0$$

gives a base consisting of $\{e_2 - e_3, \ldots, e_7 - e_8, e_7 + e_8, \frac{1}{2}(e_1 - e_2 - \ldots - e_7 + e_8)\}$.
- E_7: E_7 is the intersection of E_8 with the hypersurface $\sum x_i = 0$, so

$$R_{E_7} = \{\pm(e_i - e_j), i \neq j\} \cup \{\frac{1}{2}(\sum_{i=1}^{8} \pm e_i) \text{ with 4 minus signs}\}.$$

The polarization with

$$t(\varepsilon_1) = 18, t(\varepsilon_2) = 7, t(\varepsilon_3) = 6, \ldots, t(\varepsilon_8) = 1$$

gives a base consisting of $\{\varepsilon_2 - \varepsilon_3, \ldots, \varepsilon_7 - \varepsilon_8, \frac{1}{2}(\varepsilon_1 - \varepsilon_2 - \varepsilon_3 - \varepsilon_4 - \varepsilon_5 + \varepsilon_6 + \varepsilon_7 + \varepsilon_8)\}$.
- E_6: E_6 is the intersection of E_7 with the hypersurface $x_7 + x_8 = 0$.

$$R_{E_6} = \{\varepsilon_i - \varepsilon_j | i \neq j \leq 6\} \cup \{\pm(\varepsilon_7 - \varepsilon_8)\} \cup \{\frac{1}{2}(\pm\varepsilon_1 \pm \varepsilon_2 \pm \ldots \pm \varepsilon_7) \pm \frac{1}{2}(\varepsilon_7 - \varepsilon_8) \text{ with 3 minus signs before } v_i, i \leq 6\}.$$

The polarization

$$t(\varepsilon_1) = 11, t(\varepsilon_2) = 4, t(\varepsilon_3) = 3, t(\varepsilon_4) = 2, t(\varepsilon_5) = 1, t(\varepsilon_6) = 0, t(\varepsilon_7) = 4, t(\varepsilon_8) = 3$$

gives a base consisting of $\{\varepsilon_2 - \varepsilon_3, \ldots, \varepsilon_5 - \varepsilon_6, \varepsilon_7 - \varepsilon_8, \frac{1}{2}(\varepsilon_1 - \varepsilon_2 - \varepsilon_3 - \varepsilon_4 + \varepsilon_5 + \varepsilon_6 - \varepsilon_7 + \varepsilon_8)\}$.

$A_n^\vee \cong A_n, B_n^\vee \cong C_n, D_n^\vee \cong D_n, G_2^\vee \cong G_2, F_4^\vee \cong F_4, E_8^\vee \cong E_8, E_7^\vee \cong E_7, E_6^\vee \cong E_6$. ⌟

Remark (3.9.3.3). The polarizations t are intimately related to the averaged coroot $\rho^\vee$ (3.9.3.12). ⌟

Def. (3.9.3.4) [Dynkin Diagram]. The coxeter graph cannot determine the root system up to isomorphism, because it cannot distinguish between $n(\alpha, \beta), n(\beta, \alpha)$. So there is a **Dynkin diagram** which is constructed from the coxeter diagram by adding a vector from the longer vector to the shorter vector when $n(\alpha, \beta)n(\beta, \alpha) = 2$ or 3. ⌟

Prop. (3.9.3.5) [Listing of Dynkin Diagrams]. The Dynkin diagrams arising from indecomposable root systems are exactly the diagrams $A_n(n \geq 1), B_n(n \geq 2), C_n(n \geq 3), D_n(n \geq 4), E_6, E_7, E_8, F_4, G_2$. (graphs are given in [Etingod, Lie algebras]P109.) ⌟

Proof: This follows easily from(3.9.3.1) and(3.9.3.2). □

Prop. (3.9.3.6) [Non-Reduced Root Systems]. For any $n \geq 1$, there is exactly one non-reduced indecomposable root system of rank n, which is BC_n, the union of B_n and C_n in(3.9.3.2). ⌟

Cor. (3.9.3.7). Cf.[Kna96]P139. ⌟

Weight Lattices

Def. (3.9.3.8) [Weight Lattice]. Let (R, V) be a root system, we can define the **root lattice** as the $\mathbb{Z}$-lattice $Q(R)$ generated by R, and also the **weight lattice** $P(R) = \{x \in V | \alpha^\vee(x) \in \mathbb{Z}, \forall \alpha \in R\}$ $P(R)$ has a generator by fundamental weights ω_i that $(\omega_i, \alpha_j^\vee) = \delta_{ij}$. Then $Q(R) \subset P(R)$, and $[P(R) : Q(R)]$ is finite as they are both complete lattices. ⌟

Prop. (3.9.3.9). Let $\rho = 1/2 \sum_i \alpha_i$, then $\rho = \sum_i \omega_i$. ⌟

Proof: It follows from(3.9.2.10) that $s_\alpha \rho = \rho - \alpha$, so $(\rho, \alpha_i^\vee) = 1$, thus $\rho = \sum_i \omega_i$ by definition(3.9.2.10). □

Prop. (3.9.3.10) [Weight Lattices of Indecomposable Root Systems]. Let R be a root system, notation as in(3.9.3.2),

- A_n: $\alpha_i^\vee = \alpha_i$ for $i \leq n$, so $\omega_i = (\frac{n+1-i}{n+1}, \ldots, \frac{n+1-i}{n+1}, \frac{-i}{n+1}, \ldots, \frac{-i}{n+1})$($i$ terms) for $1 \leq i \leq n$. Then $P = \{(x_i) \in \mathbb{R}^n | x_i - x_j \in \mathbb{Z}, \sum x_i = 0\}, Q = \{(x_i) \in \mathbb{Z}^n | \sum x_i = 0\}$, and $P/Q \cong \mathbb{Z}/(n+1)\mathbb{Z}$.
- B_n: $\alpha_i^\vee = \alpha_i$ for $i < n$ and $\alpha_n^\vee = 2e_n$, so $\omega_i = (1, \ldots, 1, 0, \ldots, 0)$($i$ ones) for $1 \leq i < n$, and $\omega_n = (\frac{1}{2}, \ldots, \frac{1}{2})$. Then $P = \mathbb{Z}^n$ and $Q = \mathbb{Z}^n \cup [(\frac{1}{2}, \ldots, \frac{1}{2}) + \mathbb{Z}^n]$, $P/Q \cong \mathbb{Z}/2\mathbb{Z}$.
- C_n: $\alpha_i^\vee = \alpha_i$ for $i < n$ and $\alpha_n^\vee = e_n$, so $\omega_i = (1, \ldots, 1, 0, \ldots, 0)$($i$ ones) for $1 \leq i \leq n$. Then $P = \{(x_i) \in \mathbb{Z}^n | \sum x_i \in 2\mathbb{Z}\}$ and $Q = \mathbb{Z}^n$, $P/Q \cong \mathbb{Z}/2\mathbb{Z}$.
- D_n: $\alpha_i^\vee = \alpha_i$ for $i \leq n$, so $\omega_i = (1, \ldots, 1, 0, \ldots, 0)$($i$ ones) for $1 \leq i \leq n-2, \omega_{n-1} = (\frac{1}{2}, \ldots, \frac{1}{2}), \omega_n = (\frac{1}{2}, \ldots, \frac{1}{2}, -\frac{1}{2})$. So $P/Q \cong (\mathbb{Z}/2\mathbb{Z})^2$ for n even and $\mathbb{Z}/4\mathbb{Z}$ for n odd.
- G_2: It is clear $\omega_1 = \omega + 1, \omega_2 = 2\omega + 1$. Then $P = Q = \mathbb{Z}[\omega]$.
- F_4: $\omega_1 = (1, 1, 0, 0), \omega_2 = (2, 1, 1, 0), \omega_3 = (\frac{3}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}), \omega_4 = (1, 0, 0, 0)$. So $P = Q = \frac{1}{2}\mathbb{Z}^4$.
- E_8: **?** $\omega_1 = (1, 1, 0, \ldots, 0)$, So $P = Q = \{(x_1, \ldots, x_8) | x_i \in \mathbb{Z}$ or $x_i \in \frac{1}{2} + \mathbb{Z}, \sum x_i \in 2\mathbb{Z}\}$.
- E_7:**?**, $P/Q \cong \mathbb{Z}/2\mathbb{Z}$.
- E_6: **?**, $P/Q \cong \mathbb{Z}/3\mathbb{Z}$.

⌟

Proof: □

Prop. (3.9.3.11) [Maximal Roots]. For A_n, the maximal root is $\theta = e_1 - e_{n+1} = \alpha_1 + \ldots + \alpha_n = \omega_1 + \omega_n$. For C_n, the maximal root is $\theta = 2e_1 = 2\alpha_1 + \ldots + 2\alpha_{n-1} + \alpha_n = 2w_1$.

But for any other indecomposable root system R, the maximal root θ is a fundamental root:

- B_n: $\theta = e_1 + e_2 = \alpha_1 + 2\alpha_2 + \ldots + 2\alpha_n = \omega_2$.

- D_n: $\theta = e_1 + e_2 = \alpha_1 + 2\alpha_2 + \ldots + 2\alpha_{n-2} + \alpha_{n-1} + \alpha_n = \omega_2$.
- G_2: $\theta = 2\omega + 1 = 3\alpha_1 + 2\alpha_2 = \omega_2$.
- F_4: $\theta = e_1 + e_2 = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4 = \omega_1$.
- E_8: $\theta = e_1 + e_2 = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 5\alpha_4 + 6\alpha_5 + 4e_6 + 3e_7 + 2e_8 = \omega_1$.
- E_7: $\theta = e_1 - e_8 = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6 + 2\alpha_7 = \omega_6$.
- E_6: $\theta = \varepsilon_1 - \varepsilon_6 = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 + \alpha_5 + 2\alpha_6 = \omega_4$.

⌟

Prop. (3.9.3.12) [ρ and $\rho^\vee$]. $\rho^\vee$ is ρ of the dual system $R^\vee$. Under the identification of V and V^*, If (R,S) is simply laced, then $R \cong R^\vee$ via $\alpha \mapsto \alpha^\vee$, so by(3.9.3.10),

- $A_n : \rho_{A_n} = \rho^\vee_{A_n} = (\frac{n}{2}, \frac{n-2}{2}, \ldots, -\frac{n}{2}) = \sum_i \frac{i(n+1-i)}{2}\alpha_i$.
- $B_n : \rho_{B_n} = \rho^\vee_{C_n} = (\frac{2n-1}{2}, \frac{2n-3}{2}, \ldots, \frac{3}{2}, \frac{1}{2}) = \sum_i \frac{i(2n-i)}{2}\alpha_i$.
- $C_n : \rho_{C_n} = \rho^\vee_{B_n} = (n, n-1, \ldots, 1) = \sum_{i\leq n-1} \frac{i(2n+1-i)}{2}\alpha_i + \frac{n(n+1)}{4}\alpha_n$.
- $D_n : \rho_{D_n} = \rho^\vee_{D_n} = (n-1, n-2, \ldots, 0) = \sum_{i\leq n-2} \frac{i(2n-1-i)}{2}\alpha_i + \frac{1}{2}\alpha_{n-1} + \frac{n(n-1)}{4}\alpha_n$.
- $G_2 : \rho_{G_2} = 3\omega + 2 = 5\alpha + 3\beta, \rho^\vee_{G_2} = \frac{10}{3}\omega + \frac{8}{3} = 6\alpha + \frac{10}{3}\beta$.
- $F_4 : \rho_{F_4} = (\frac{11}{2}, \frac{5}{2}, \frac{3}{2}, \frac{1}{2}), \rho^\vee_{F_4} = (8, 3, 2, 1)$.
- $E_8 : \rho_{E_8} = \rho^\vee_{E_8} = (23, 6, 5, 4, 3, 2, 1, 0)$.
- $E_7 : \rho_{E_7} = \rho^\vee_{E_7} = (18, 7, 6, \ldots, 1) - (\frac{23}{4}, \ldots, \frac{23}{4})$.
- $E_6 : \rho_{E_6} = \rho^\vee_{E_6} = (\frac{15}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{3}{2}, -\frac{5}{2}, -\frac{7}{2}, \frac{1}{2}, -\frac{1}{2})$.

⌟

Def. (3.9.3.13) [Coxeter Numbers]. Let (R,S) be an indecomposable root system, defined the **Coxeter root** to be $h_R = (\theta, \rho^\vee) + 1 = \mathrm{ht}(\theta) + 1$, and the **dual Coxeter number** $h^\vee_R = (\rho, (\theta)^\vee) + 1$. Clearly if (R,S) is simply laced, then $R \cong R^\vee$ via $\alpha \mapsto \alpha^\vee$, so if $\theta = \sum m_i\alpha_i$, then $\theta^\vee = \sum m_i\alpha_i^\vee$, so $h^\vee_R = h_R = \sum m_i + 1$. ⌟

Prop. (3.9.3.14) [Listing of Coxeter Numbers]. We can determine the Coxeter numbers and dual coxeter numbers of indecomposable root systems:

- $h_{A_n} = h^\vee_{A_n} = n + 1$.
- $h_{B_n} = 2n$, and $\theta^\vee = e_1 + e_2 = \alpha_1^\vee + 2\alpha_2^\vee + \ldots + \alpha_n^\vee$, so $h^\vee_{B_n} = 2n - 1$.
- $h_{C_n} = 2n$, and $\theta^\vee = e_1 = \alpha_1^\vee + \ldots + \alpha_n^\vee$, so $h^\vee_{C_n} = n + 1$.
- $h_{D_n} = h^\vee_{D_n} = 2n - 2$.
- $h_{G_2} = 6$, and $\theta^\vee = \frac{2}{3}(2\omega + 3) = \alpha_1^\vee + 2\alpha_2^\vee$, so $h^\vee_{G_2} = 4$.
- $h_{F_4} = 12$, and $\theta^\vee = e_1 + e_2 = 2\alpha_1^\vee + 3\alpha_2^\vee + 2\alpha_3^\vee + \alpha_4^\vee$, so $h^\vee_{F_4} = 9$.
- $h_{E_8} = h^\vee_{E_8} = 30$.
- $h_{E_7} = h^\vee_{E_7} = 18$.
- $h_{E_6} = h^\vee_{E_6} = 12$.

⌟

Minuscule Weights

Def. (3.9.3.15)[Minuscule Weights]. Let (R, S) be a root system, then a dominant weight ω is called **minuscule** if $(\omega, \beta^\vee) \leq 1$ for any positive coroot $\beta^\vee$. ⌟

Prop. (3.9.3.16) [Minuscule and Fundamental Weights]. Let $\theta^\vee = \sum m_i \alpha_i^\vee$ the maximal coroot, where m_i are positive integers, and $m_i = (\omega_i, \theta^\vee)$. Then any minuscule weight is fundamental, and a fundamental weight ω_i is minuscule iff $m_i = 1$. ⌟

Proof: The definition of minuscule weight requires $m_i \leq 1$, and any other coroot is of the form $\beta^\vee = \sum n_i \alpha_i^\vee$, where $n_i \leq m_i$, so $n_i = (\omega_i, \beta^\vee) \leq 1$. □

Lemma (3.9.3.17). If $\omega \in Q$ and $|(\omega, \beta^\vee)| \leq 1$ for any coroot β, then $\omega = 0$. ⌟

Proof: If not, choose a counterexample $\omega = \sum m_i \alpha_i$ with $\sum |m_i| > 0$ minimum, then $(\omega, \omega) = \sum m_i (\omega, \alpha_i^\vee) > 0$, so changing ω to $-\omega$ if necessary, we can assume $m_i > 0, (\omega, \alpha_i^\vee) > 0$ for some i, so $(\omega, \alpha_i^\vee) = 1$, and $s_i \omega = \omega - \alpha_i$ is another counterexample with smaller $|m_i|$, contradiction. □

Prop. (3.9.3.18). The following are equivalent for a dominant integral weight ω of a root system:

- ω is minuscule(3.9.3.15).
- If λ is a dominant integral weight and $\omega - \lambda \in Q^+$, then $\lambda = \omega$.

⌟

Proof: Cf.[Etingof, P141]**?**. □

Prop. (3.9.3.19) [Number of Minuscule Roots]. Every coset in P/Q contains a unique minuscule weight. This gives a bijection between the P/Q and the set of minuscule weights. In particular, the number of minuscule weights equals the determinant of the Cartan matrix. ⌟

Proof: For any $a \in P$, let $C = a + Q$ be a coset, let $\omega \in C \cap P^+$ be an element with minimum (ω, ρ), then for any dominant weight $\lambda < \omega \in C$, $(\omega - \lambda, \rho) \geq 0$, so $\lambda = \omega$. Thus ω is minuscule(3.9.3.18).

Conversely, if $\omega_1 \neq \omega_2 \in C$ are minuscule, then by(3.9.3.17), there is a positive coroot $\beta^\vee$ that $|(\omega_1 - \omega_2, \beta)| > 2$. But then as ω_1, ω_2 are both dominant, $|(\omega_1 - \omega_2, \beta)| \leq 1$, contradiction. □

Cor. (3.9.3.20) [Listing of Minuscule Weights]. By(3.9.3.19) and(3.9.3.2)(3.9.3.10), we can determine minuscule weights for indecomposable root system (R, S),

- A_n: $P/Q \cong \mathbb{Z}/(n+1)\mathbb{Z}$, so it has $n+1$ minuscule weight, which are all the fundamental weights ω_i and 0.
- B_n: $P/Q \cong \mathbb{Z}/2\mathbb{Z}$, so there is exactly one non-zero minuscule weight, which is $\omega_n = (\frac{1}{2}, \ldots, \frac{1}{2})$, by(3.9.3.18).
- C_n: $P/Q \cong \mathbb{Z}/2\mathbb{Z}$, so there is exactly one non-zero minuscule weight, which is $\omega_n = (1, 0, \ldots, 0)$, by(3.9.3.18). The corresponding fundamental representation is the standard representation of $\mathfrak{sp}_{2n}$.
- D_n: $|P/Q| = 4$, so there are exactly 3 non-zero minuscule weights, which are ω_1, ω_{n-1} and ω_n, with corresponding fundamental representations of dimension $2n, 2^{n-1}, 2^{n-1}$. This is because the maximal coroot $\beta^\vee = \alpha_1^\vee + 2\alpha_2^\vee + \ldots + 2\alpha_{n-2}^\vee + \alpha_{n-1}^\vee + \alpha_n^\vee$.
- G_2: $|P/Q| = 1$, so there are no non-zero minuscule weights.
- F_4: There are no non-zero minuscule weights.

- E_8: There are no non-zero minuscule weights.
- E_7: $P/Q \cong \mathbb{Z}/2\mathbb{Z}$, so there is exactly one non-zero minuscule weight.
- E_6: $P/Q \cong \mathbb{Z}/3\mathbb{Z}$, so there are exactly two non-zero minuscule weights.

⌟

Prop. (3.9.3.21) [w_0]. Notice $-w_0$ is an automorphism of (R, S) that permutes fundamental weights and simple roots, so it induces an automorphism of the Dynkin diagram of R. So if the Dynkin diagram of $\mathfrak{g}$ has no non-trivial automorphism, $w_0 = -1$. This is case for $R = A_1, B_n, C_n, G_2, F_4, E_7$ and E_8.

For D_n, if n is even, then $-1 \in W$ so $w_0 = -1$. If n is odd, then $w_0(e_i) = -e_i$ for $i < n$ and $w_0(e_n) = e_n$.

Notice also each s_i acts trivially on P/Q, so $-w_0$ acts by -1 on P/Q. For $A_n, n \geq 2$, $P/Q \cong \mathbb{Z}/(n+1)\mathbb{Z}$, thus $-w_0$ is the flip of the chain. Likewise for E_6, $P/Q \cong \mathbb{Z}/3\mathbb{Z}$, thus $-w_0$ flips the two minuscule weights. But for D_n, $P/Q \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for n even and $P/Q \cong \mathbb{Z}/4\mathbb{Z}$ for n odd, so $-w_0$ preserves the minuscule weights or flip w_{n-1} and w_n. ⌟

4 Notations for a Root System

Def. (3.9.4.1) [Notations for a Root System]. Let (R, S) be a root system, then

- R^+/R^- is the positive/negative roots w.r.t. S.
- $S = \{\alpha_1, \ldots, \alpha_r\}$.
- s_i is the reflection w.r.t. α_i.
- θ is the maximal root.
- $\theta^\vee$ is the maximal coroot(maximal root of the dual root system).(It may not be dual to θ)
- $\rho = \frac{1}{2}\sum_i \alpha_i = \sum \omega_i$.
- $\rho^\vee$ is ρ of the dual system $R^\vee$.
- The height of weights is defined as in(3.9.2.17).
- W is the Weyl group.
- $w_0 \in W$ is the unique element with length $|R^+|$(3.9.2.14).
- n_{ij} is the Cartan number $n(\alpha_i, \alpha_j)$.
- $Q(R)$ is the root lattice(3.9.3.8).
- $P(R)$ is the weight lattice, generated by the fundamental weights ω_i(3.9.3.8).
- $P^+(R)$ is the dominant integral weights.
- $\mathfrak{P}$ is the Kostant partition function on $Q(R)$.

⌟

3.10 Algebraic K-Theory

Main references are [Algebraic K-Theory of Fields, Suslin, in Proc. ICM 1986, P222-244], [Algebraic K-Theory, Olivier Isely] and [G-S17], [nLab]. [Totaro, Milnor K-theory is the Simplest Part of Algebraic K-Theory, K-theory 6, 177-189, 1992].

1 Milnor K-Groups of Fields

Def. (3.10.1.1) [K_0]. The Grothendieck group $K_0(A)$ for a ring A is the free group generated by f.g. projective module over A modulo exact sequences. Then we have $P \sim Q$ iff $P \oplus A^n \cong Q \oplus A^n$ for some n. This is a functor $\mathcal{CA}\mathrm{lg} \to \mathcal{A}\mathrm{b}$. ⌟

Def. (3.10.1.2) [Milnor K-Groups]. For $k \in \texttt{Field}$, define the n-th **Milnor K-group** to be the groups

$$K_0^{\mathrm{Mil}}(k) = \mathbb{Z}, \quad K_1^{\mathrm{Mil}}(k) = k^\times, \quad K_n^{\mathrm{Mil}}(k) = (k^\times)^{\otimes n}/\{a_1 \otimes \ldots \otimes a_n | \exists 1 \le i < j \le n, a_i + a_j = 1\}, n \ge 2.$$

The elements in $K_n^{\mathrm{Mil}}(k)$ are called **symbols**, and the class of $a_1 \otimes \ldots \otimes a_m$ is denoted by $\{a_1, \ldots, a_n\}$. ⌟

Prop. (3.10.1.3) [Total Milnor K-Groups]. For $m, n \in \mathbb{N}$, the tensor product $(k^\times)^{\otimes m} \times (k^\times)^{\otimes n} \to (k^\times)^{\otimes(m+n)}$ induces a surjective map

$$K_m^{\mathrm{Mil}}(k) \otimes K_m^{\mathrm{Mil}}(k) \to K_{m+n}^{\mathrm{Mil}}(k),$$

which induces a graded group structure on

$$K_*^{\mathrm{Mil}}(k) = \bigoplus_{n \in \mathbb{N}} K_n^{\mathrm{Mil}}(k).$$

Then $K_*^{\mathrm{Mil}}(k)$ is graded commutative. ⌟

Proof: Firstly we show that $\{x, -x\} = 0$:

$$\{x, -x\} + \{x, -(1-x)x^{-1}\} = \{x, 1-x\} = 0,$$

so

$$\{x, -x\} = -\{x, 1 - x^{-1}\} = \{x^{-1}, 1 - x^{-1}\} = 0.$$

Thus for any $x, y \in k^\times$,

$$0 = \{xy, -xy\} = \{x, y\} + \{x, -x\} + \{y, -y\} + \{y, x\}.$$

The general cases follow by induction. □

Prop. (3.10.1.4) [Finite Fields]. If $k \in \texttt{Field}^{\mathrm{fin}}$, then for any $n \ge 2$, $K_n^{\mathrm{Mil}}(k) = 0$. ⌟

Proof: By(3.10.1.3), it suffices to show that $K_2^{\mathrm{Mil}}(k) = 0$. And if ω is a generator of the cyclic group $k^\times$, then it suffices to show that $\{\omega, \omega\} = \{\omega, -1\} = 0$. If $\#k = 2^m$, then

$$0 = \{1, \omega\} = \{\omega^{2^m - 1}, \omega\} = (2^m - 1)\{\omega, \omega\},$$

thus we are done. And if $\mathrm{char}\, k \ne 2$, then we can find two non-squares in $k^\times$ s.t. $a + b = 1$. Then

$$0 = \{a, b\} = \{\omega^l, \omega^k\} = kl\{\omega, \omega\},$$

so $\{\omega, \omega\} = 0$. □

Tame Symbols and Specialization Maps

Def. (3.10.1.5) [Tame symbols and Specialization Maps]. Let (R, K, κ) be a DVR, then for any $n \in \mathbb{Z}_+$, there exists a unique homomorphism

$$\partial^{\mathrm{Mil}} : K_n^{\mathrm{Mil}}(K) \to K_{n-1}^{\mathrm{Mil}}(\kappa)$$

called the **tame symbol map**, s.t. for any uniformizer ϖ and units $u_1, \ldots, u_{n-1} \in R^*$,

$$\partial^{\mathrm{Mil}}(\{\varpi, u_1, \ldots, u_{n-1}\}) = \{\overline{u}_1, \ldots, \overline{u}_{n-1}\}.$$

Moreover, for any uniformizer ϖ and $n \in \mathbb{Z}_+$, there exists a **specialization map**

$$s_{\varpi}^{\mathrm{Mil}} : K_n^{\mathrm{Mil}}(K) \to K_n^{\mathrm{Mil}}(\kappa)$$

s.t.

$$s_{\varpi}^{\mathrm{Mil}}(\{\varpi^{i_1} u_1, \ldots, \varpi^{i_n} u_n\}) = \{\overline{u}_1, \ldots, \overline{u}_n\}$$

for any $u_1, \ldots, u_n \in R^*$. ⌟

Proof: Cf.[Central Simple Algebras]P217.? □

Cor. (3.10.1.6). $\partial^{\mathrm{Mil}}(\{a, b\}) = (-1)^{v(a)v(b)}\overline{a^{-v(b)} b^{v(a)}}$. ⌟

Proof: □

Thm. (3.10.1.7) [Berrick-Keating]. Let $R, S \in \mathfrak{Ring}$ and $U \in \mathfrak{Mod}_{R\text{-}S}$, let $T = \begin{bmatrix} R & U \\ & S \end{bmatrix} \in \mathfrak{Ring}$, then the map

$$\pi_i : K_i(T) \to K_i(T) \oplus K_i(S)$$

is an isomorphism for any $i \in \mathbb{Z}$. ⌟

Proof: [The K-Theory of Triangular Matrix Rings, Berrick-Keating, in Applications of algebraic K-theory to algebraic geometry and number theory, 1986]. □

2 Bloch-Kato Conjecture

Lemma (3.10.2.1) [Hilbert's Theorem90 for K_2]. Let K/k be a cyclic Galois field extension with a generator $\sigma \in \mathrm{Gal}(K/k)$, then the complex

$$K_2^{\mathrm{Mil}}(K) \xrightarrow{\sigma - 1} K_2^{\mathrm{Mil}}(K) \xrightarrow{\mathrm{Nm}_{K/k}} K_2^{\mathrm{Mil}}(k)$$

is exact. ⌟

Proof: Cf.[Central Simple Algebras]P276.? □

Prop. (3.10.2.2) [Galois Symbols]. Let $k \in \texttt{Field}, m \in \mathbb{Z} \cap k^\times, n \in \mathbb{Z}_+$, the boundary map

$$\partial k^\times \to H^1(k, \mu_m)$$

induces a map

$$\partial^n : (k^\times)^{\otimes n} \to (H^1(k, \mu_m))^{\otimes n} \xrightarrow{\cup} H^n(k, \mu_m^{\otimes n}),$$

and this map factors through $K_n^{\mathrm{Mil}}(k)$ and gives a **Galois symbol map**

$$h_{k,m}^n : K_n^{\mathrm{Mil}}(k) \to H^n(k, \mu_m^{\otimes n}).$$

⌟

Proof: To show this map factors through $K_n^{\mathrm{Mil}}(k)$, it suffices to show for $n=2$ and $\partial^2(a\otimes(1-a))=0$. Take an irreducible factorization

$$x^m - a = \prod_l f_l \in k[x],$$

and let α_l be a root of f_l in k_{sep}, $K_l = k(\alpha_l)$, then

$$(1-a) = \prod_l \mathrm{Nm}_{K_l/k}(1-\alpha_l).$$

and

$$\partial^2(a\otimes(1-a)) = \sum_l \partial^2(a\otimes \mathrm{Nm}_{K_l/k}(1-\alpha_l)).$$

But

$$\begin{aligned}\partial^2(a\otimes \mathrm{Nm}_{K_l/k}(1-\alpha_l)) &= \partial(a)\cup\partial(\mathrm{Nm}_{K_l/k}(1-\alpha_l)) = \partial(a)\cup \mathrm{cor}_k^{K_l}(1-\alpha_l)\\ &= \mathrm{cor}(\mathrm{res}_k^{K_l}(\partial(a))\cup(1-\alpha_l)) = \mathrm{cor}(\partial_{K_l}(a)\cup(1-\alpha_l))\end{aligned}$$

But by definition $a\in(K_l^\times)^m$, so $\partial_{K_l}(a)=0$, by(8.7.3.9). Thus $\partial^2(a\otimes(1-a))=0$. □

Thm. (3.10.2.3) [Bloch-Kato Conjecture, Voevodsky-Rost/Merkurjev–Suslin]. Situation as in(3.10.2.2), the Galois symbol(3.10.2.2) induces an isomorphism

$$K_n^{\mathrm{Mil}}(k)/mK_n^{\mathrm{Mil}}(k) \xrightarrow{h_{k,m}^n,\cong} H^n(k,\mu_m^{\otimes n}).$$

⌟

Proof: The $n=1$ case follows from(8.7.3.9).

For the $n=2$ case**?** □

3.11 Hopf Algebras

Main references are [Dri86], [A Brief Introduction To Quantum Groups, Etingof-Semenyakin]. [A Guide to Quantum Groups].

1 Poisson Algebras

Def. (3.11.1.1) [Poisson Algebras]. For $R \in \mathcal{CR}\text{ing}$, a **Poisson algebra** is a triple $(A, \cdot, \{-,-\})$ where $\cdot, \{-,-\} : A \times A \to A$ are R-bilinear operators, s.t.

- $(A, \cdot) \in \mathcal{A}\text{lg}_k$.
- $(A, \{-,-\}) \in \texttt{LieAlg}_k$.
- For any $x, y, z \in A$, $\{x, yz\} = \{x, y\}z + y\{x, z\}$.

⌟

Cor. (3.11.1.2). For any $R \in \mathcal{CR}\text{ing}$ and a Poisson algebra A over R, if $a \in A$, then $\{a, 1\} = 0$. ⌟

Prop. (3.11.1.3) [Commutator]. For any $R \in \mathcal{CR}\text{ing}$ and $A \in \mathcal{A}\text{lg}_R$, the commutator $[x, y] = xy - yx$ defines a Poisson algebra structure on A. ⌟

Prop. (3.11.1.4) [Tensor Products of Commutative Poisson Algebras]. Let A, B be two commutative Poisson k-algebras, then there is a canonical Poisson structure on $A \otimes_k B$:

$$\{a \otimes a', b \otimes b'\} = \{a, a'\} \otimes bb' + aa' \otimes \{b, b'\}.$$

⌟

Prop. (3.11.1.5). If $R \in \mathcal{CR}\text{ing}$ and A is a Poisson algebra over R, then for any $a, b, c, d, e \in A$,

$$\{a, b\}e[c, d] = [a, b]e\{c, d\}.$$

⌟

Proof: We first show that $\{a, b\}[c, d] = [a, b]\{c, d\}$ using the two ways of calculating $[ac, bd]$, and then we expand the expression

$$\{a, b\}[ec, d] = [a, b]\{ec, d\}$$

to get $\{a, b\}e[c, d] = [a, b]e\{c, d\}$. □

2 Coalgebras and Bialgebras

Def. (3.11.2.1) [Coalgebras]. For $R \in \mathcal{CR}\text{ing}$, a **coalgebra** is a co-monoid object in the category $\mathcal{M}\text{od}_R$.

Usually for a coalgebra, its comultiplication is denoted by Δ, and counit denoted by ε. ⌟

Remark (3.11.2.2) [Yoneda Interpretation]. A coalgebra (C, Δ, ε) needs to satisfy the following relations:

$$\Delta^{(2)} \triangleq (\mathrm{id} \otimes \Delta) \circ \Delta = (\Delta \otimes \mathrm{id}) \circ \Delta,$$

$$\mathrm{mul.} \circ (\mathrm{id} \otimes \varepsilon) \circ \Delta = \mathrm{mul.} \circ (\varepsilon \otimes \mathrm{id}) \circ \Delta = \mathrm{id}\,.$$

We do not need to verify all the relations defining a coalgebra C, whenever we have a functorial monoidal structure on all the set $\mathrm{Hom}_R(H, T)$, we immediately recover the maps

- (Comultiplication):$\Delta : C \to C \otimes_R C$(or denoted by μ) as $i_1 \cdot i_2$ in $\mathrm{Hom}_R(C, C \otimes C)$,
- (Counit):$\varepsilon : C \to R$ as 1 in $\mathrm{Hom}_R(C, R) = C^\vee$.

by Yoneda lemma.

$C^\vee$ is an monoid by definition, and C is called **cocommutative** iff $C^\vee$ is commutative. ⌟

Prop. (3.11.2.3) [Tensor Products of Co-Algebras]. Let $R \in \mathcal{CR}\mathrm{ing}$ and C, D be co-algebras over R, then $C \otimes D$ is a co-algebras with

$$\Delta_{C\otimes D} = \sigma_{23} \circ (\Delta_C \otimes \Delta_D), \quad \varepsilon_{C\otimes D} = \varepsilon_C \otimes \varepsilon_D.$$

⌟

Def. (3.11.2.4) [Primitive Elements]. Let $R \in \mathcal{CR}\mathrm{ing}$ and H be a coalgebra over R, then an element $x \in H$ is called a **primitive element** if $\mu(x) = 1 \otimes x + x \otimes 1$. It is called **group-like element** if $\Delta(x) = x \otimes x$. ⌟

Def. (3.11.2.5) [Sweedler Notations]. For a coalgebra A and $a \in A$, if $\Delta(a) = \sum_i a_{1i} \otimes a_{2i}$, then we can write

$$\Delta(a) = \sum_{\mathrm{Swe}} a_1 \otimes a_2.$$

And similarly, by the first defining relation of(3.11.2.2), we can also write

$$(\mathrm{id} \otimes \Delta) \circ \Delta(a) = (\Delta \otimes \mathrm{id}) \circ \Delta(a) = \sum_{\mathrm{Swe}} a_1 \otimes a_2 \otimes a_3.$$

Then the second defining relation just writes

$$a = \sum_{\mathrm{Swe}} a_1 \varepsilon(a_2) = \sum_{\mathrm{Swe}} \varepsilon(a_1) a_2.$$

⌟

Prop. (3.11.2.6). For any coalgebra (A, Δ, ε) and $h \in A$, by defining relations,

$$h = \sum_{\mathrm{Swe}} \varepsilon(h_1) h_2, \quad \varepsilon(h) = \sum_{\mathrm{Swe}} \varepsilon(h_1)\varepsilon(h_2).$$

⌟

Def. (3.11.2.7) [Co-Derivations]. For a co-algebra (C, Δ, ε), a **co-derivation** is a map $d : C \to C$ s.t. for any $c \in C$,

$$\Delta(d(c)) = d(c_1) \otimes c_2 + c_1 \otimes d(c_2).$$

⌟

Co-Poisson Co-Algebras

Def. (3.11.2.8) [Lie Co-Algebras]. For $k \in \texttt{Field}$, **Lie co-algebra** over k is a module $C \in \mathcal{V}\mathrm{ect}_k$ together with a k-linear map $q : C \to C \otimes C$ s.t.

$$(1 + t_2) \circ q = 0$$

$$(1 + t_3 + t_3^2) \circ (q \otimes \mathrm{id}) \circ q = 0.$$

where $t_3 : C^3 \to C^3$ is given by $t_3(v_1 \otimes v_2 \otimes v_3) = v_3 \otimes v_1 \otimes v_2$. ⌟

Def. (3.11.2.9) [Sweedler Notations]. For $k \in \texttt{Field}$ and a Lie co-algebra C over k and $a \in C$, if $q(a) = \sum_i a_{1i} \otimes a_{2i}$, we can write

$$q(a) = \sum_{\text{Swe}} a_{(1)} \otimes a_{(2)}.$$

And similarly, we can also write

$$(q \otimes \mathrm{id}) \circ q(a) = \sum_{\text{Swe}} a_{(1)} \otimes a_{(2)} \otimes a_{(3)}.$$

Then the defining relation of Lie co-algebras writes

$$\sum_{\text{Swe}} a_{(1)} \otimes a_{(2)} = -\sum_{\text{Swe}} a_{(2)} \otimes a_{(1)},$$

$$\sum_{\text{Swe}} a_{(1)} \otimes a_{(2)} \otimes a_{(3)} + \sum_{\text{Swe}} a_{(3)} \otimes a_{(1)} \otimes a_{(2)} + \sum_{\text{Swe}} a_{(2)} \otimes a_{(3)} \otimes a_{(1)} = 0.$$

⌟

Def. (3.11.2.10) [Co-Poisson Co-Algebras]. For $k \in \mathcal{CR}\text{ing}$, a **co-Poisson co-algebra** is a co-algebra (C, Δ, ε) over R together with a R-linear map $q : C \to C \otimes C$ s.t.

- (C, q) is a Lie co-algebra(3.11.2.8).
- (Co-Leibniz rule)
$$(\Delta \otimes \mathrm{id}) \circ q = (\mathrm{id} \otimes q) \circ \Delta + \sigma_{23}(q \otimes \mathrm{id}) \circ \Delta.$$

Equivalently,

$$\sum_{\text{Swe}} c_{(1)1} \otimes c_{(1)2} \otimes c_{(2)} = \sum_{\text{Swe}} c_1 \otimes c_{2(1)} \otimes c_{2(2)} + \sum_{\text{Swe}} c_{1(1)} \otimes c_2 \otimes c_{1(2)}.$$

⌟

Cor. (3.11.2.11). For any co-Poisson co-algebra $(C, \Delta, \varepsilon, q)$,

$$(\mathrm{id} \otimes \Delta) \circ q = (q \otimes \mathrm{id}) \circ \Delta + \sigma_{12}(\mathrm{id} \otimes q) \circ \Delta.$$

⌟

Prop. (3.11.2.12) [Poisson Algebras and Co-Poisson Co-algebras]. Let $R \in \mathcal{CR}\text{ing}$ and (C, Δ, ε) be a co-algebra over R with an R-linear map $q : C \to C \otimes C$, then (C, q) is a co-Poisson structure iff (C^*, q^*) is a Poisson algebra.

And if $\sigma : C \to D$ is a linear map between co-Poisson co-algebras over R, then σ is a homomorphism of co-Poisson co-algebras iff $\sigma^* : D^* \to C^*$ is a homomorphism of Poisson algebras. ⌟

Prop. (3.11.2.13) [Co-Commutator]. For any $k \in \texttt{Field}$ and a co-algebra (C, Δ, ε) over k, the co-commutator $\Delta' = \Delta - \sigma_{12} \circ \Delta$ defines a co-Poisson co-algebra structure on C. ⌟

Prop. (3.11.2.14) [Tensor Products of Co-Commutative Co-Poisson Co-Algebras]. Let $R \in \mathcal{CR}\text{ing}$ and C, D be co-commutative co-Poisson co-algebras over R, then $C \otimes D$ is also a co-commutative co-Poisson co-algebras with the co-algebra structure given by(3.11.2.3) and

$$q_{C \otimes D} = \sigma_{23} \circ (q_C \otimes \Delta_D + \Delta_C \otimes q_D),$$

i.e..

$$q_{C \otimes D}(a \otimes b) = (a_{(1)} \otimes b_1) \otimes (a_{(2)} \otimes b_2) + (a_1 \otimes b_{(1)}) \otimes (a_2 \otimes b_{(2)}).$$

⌟

Proof: ? □

Prop. (3.11.2.15). There are no co-Poisson algebra structures on a group co-algebra $k[\Gamma]$.? ⌟

Proof: □

Prop. (3.11.2.16). If C is a co-commutative co-algebra and d_1, d_2 are two co-derivatives of C s.t. $d_1 d_2 = d_2 d_1$, then the the map

$$q : C \to C \otimes C : q(c) = d_1(c_1) \otimes d_2(c_2) - d_2(c_1) \otimes d_1(c_2)$$

defines a co-Poisson co-algebra on C. ⌟

Prop. (3.11.2.17). For any co-commutative co-algebra $(C, \Delta, \varepsilon, q)$,

$$(q \otimes \Delta') \circ \Delta = (\Delta' \otimes q) \circ \Delta.$$

And also

$$(\Delta' \otimes \mathrm{id} \otimes q) \circ \Delta^{(2)} = (q \otimes \mathrm{id} \otimes \Delta') \circ \Delta^{(2)}.$$

⌟

Proof: These follow from(3.11.2.12) and(3.11.1.5). □

Prop. (3.11.2.18). For any co-Poisson co-algebra $(C, \Delta, \varepsilon, q)$ and $f \in C^*$, $(f \otimes \mathrm{id}) \circ q : C \to C$ and $(\mathrm{id} \otimes f) \circ q : C \to C$ are co-derivatives of C. ⌟

Proof:

□

Prop. (3.11.2.19). For any co-Poisson co-algebra $(C, \Delta, \varepsilon, q)$, $(\varepsilon \otimes \mathrm{id}) \circ q = (\mathrm{id} \otimes \varepsilon) \circ q = 0$, i.e.

$$\sum_{\mathrm{Swe}} \varepsilon(c_{(1)}) c_{(2)} = \sum_{\mathrm{Swe}} c_{(1)} \varepsilon(c_{(2)}) = 0.$$

⌟

Proof:

□

Bialgberas

Def. (3.11.2.20) [Bialgebras]. For $R \in \mathcal{CR}\mathrm{ing}$, a **bialgbera** A is an unital R-algebra A with algebra homomorphisms $\Delta, \varepsilon : A \to A \times A$ s.t. (A, Δ, ε) is a co-algebra over R. Equivalently, Δ and ε need to satisfy properties as listed in https://en.wikipedia.org/wiki/Bialgebra.

WARNING: A cannot be defined as the co-unital-monoid algebra in $\mathcal{R}\mathrm{ing}/R$, because tensor products are not coproducts for non-commutative rings, Cf.https://math.stackexchange.com/questions/984151/proof-that-the-tensor-product-is-the-coproduct-in-the-category-of-r-algebras.
⌟

Cor. (3.11.2.21). For any bialgebra $(A, \cdot, \Delta, \varepsilon)$, $\Delta(1) = 1$. ⌟

Co-modules

Def. (3.11.2.22) [Co-modules]. Ket A be a coalgebra over a field k, then a right **co-module** is a k-vector space V together with a k-linear map $\rho : V \to V \otimes A$ that satisfies

$$(\mathrm{id}_V \otimes \mu) \circ \rho = (\rho \otimes \mathrm{id}_A) \circ \rho, \quad (\mathrm{id}_V \otimes \varepsilon) \circ \rho = \mathrm{id}_V .$$

The map ρ is called the **co-action**, and a k-subspace $W \subset V$ that $\rho(W) \subset W \otimes A$ is called a **sub-comodule** of V. ⌟

Def. (3.11.2.23) [Tensor Product of Co-modules]. ⌟

3 Hopf Algebras

Def. (3.11.3.1) [Hopf Algebra]. For $R \in \mathcal{CR}\mathrm{ing}$, a **Hopf algebra** over a R is an R-bi-algebra $(A, \mathrm{mul.}, \eta, \Delta, \varepsilon)$ together with an R-linear isomorphism $S : A \to A$(the antipode) that satisfies:

$$\mathrm{mul.} \circ (\mathrm{id} \otimes S) \circ \Delta = \mathrm{mul.} \circ (S \otimes \mathrm{id}) \circ \Delta = \eta \circ \varepsilon : A \to A,$$

or equivalently,

$$\sum_{\mathrm{Swe}} a_1 S(a_2) = \sum_{\mathrm{Swe}} S(a_1) a_2 = \varepsilon(a), \quad a \in A.$$

If $S^2 = \mathrm{id}_A$, then A is called an **involutive Hopf algebra**.

Similarly we can define **topological Hopf algebras** or **graded Hopf algebras**. ⌟

Remark (3.11.3.2). The motivating example is $A = \mathcal{O}(G)$ where $G \in \mathcal{G}\mathrm{rp}$. ⌟

Prop. (3.11.3.3). For a Hopf algebra A, S is an anti-homomorphism both for the algebra structure and coalgebra structure.

And if A is commutative or co-commutative, then A is involutive. ⌟

Proof: Cf.https://ncatlab.org/nlab/show/Hopf+algebra, and [Abe (1980), Theorem2.1.4]. □

Prop. (3.11.3.4). For any $(A, \mathrm{mul.}, \eta, \Delta, \varepsilon, S) \in \mathcal{H}\mathrm{opf}$, S is determined by the bi-algebra structure of A. ⌟

Proof:

□

Example (3.11.3.5) [Group Algebras]. For $\Gamma \in \mathcal{G}\mathrm{rp}$, the group algebra $R[\Gamma]$ with the coalgebra structure

$$\Delta : R[\Gamma] \to R[\Gamma] \times R[\Gamma] : g \mapsto g \otimes g, \quad \varepsilon : R[\Gamma] \to R : \sum a_g g \mapsto \sum a_g$$

and the antipode

$$S : R[\Gamma] \to R[\Gamma] : g \mapsto g^{-1}$$

is a Hopf algebra. ⌟

Prop. (3.11.3.6) [Universal Enveloping Algebras]. ⌟

Def. (3.11.3.7)[Hopf Ideal and Quotient Hopf Algebra]. Let A be a Hopf algebra, then a quotient Hopf algebra is a quotient A/I that has a Hopf algebra structure compatible with that of A. In another words, there are commutative diagrams

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A\otimes_R A \\ \downarrow & & \downarrow \\ A/I & \xrightarrow{\overline{\Delta}} & A/I\otimes_R A/I \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{\varepsilon} & R \\ \downarrow & \nearrow & \\ A/I & & \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{S} & A \\ \downarrow & & \downarrow \\ A/I & \xrightarrow{\overline{S}} & A/I \end{array}$$

In particular, quotient Hopf algebras correspond to ideals of A s.t.

$$\Delta(I)\subset A\otimes I+I\otimes A,\quad \varepsilon(I)=0,\quad S(I)\subset I,$$

called **Hopf ideals** of A. ⌟

Remark (3.11.3.8) [Examples]. If $\Gamma'\lhd\Gamma\in\mathcal{G}\mathrm{rp}$, then $R[\Gamma]$ has a quotient Hopf algebra $R[\Gamma/\Gamma']$. In particular, $R[t]/(t^n-1)$ is a quotient Hopf algebra of $R[t,t^{-1}]$. ⌟

Def. (3.11.3.9) [Dual Hopf Algebras]. Let H be a Hopf algebra, matrix coefficients. H^0.**?** ⌟

Prop. (3.11.3.10). $\mathrm{Rep}(H)\cong\mathcal{M}\mathrm{od}_{H^0}$. ⌟

Topologists' Hopf Algebras

Def. (3.11.3.11) [Topologist's Hopf Algebra]. A **topologist's Hopf algebra** over a commutative ring R is a unital magma object in the dual category of graded R-algebras with 0-degree term R, given by maps $\Delta:A\to A\otimes A$, and $\varepsilon:A\to R$ the canonical projection map. So in particular, Δ is of the form

$$\Delta(\alpha)=1\otimes\alpha+\alpha\otimes 1+\sum_i\alpha_i'\otimes\alpha_i'',|\alpha_i'|>0,|\alpha_i''|>0$$

⌟

Prop. (3.11.3.12). The tensor product of two topologists' Hopf algebra is a topologists' Hopf algebra. ⌟

Prop. (3.11.3.13). Let $\mathbb{F}$ be a field, then $\mathbb{F}[\alpha]/(\alpha^n)$, where α is placed at even dimension or $\mathbb{F}$ has characteristic 2, is a topologists' Hopf algebra iff $\mathbb{F}$ has positive characteristic p and n is a power of p. ⌟

Proof: By definition, it is easy to see that α is primitive, thus

$$\Delta(\alpha^n)=0=\sum_{0<i<n}\binom{n}{i}\alpha^i.$$

Which then implies that n is a p-power. □

Prop. (3.11.3.14) [Hopf-Borel]. Let A be a topologists' Hopf algebra over a perfect field K, and A is of f.d. in each degree, then:

- If K has characteristic 0, A is isomorphic as an algebra to the tensor product of an exterior product of odd-dimensional generators and a polynomial ring of even-dimensional generators.

- If K has characteristic p, then A is isomorphic as an algebra to the tensor product of algebras of the following types:
  - $K[\alpha]$, where α is even-dimensional if $p \neq 2$.
  - $\wedge_K[\alpha]$ where α is odd-dimensional.
  - $K[\alpha]/(\alpha^{p^i})$, where α is even-dimensional if $p \neq 2$.

⌟

Proof: We only prove the 0-characteristic case, Cf.[Hat02]P285.**?** □

4 Commutative Hopf Algebras

Prop. (3.11.4.1) [Commutative Hopf Algebra]. For $R \in \mathcal{CR}\mathrm{ing}$, a commutative Hopf algebra over R is equivalent to a cogroup object in $\mathcal{CA}\mathrm{lg}_R$. A homomorphism of Hopf algebras is a morphism of algebras that represents a natural transformation of functors from $\mathcal{CA}\mathrm{lg}_R$ to $\mathcal{G}\mathrm{rp}$. ⌟

Proof: The critical point is to look at the definition of Hopf algebra. In this case, S is a homomorphism of algebras(3.11.3.3), and notice tensor product is just the product in the dual category, and $m : A \otimes A \to A$ is the diagonal in the dual category, thus a cogroup object is a map $\Delta : A \to A \otimes A$ together with a map $\mathrm{inv} : A \to A$ that

$$m \circ (\mathrm{id} \otimes \mathrm{inv}) \circ \Delta = m \circ (\mathrm{inv} \otimes \mathrm{id}) \circ \Delta\, \mathrm{id} = \mathrm{id} : A \to A,$$

which is exactly the definition of the Hopf algebra(3.11.3.1). □

Cor. (3.11.4.2) [Yoneda Interpretation]. We do not need to verify all the relations defining a Hopf algebra H, whenever we have a functorial commutative group structure on all the set $\mathrm{Hom}_R(H, T)$, we immediately recover the maps:

- (Comultiplication):$\mu : H \to H \otimes_R H$ as $i_1 \cdot i_2$ in $\mathrm{Hom}_R(H, H \otimes H)$,
- (Antipode):$\iota : H \to H$ as inv in $\mathrm{Hom}_R(H, H)$,
- (Counit):$\varepsilon : H \to R$ as 1 in $\mathrm{Hom}_R(H, R) = H^\vee$.

by Yoneda lemma.

For convenience, we denote the structure maps $\eta_H : R \to H, \mu : H \times_R H \to H, (-)^{-1} : H \to H$. ⌟

Prop. (3.11.4.3) [Group Algebras]. Let Γ be a commutative group, then the group algebra $R[\Gamma]$(3.11.3.5) represents the group functor that maps a commutative R-algebra S to the commutative group $\mathrm{Hom}_{\mathcal{G}\mathrm{rp}}(\Gamma, S)$. ⌟

Cor. (3.11.4.4) [Multiplicative Groups]. $\mathbb{G}_{m,R} = R[t, t^{-1}]$ is a Hopf algebra that represents the group functor of multiplicative groups on $\mathcal{CA}\mathrm{lg}_R$. ⌟

Cor. (3.11.4.5) [Roots of Unity $\mu_{n,R}$]. Let $\Gamma \cong \mathbb{Z}/n\mathbb{Z}$, then $R[\Gamma] \cong R[t]/(t^n - 1)$ is a Hopf algebra that represents the group functor of multiplicative groups of n-th roots of unity on $\mathcal{CA}\mathrm{lg}_R$. ⌟

Prop. (3.11.4.6) [Additive Groups]. $R[t]$ can be given a Hopf algebra structure that represents the group functor that maps a commutative R-algebra S to the additive group S^+. ⌟

Def. (3.11.4.7) [$G_{(a,b),R}$]**.** Given elements $a, b \in R$ that $ab = 2$, for any commutative R-algebra S, the group $G_{(a,b),R}(S)$ of elements x of S that $x^2 + ax = 0$ is a group under the mapping $(m, n) \mapsto m + n + bmn$. Notice the inverse of m is m itself. Then $R[t]/(t^2 + at)$ can be given a Hopf algebra that represents the functor $S \mapsto G_{(a,b),R}(S)$. ⌟

Def. (3.11.4.8) [$V_{\mathfrak{a}}$]**.** Let V be a vector space over k, then $\mathrm{Sym}(V^\vee)$ can be given a Hopf algebra structure representation the functor $V_{\mathfrak{a}} : R \mapsto R \otimes_k V \cong \mathrm{Hom}_k(V^\vee, R)$. ⌟

Def. (3.11.4.9) [Locally Constant Functions]. Let Γ be a group, then $\underline{\Gamma}_R = \prod_{\gamma\in\Gamma} R$ represents the group functor that maps an R-algebra T to the group of locally constant functions on $\mathrm{Spec}\, R$ with value in Γ. ⌟

Remark (3.11.4.10). To illustrate the philosophy of(9.1.1.2), we figure out the Hopf structure of the local constant functions: a map $\prod_{\gamma\in\Gamma} R \to T$ is equivalent to a set of idempotents e_γ of T that $\sum e_\gamma = 1$. This is equivalent to a locally constant function on $\mathrm{Spec}\, T$ that takes value γ on $V(e_\gamma)$. Then the product takes values $\gamma\delta$ on $V(e_\gamma \otimes e_\delta) \subset \mathrm{Spec}\, T \otimes T$, or equivalently takes values γ on $V(\sum_{gg'=\gamma} e_g \otimes e_{g'})$, so $\Delta(e_\gamma) = \sum_{gg'=\gamma} e_g \otimes e_{g'}$. ⌟

Lemma (3.11.4.11) [Modulo $\ker(\varepsilon)$**].** For a Hopf algebra A over R, the comultiplication and counit are determined by $\ker \varepsilon$:

- $R \oplus \ker \varepsilon \to A : (a, b) \mapsto a + b$ is an isomorphism of R-modules.
- $\mu(a) \equiv -\varepsilon(a) + a \otimes 1 + 1 \otimes a \mod \ker \varepsilon \otimes_R \ker \varepsilon$.
- $\iota(a) \equiv -a \mod (\ker \varepsilon)^2$ for $a \in \ker \varepsilon$.

⌟

Proof: 1: this is because the counit $0 \to \ker \varepsilon \to A \to R \to 0$ has an inverse by the R-algebra map $R \to S$.

2: item1 allows us to write

$$A \otimes_R A = R \oplus (\ker \varepsilon \otimes_R R) \oplus (R \otimes_R \ker \varepsilon) \oplus (\ker \varepsilon \otimes \ker \varepsilon)$$

so for $a \in A$,

$$\mu(a) = b + c \otimes 1 + 1 \otimes d + z$$

where $b \in R, c, d \in \ker \varepsilon, z \in \ker \varepsilon \otimes_R \ker \varepsilon$. Then $a = (\varepsilon \otimes \mathrm{id}_A)(b + c \otimes 1 + 1 \otimes d + z) = b + d$, and also $a = b + c$. Applying ε shows $b = \varepsilon(a)$, and thus

$$\mu(a) = \varepsilon(a) + (a - \varepsilon(a)) \otimes 1 + 1 \otimes (a - \varepsilon(a)) + z = -\varepsilon(a) + a \otimes 1 + 1 \otimes a + z.$$

3: Let $\iota(a) = b + c$ where $b \in R, c \in \ker \varepsilon$, then

$$\varepsilon(a) = \mathrm{mul}.(\iota \otimes \mathrm{id})(-\varepsilon(a) + a \otimes 1 + 1 \otimes a + z) = -\varepsilon(a) + \iota(a) + a + \mathrm{mul}.(\iota \otimes \mathrm{id})(z)$$

so for $a \in \ker \varepsilon$, $\iota(a) \equiv -a \mod (\ker \varepsilon)^2$, as $\mathrm{mul}.(\iota \otimes \mathrm{id})(z) \in (\ker \varepsilon)^2$, because ι commutes with ε. □

Prop. (3.11.4.12) [Hopf Ideals of Additive Groups]. Let $f = \sum_{i=0}^d a_i t^i \in R[t]$ be a monic polynomial$\neq t$, then (f) is a Hopf ideal of $R[t]$ iff R is of char $p > 0$ and the derivative $f' = 0$. ⌟

Proof: We check conditions in(3.11.3.7), the first says $\sum a_i(t \otimes 1 + 1 \otimes t)^i$ vanishes in $R[t]/(f) \otimes_R R[t]/(f)$. But f is monic, so this is equivalent to $a_i\binom{i}{j} = 0$ for any $0 < j < i \leq d$, But we have $gcd_{0<j<i}\{\binom{i}{j}\} = p$ if $i = p^r$ for some $r \geq 1$ and 1 otherwise, so $a_d = 0$ unless d is a power of p, and $p = 0 \in R$ because $a_d = 1$. In particular, $f = \sum_{i=0}^k b_i t^{p^i}$, and it automatically satisfies the other two conditions. □

Cor. (3.11.4.13) [$\alpha_{p^r,R}$]. Let R be a commutative ring of char $p>0$, then the quotient Hopf algebra $R[t]/(t^{p^r})$ corresponding to the Hopf ideal (t^{p^r}) is denoted by $\alpha_{p^r,R}$.

WARNING: $\alpha_{p^r,R}$ is isomorphic to $\mu_{p^r,R}$ as R-algebras, but they are not isomorphic as Hopf algebras. ⌟

Prop. (3.11.4.14) [Irreducibility of Hopf Algebras]. For $k\in\texttt{Field}$, the following Hopf algebra contains no proper Hopf ideals:

- $\mathbb{G}_{a,k}$ if char $k=0$.
- $\alpha_{p,k}$ if char $k=p>0$.

⌟

Proof: Any Hopf ideal fo $k[t]$is principal, thus this proposition follows from(3.11.4.12). □

Def. (3.11.4.15) [Cokernel Hopf Algebra]. Let $A\to B$ be a homomorphism of Hopf Algebras over R, then the **cokernel Hopf algebra** is the algebra $B\otimes_A R=B/B\otimes_A\ker(\varepsilon_A)$, which represents the functor of kernels of $\mathrm{Hom}_R(B,T)\to\mathrm{Hom}_R(A,T)$, thus is a Hopf algebra. ⌟

Lemma (3.11.4.16). A Hopf algebra over a field k is direct limit of Hopf algebra of f.t. over k. ⌟

Def. (3.11.4.17) [Group-Like Elements]. Let A be a Hopf algebra, then a **group-like element** $a\in A$ is an invertible element that satisfies $\mu(a)=a\otimes a\in A\otimes A$.

If a is a group-like element in a Hopf algebra A, then $a=(\varepsilon,\mathrm{id})\mu(a)=\varepsilon(a)a$, so $\varepsilon(a)=1$. ⌟

Prop. (3.11.4.18) [Group-Like Elements are Linearly Independent]. Let A be a Hopf algebra over a field k, then the set of group-like elements are linearly independent over k. ⌟

Proof: If $e=\sum a_ie_i$ that e,e_i are all group-like elements, then

$$\mu(e)=e\otimes e=\sum c_ic_je_i\otimes e_j=\sum c_i\mu(e_i)=\sum c_ie_i\otimes e_i$$

so $c_i^2=c_i$ and $c_ic_j=0$. Now also notice $1=\varepsilon(e)=\sum c_i\varepsilon(e_i)=\sum c_i$(3.11.4.17), contradiction. □

Cor. (3.11.4.19). The set of group-like elements in the Hopf algebra $k[\Gamma]$(3.11.4.3) are just the set $\Gamma\subset k[\Gamma]$. ⌟

Prop. (3.11.4.20) [Cartier Theorem]. For $k\in\texttt{Field}^0$, any Hopf algebra A over k is reduced. ⌟

Proof: We can base change to the algebraic closure $\overline{k}$ of k and assume k is alg.closed. Because reducedness is stalkwise and Hilbert's Nullstellensatz, it suffices to show A_s is reduced at each $s\in G(k)$. The translation by $g\in G(k)$ acts transitively on $G(k)$, so it suffices to show it vanishes at the kernel of the counit map $\ker(\varepsilon)$. Cf.[Jakob, Stix].

We may assume by taking direct limits that A is f.g. over k. Let $\mathfrak{m}$ be the kernel of the counit $\varepsilon:A\to k$, then $\mathfrak{m}/\mathfrak{m}^2$ is a f.g. k-vector space with a basis lifting to $x_1,\ldots,x_r\in\mathfrak{m}$.

We prove that $\mathrm{gr}_{\mathfrak{m}}(A)$ is a polynomial ring in x_i, Cf.[Shatz]. □

Prop. (3.11.4.21) [Faithfully Flatness]. If $A\subset B$ are f.g. Hopf algebras over a field k, then B is f.f. over A. ⌟

Proof: Cf.[Milne, P73]?. □

Cor. (3.11.4.22). If $A\subset B$ are Hopf algebras that B is an integral domain, and let K,L be their fraction field, then $B\cap L=A$. In particular, if $K=L$, then $A=B$. ⌟

Proof: Since $A\to B$ is f.f. by(3.11.4.21), $cB\cap A=cA$ for any $c\in A$ by(3.11.4.21). Thus if $a/c\in B$ for $a,c\in A$, then $a\in cB\cap A=cA$, so $a/c\in A$. □

5 Quantization

Cf.[Dri85], [Dri86].

Quantizing is somewhat like replacing commutative algebras by noncommutative ones. One way to try to construct non-classical examples of quantum groups is to look for deformations, in the category of Hopf algebras, of classical algebras of functions on a group.

(Co-)Poisson Hopf Algebras

Def. (3.11.5.1) [Poisson-Hopf Algebras]. A **Poisson Hopf algebra** is a Hopf algebra $(A, \mathrm{mul.}, \eta, \Delta, \varepsilon, S)$ with a Poisson structure $\{-,-\}$ s.t.

$$\Delta(\{a,b\}) = \sum_{\mathrm{Swe}}\{a_1,b_1\}\otimes a_2b_2 + \sum_{\mathrm{Swe}} a_1b_1\otimes\{a_2,b_2\}.$$

Notice if A is commutative, then this just means $\Delta : A \to A\otimes A$ is a homomorphism of Poisson structures, by(3.11.1.4).

(The motivating example is $A = \mathcal{O}(G)$ where G is a Poisson-Lie group.) ⌟

Cor. (3.11.5.2). For any Poisson Hopf algebra $(A, \mathrm{mul.}, \eta, \Delta, \varepsilon, S, \{-,-\})$ and $a, b\in A$,

$$\sum_{\mathrm{Swe}}\{a, S(b_1)\}b_2 = \sum_{\mathrm{Swe}} S(b_1)\{b_2, a\}.$$

⌟

Proof: It follows from the Leibniz rule that

$$\sum_{\mathrm{Swe}}\{a,S(b_1)\}b_2 + \sum_{\mathrm{Swe}} S(b_1)\{a,b_2\} = \sum_{\mathrm{Swe}}\{a, S(b_1)b_2\} \overset{(3.11.3.1)}{=} \{a,\varepsilon(b)\} \overset{(3.11.1.2)}{=} 0.$$

□

Prop. (3.11.5.3). If $k\in$ `Field`, $\mathrm{char}\, k \neq 2$, and $\mathfrak{g}\in$ $\mathtt{LieAlg}_k$ is non-Abelian, then there are no non-trivial Poisson Hopf algebra structures on $U(\mathfrak{g})$. ⌟

Proof: Cf.[Co-Poisson structures on polynomial Hopf algebras]P816. □

Prop. (3.11.5.4). For a Poisson Hopf algebra $(H, \mu, \eta, \Delta, \varepsilon, S, \{-,-\})$, the counit $\varepsilon : H \to R$ is a Poisson algebra homomorphism: $\varepsilon(\{a,b\}) = 0$ for any $a, b\in H$. And if H is commutative, then $S : H\to H$ is a Poisson algebra anti-homomorphism. ⌟

Proof: For ε, because of the defining relation for coalgebras, for any $a, b\in A$,

$$\varepsilon(\{a,b\}) = \varepsilon(\mathrm{mul.}\circ(\varepsilon\otimes \mathrm{id})\circ\Delta(\{a,b\})) = \sum_{\mathrm{Swe}}\varepsilon(\{a_1,b_1\})\varepsilon(a_2b_2) + \sum_{\mathrm{Swe}}\varepsilon(a_1b_1)\varepsilon(\{a_2,b_2\}),$$

but also by(3.11.2.6),

$$\varepsilon(\{a,b\}) = \varepsilon(\{\sum_{\mathrm{Swe}}\varepsilon(a_1)a_2, \sum_{\mathrm{Swe}}\varepsilon(b_1)b_2\}) = \sum_{\mathrm{Swe}}\varepsilon(a_1b_1)\{a_2,b_2\}.$$

similarly,

$$\varepsilon(\{a,b\}) = \sum_{\mathrm{Swe}}\{a_1,b_1\}\varepsilon(a_2b_2).$$

Thus $\varepsilon(\{a,b\}) = 2\varepsilon(\{a,b\})$, so $\varepsilon(\{a,b\}) = 0$.

For S, Firstly for any $a,b \in A$,

$$\{a_1,b_1\}S(a_2b_2) + a_1b_1S(\{a_2,b_2\}) = 0,$$

by(3.11.5.1) and the fact $\varepsilon(\{a,b\}) = 0$. Then by(3.11.5.2)(3.11.3.1) and(3.11.3.3),

$$\begin{aligned}
\{S(b),S(a)\} &= \sum_{\text{Swe}}\{S(b_1),S(a)\}b_2S(b_3) \\
(3.11.5.2) &= -\sum_{\text{Swe}} S(b_1)\{b_2,S(a)\}S(b_3) \\
&= -\sum_{\text{Swe}} S(b_1)\{b_2,S(a_1)\}a_2S(a_3)S(b_3) \\
(3.11.5.2) &= \sum_{\text{Swe}} S(b_1)S(a_1)\{b_2,a_2\}S(a_3)S(b_3) \\
&= -\sum_{\text{Swe}} S(b_1)S(a_1)b_2a_2S(\{b_3,a_3\}) \\
(3.11.2.5) &= S(\{a,b\}).
\end{aligned}$$

□

Def. (3.11.5.5) [Co-Poisson Hopf Algebras]. A **co-Poisson Hopf algebra** is a Hopf algebra $(H, \text{mul.}, \eta, \Delta, \varepsilon, S)$ equipped with a co-Poisson co-algebra structure $q : H \to H \otimes H$(3.11.2.10) s.t. for any $a,b \in H$,

$$q(ab) = q(a)\Delta(b) + \Delta(a)q(b).$$

Notice if H is co-commutative, then this just means that mul. $: H \otimes H \to H$ is a co-Poisson co-algebra homomorphism, by(3.11.2.14). ⌟

Prop. (3.11.5.6) [Poisson-Hopf Algebras and Co-Poisson Hopf-algebras]. Let $R \in \mathcal{CR}\text{ing}$ and $(H, \text{mul.}, \eta, \Delta, \varepsilon, S)$ be a Hopf algebra over R with an R-linear map $q : H \to H \otimes H$, then (H,q) is a co-Poisson structure iff (H^*, q^*) is a Poisson-Hopf algebra.

And if $\sigma : H_1 \to H_2$ is a linear map between co-Poisson Hopf algebras over R, then σ is a homomorphism of co-Poisson Hopf algebras iff $\sigma^* : D^* \to C^*$ is a homomorphism of Poisson-Hopf algebras. ⌟

Prop. (3.11.5.7). For a co-Poisson Hopf algebra $(H, \mu, \eta, \Delta, \varepsilon, S, \{-,-\})$, the unit $\eta : R \to H$ is a co-Poisson co-algebra homomorphism: $q(1) = 0$. And if H is co-commutative, then $S : H \to H$ is a co-Poisson co-algebra anti-homomorphism. ⌟

Proof: This follows from(3.11.5.6) and(3.11.5.4). □

Prop. (3.11.5.8) [Co-Poisson Hopf Structures on $U(\mathfrak{g})$]. For $k \in \texttt{Field}^0$ and $\mathfrak{g} \in \texttt{LieAlg}_k$, co-Poisson Hopf structures on $U(\mathfrak{g})$ are equivalent to Lie bi-algebra structures on $\mathfrak{g}$. ⌟

Proof: Cf.[A guide to quantum groups]P178. □

Quantization of (Co-)Poisson Hopf Algebras

Def. (3.11.5.9) [Deformations of Hopf Algebras]. For $k \in \mathtt{Field}$ and a Hopf algebra $(A, \text{mul.}, \eta, \Delta, \varepsilon, S)$ over k, a **deformation of Hopf algebra** is a topological Hopf algebra $(A_\hbar, \text{mul.}, \eta_\hbar, \Delta_\hbar, \varepsilon_\hbar, S_\hbar)$ over $k[[\hbar]]$ s.t.

- $A_\hbar \cong A[[\hbar]]$ as $k[[\hbar]]$-modules.
- $\mu_\hbar \equiv \mu (\text{mod } \hbar), \Delta_\hbar \equiv \Delta (\text{mod } \hbar)$.

Two deformations $A_\hbar, A'_\hbar$ are called equivalent if there is an isomorphism of Hopf algebras $f : A_\hbar \cong A'_\hbar$ over $k[[\hbar]]$ s.t. $f \equiv 1 (\text{mod } \hbar)$. ⌟

Def. (3.11.5.10) [Infinitesimal Deformations of Hopf Algebras]. Cf.[A guide to Hopf algebras]P172. ⌟

Def. (3.11.5.11) [Quantization of Poisson-Hopf Algebras]. For $k \in \mathtt{Field}$ and a commutative Poisson algebra $(A, \cdot, \{-,-\})$ over k, a **quantization of Poisson algebra** $A_\hbar$ is a topological associative algebra $(A_\hbar, \cdot_\hbar) \in \mathcal{A}\mathrm{lg}_{\mathbb{C}[[\hbar]]}$ s.t.

- $A_\hbar \cong A[[\hbar]]$ as $k[[\hbar]]$-modules.

$$\cdot_\hbar = \cdot (\text{mod } \hbar).$$

$$\{\bar{a}, \bar{b}\} \equiv \frac{ab - ba}{\hbar} (\text{mod } \hbar), \quad a, b \in A_\hbar.$$

And if A is a Poisson-Hopf algebra(3.11.5.1), then a **quantization of Poisson-Hopf algebra** $A_\hbar$ is a Hopf algebra deformation of A over $k[[\hbar]]$(3.11.5.9) that is also a quantization of the Poisson structure. ⌟

Def. (3.11.5.12) [Quantization of Poisson-Lie Groups]. if $(G, \{-,-\})$ is a Poisson-Lie algebra, then a **quantization of Poisson-Lie group** $\mathcal{F}_\hbar(G)$ is a quantization of the Poisson-Hopf algebra $\mathcal{O}(G)$(3.11.5.11). And $(G, \{-,-\})$ is called the **classical limit** of $\mathcal{F}_\hbar(G)$. ⌟

Prop. (3.11.5.13). Let $k \in \mathtt{Field}, \operatorname{char} k \neq 2$, and $\mathfrak{g} \in \mathtt{LieAlg}_k$ is non-Abelian, then there are no non-trivial Poisson Hopf structures on $U(\mathfrak{g})$. ⌟

Proof: ? □

Quantized Universal Enveloping Algebras

6 Lie Bi-algebras

Def. (3.11.6.1) [Lie bi-algebras]. For $k \in \mathtt{Field}$, a **Lie bi-algebra** is a Lie algebra $\mathfrak{g} \in \mathtt{LieAlg}_k$ together with a skew-symmetric linear map $\delta : \mathfrak{g} \to \mathfrak{g} \otimes \mathfrak{g}$ called the **co-commutator** s.t.

- $\delta^* : \mathfrak{g}^* \otimes \mathfrak{g}^* \to \mathfrak{g}^*$ is a Lie algebra structure on $\mathfrak{g}$.
- δ is a 1-cocycle on $\mathfrak{g}$ with values in $\mathfrak{g} \otimes \mathfrak{g}$, i.e.

$$\delta[X, Y] = (\mathrm{ad}_X \otimes \mathrm{id} + \mathrm{id} \otimes \mathrm{ad}_X)\delta(Y) + (\mathrm{ad}_Y \otimes \mathrm{id} + \mathrm{id} \otimes \mathrm{ad}_Y)\delta(X).$$

⌟

7 Yang-Baxter Equations

Set-Theoretical Solutions

Def. (3.11.7.1) [Quantum Yang-Baxter Equations]. For $S \in \mathcal{S}\mathrm{et}$, a map $R : S \times \times S \to S \times S$ is said to satisfy the (set-theoretic)**quantum Yang-Baxter equation** if R is a bijection and

$$R_{12} \circ R_{13} \circ R_{23} = R_{23} \circ R_{13} \circ R_{12} : S \times S \times S \to S \times S \times S.$$

⌟

Thm. (3.11.7.2). Suppose $G \in \mathcal{G}\mathrm{rp}$, and ξ, η are left and right actions of G on itself satisfying the following condition:

$$uv = ({}^{\xi(u)}v)(u^{\eta(v)}), \quad \forall u, v \in G,$$

then

$$R : G \times G \to G \times G : (u, v) \mapsto (u^{\eta(v)}, {}^{\xi(u)}v)$$

is a solution of the set-theoretic Yang-Baxter equation(3.11.7.1) on G. ⌟

Proof: Cf.[ON THE SET-THEORETICAL YANG-BAXTER EQUATION]. □

Thm. (3.11.7.3) [Universal Braid relations]. Let $\sigma : S \times S \to S \times S$ be a non-degenerate solution of the braid relation, and let $G(S, \sigma)$ be the group generated by S subject to the relation $uv \sim yx$ whenever $\sigma(u, v) = (y, x)$, with a natural map $i : S \to G(S, \sigma)$. Then there is a unique braiding operator σ^G on $G(S, \sigma)$ commuting with i, and it is the initial object in the category of such groups with a braiding operator. ⌟

Proof: Cf.[ON THE SET-THEORETICAL YANG-BAXTER EQUATION]P16. □

8 Quiver Hecke Algebra

Cf.[Bru13].

4 Categories and Algebraic Topology

4.1 Categories

Main references are [Mac98], [Bor94], [Coend Calculus, Fosco Loregian].

1 Basics

Def. (4.1.1.1)[Categories, Eilenberg-Mac.Lane1945]. A **category** $\mathcal{C}$ consists of the following data:

- A class $\mathrm{Ob}(\mathcal{C})$ of **objects of** $\mathcal{C}$.
- For any $x, y \in \mathrm{Ob}(\mathcal{C})$ a class $\mathrm{Mor}(x, y)$ of **morphisms from** x **to** y.
- For any $(x, y, z) \in \mathrm{Ob}(\mathcal{C})$, a map of classes $\circ : \mathrm{Mor}(y, z) \times \mathrm{Mor}(x, y) \to \mathrm{Mor}(x, z)$, called the **composition law** of $\mathcal{C}$.

that satisfies:

- (Identity)For any $x \in \mathrm{Ob}(\mathcal{C})$, there exists an element $\mathrm{id}_x \in \mathrm{Mor}(x, x)$ s.t. $\mathrm{id}_x \circ \varphi = \varphi, \psi \circ \mathrm{id}_x = \psi$ whenever these composition makes sense. It is clear such an element is unique.
- (Associativity)$(\varphi \circ \psi) \circ \chi = \varphi \circ (\psi \circ \chi)$ whenever these compositions make sense.

⌟

Remark (4.1.1.2). For $\mathcal{C} \in \mathcal{C}\mathrm{at}$, we will sometimes say $x \in \mathcal{C}$ to mean that x is an element of $\mathrm{Ob}(\mathcal{C})$ and $f : x \to y \in \mathcal{C}$ or f is a morphism in $\mathcal{C}$ to mean: $x, y \in \mathrm{Ob}(\mathcal{C})$ and $f \in \mathrm{Mor}(x, y)$. Hopefully this won't make any confusions. ⌟

Def. (4.1.1.3)[Dual Categories]. Let $\mathcal{C}$ be a category, then the **dual category** of $\mathcal{C}$ is a category $\mathcal{C}^{\mathrm{op}}$ with

- $\mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathcal{C})$.
- For $x, y \in \mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) = \mathrm{Ob}(\mathcal{C})$, $\mathrm{Mor}_{\mathcal{C}^{\mathrm{op}}}(x, y) = \mathrm{Mor}_{\mathcal{C}}(y, x)$.
- The composition law of $\mathcal{C}^{\mathrm{op}}$ is induced from that of $\mathcal{C}$.

⌟

Def. (4.1.1.4) [Isomorphisms]. Let $\mathcal{C}$ be a category, an **isomorphism** in $\mathcal{C}$ is a morphism $\varphi \in \mathrm{Mor}(x, y)$ in $\mathcal{C}$ s.t. there exists a morphism $\psi \in \mathrm{Mor}(y, x)$ s.t. $\varphi \circ \psi = \mathrm{id}_y$ and $\psi \circ \varphi = \mathrm{id}_x$. it is clear that such a ψ is unique, and if it exists, it is called the **inverse morphism** of φ.

For $x, y \in \mathcal{C}$, if there exists an isomorphism in $\mathrm{Mor}(x, y)$, x, y are said to be **equivalent objects**. ⌟

Def. (4.1.1.5) [Functors]. Let $\mathcal{C}, \mathcal{C}'$ be categories, a **functor** F from $\mathcal{C} \to \mathcal{C}'$ consists of the following data:

- a morphism of sets $\mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{C}') : x \mapsto F(x)$.

- for any $x, y \in \mathrm{Ob}(\mathcal{C})$, a morphism of sets $\mathrm{Mor}(x, y) \to \mathrm{Mor}(F(x), F(y)) : f \mapsto F(f)$.

that satisfies:

- $F(\mathrm{id}_x) = \mathrm{id}_{F(x)}$.
- $F(\varphi \circ \psi) = F(\varphi) \circ F(\psi)$ whenever $\varphi \circ \psi$ is defined.

A **contravariant functor** from $\mathcal{C}$ to $\mathcal{C}'$ is defined to be a functor from $\mathcal{C}^{\mathrm{op}}$ to $\mathcal{C}'$. ⌟

Def. (4.1.1.6) [Identity Functor $\mathrm{id}_{\mathcal{C}}$]. For any $\mathcal{C} \in \mathcal{C}\mathrm{at}$, there is an identity functor $\mathrm{id}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$. ⌟

Def. (4.1.1.7) [Natural Transformations]. Let $\mathcal{C}, \mathcal{C}'$ be categories and $F, G : \mathcal{C} \to \mathcal{C}'$ be functors between categories, then a **natural transformation** η from F to G consists of an element η_x for each $x \in \mathrm{Ob}(\mathcal{C})$ s.t. for any $f : x \to y \in \mathcal{C}$, the following diagram is commutative:

$$\begin{array}{ccc} F(x) & \xrightarrow{F(f)} & F(y) \\ \downarrow{\scriptstyle \eta_x} & & \downarrow{\scriptstyle \eta_y} \\ G(x) & \xrightarrow{G(f)} & G(y) \end{array}.$$

Then for any two categories $\mathcal{C}, \mathcal{C}'$, there is a category $\mathrm{Fun}(\mathcal{C}, \mathcal{C}')$ consisting of the set of functors from $\mathcal{C}$ to $\mathcal{C}\prime$, and natural transformations as morphisms between functors. ⌟

Def. (4.1.1.8) [Final and Initial Objects]. An object Z of a category is called a **final object** if $\#\,\mathrm{Hom}(X, Z) = 1$ for any object X. It is called **weakly final** if $\mathrm{Hom}(X, Z) \neq \varnothing$ for every object X.

Dually an object is called **(weakly)initial** if it is (weakly)initial as an object of $\mathcal{C}^{\mathrm{op}}$. ⌟

Def. (4.1.1.9) [Filtered Categories]. A **filtered category** is a category $\mathcal{I}$ that:

- It is nonempty.
- for any $a, b \in \mathcal{I}$, there is some $c \in \mathcal{I}$ with morphisms $a \to c, b \to c$
- for any two morphisms $a, b : x \to y$, there is a morphism $c : y \to z$ that $c \circ a = c \circ b$.

⌟

Def. (4.1.1.10) [Fully Faithful Functors]. A functor of category $F : \mathcal{C} \to \mathcal{D}$ is called:

- a **full/faithful functor** if for any $x, y \in \mathrm{Ob}(\mathcal{C})$, $F : \mathrm{Hom}(X, Y) \to \mathrm{Hom}(F(x), F(y))$ is surjective/injective.
- an **essentially surjective functor** if any object of $\mathcal{D}$ is equivalent to some $f(x)$, where $x \in \mathcal{C}$.
- an **equivalence** if there is a functor $G : \mathcal{D} \to \mathcal{C}$ that $F \circ G \cong \mathrm{id}_{\mathcal{D}}$ and $G \circ F \cong \mathrm{id}_{\mathcal{C}}$.

⌟

Prop. (4.1.1.11) [Category Equivalences]. A Functor $\mathcal{C} \to \mathcal{D}$ is an equivalence if and only if it's fully faithful and essentially surjective. ⌟

Proof: There exist an object $G(X) \in \mathcal{C}$ and an isomorphism $\xi_X : FG(X) \to X$ for every $X \in \mathcal{D}$. Because F is fully faithful, there exists a unique morphism $G(f) : G(X) \to G(Y)$ such that $F(G(f)) = \xi_Y^{-1} \circ f \circ \xi_X$ for every morphism $f : X \to Y$ in $\mathcal{D}$. Thus we obtain a functor $G : \mathcal{C} \to \mathcal{D}$ as well as a natural isomorphism $\xi : F \circ G \to \mathrm{Id}_{\mathcal{D}}$. Moreover, the isomorphism $\xi_{F(Z)} : FGF(Z) \to F(Z)$ decides an isomorphism $\eta_Z : GF(Z) \to Z$ for every $Z \in \mathcal{C}$. This yields a natural isomorphism $\eta : G \circ F \to \mathrm{Id}_{\mathcal{C}}$. □

Def. (4.1.1.12) [Setoids]. A **setoid** is a category that is equivalent to a category that has only the identity morphisms. ⌟

Def. (4.1.1.13) [Groupoids]. A **groupoid** is a category that all morphisms are isomorphisms. The full subcategory of $\mathcal{C}at$ consisting of groupoids is denoted by $\mathcal{G}rpd$. ⌟

Prop. (4.1.1.14) [Equivalence Relations]. An **equivalence relation** is a groupoid that $\# \operatorname{Mor}_{\mathcal{C}}(x, y) \leq 1$ for any $x, y \in \mathcal{C}$. ⌟

Prop. (4.1.1.15). A category is equivalent to a setoid iff it is an equivalence relation. ⌟

Proof:

□

Def. (4.1.1.16) [Subcategories]. Let $\mathcal{C}$ be a category, a **subcategory** $\mathcal{C}'$ of $\mathcal{C}$ is a category together with a functor $F : \mathcal{C}' \to \mathcal{C}$ s.t. $F : \operatorname{Ob}(\mathcal{C}') \to \operatorname{Ob}(\mathcal{C})$ is injective and F is faithful. And it is called a **full subcategory** if F is fully fatihful. It is called a **strictly full subcategory** if for any $y \in \mathcal{C}$, y is equivalent to some $F(x), x \in \operatorname{Ob}(\mathcal{C}')$ iff $y \in F(\mathcal{C}')$. ⌟

Def. (4.1.1.17) [Comma Categories]. For a category $\mathcal{C}$ and an object S, the **comma category** $\mathcal{C}/S$ is defined to be the category of arrows $T \to S$ with the arrows being compatible arrows over S. ⌟

Def. (4.1.1.18) [Category of Arrows]. For a category $\mathcal{C}$, the category of arrows $\mathcal{A}rr(\mathcal{C})$ is a category whose objects are arrows in $\mathcal{C}$ and a morphism $f \to g$ is a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{h} & B \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ A' & \xrightarrow{k} & B' \end{array}$$

⌟

Def. (4.1.1.19) [Twisted Arrow Category]. For a category $\mathcal{C}$, the category of twisted arrows $TW(\mathcal{C})$ is a category whose objects are arrows in $\mathcal{C}$ and a morphism $f \to g$ is a diagram

$$\begin{array}{ccc} A & \xleftarrow[h]{} & B \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ A' & \xrightarrow{k} & B' \end{array}$$

⌟

Def. (4.1.1.20) [Epimorphisms and Monomorphisms]. An **epimorphism** in a category is a morphism $X \to Y$ that the map $\operatorname{Map}(Y, Z) \to \operatorname{Map}(X, Z)$ induced by composition is injective. Dually, an **monomorphism** is an epimorphism in the dual category.

A **balanced category** is a category s.t. every morphism that is both epi and mono is an isomorphism. ⌟

Def. (4.1.1.21) [Projective and Injective]. A **projective object** X in a category is an object that for any epimorphism(4.1.1.20) $Y \to Z$, $\operatorname{Hom}(X, Y) \to \operatorname{Hom}(X, Z)$ is surjective. Dually, an **injective object** X is a projective object in the dual category. ⌟

Def. (4.1.1.22) [Retract]. A morphism f in a category $\mathcal{C}$ is called a **retract** of g if there are morphisms $F, G : f \to g$ in $\operatorname{Mor}(\mathcal{C})$(4.1.1.18) that $G \circ F = \operatorname{id}_f$. ⌟

Def. (4.1.1.23) [Equivalence relations]. For $\mathcal{C} \in \mathcal{C}at$ has finite products, $X_0 \in \mathcal{C}$, an **equivalence relation on** X_0 is a tuple (X_1, u), where $X_1 \in \mathcal{PS}h(\mathcal{C})$ and $u \in \mathrm{Hom}(X_1, X_0 \times X_0)$ s.t for any $X \in \mathcal{C}$, the map

$$\widetilde{X}_1(T) \xrightarrow{u} \widetilde{X}_0(T) \times \widetilde{X}_0(T)$$

is a bijection of $\widetilde{X}_1(T)$ onto the graph of an equivalence relation on $\widetilde{X}_1(T)$. Similarly, we can define **pre-relations on** X_0, **relations on** X_0 and **pre-equivalence relations on** X_0. ⌟

Prop. (4.1.1.24) [Involutions]. Situation as in(4.1.1.23), then there is a morphism $\sigma : F_0 \to F_0$, $\sigma^2 = \mathrm{id}, u_0 \circ \sigma = u_1, u_1 \circ \sigma = u_0$, by the symmetry in the definition of equivalence relations. ⌟

Def. (4.1.1.25) [Categorical Quotients]. Situation as in(4.1.1.23), for an equivalence relation $u : X_1 \to X_0 \times X_0$, a morphism $v : X_0 \to X$ is called a categorical quotient if

- u factors through $u : X_1 \to X_0 \times_X X_0$, and $u : X_1 \to X_0 \times_X X_0$ is an isomorphism.
- For any $T \in \mathcal{C}$, there is a cokernel sequence

$$\mathrm{Mor}(X, T) \to \mathrm{Mor}(X_0, T) \rightrightarrows \mathrm{Mor}(X_1, T)$$

  is exact.

⌟

Representable Functors

Def. (4.1.1.26) [Presheaves]. A **presheaf** on a category $\mathcal{C}$ is defined to be a contravariant functor from $\mathcal{C}$ to $\mathcal{S}et$. The category of presheaves on $\mathcal{C}$ is denoted by $\mathcal{PS}h(\mathcal{C})$. ⌟

Prop. (4.1.1.27) [Representability Criterion]. Let $\mathcal{C}$ be a complete category, $F : \mathcal{C} \to \mathcal{S}et$ be a functor. Assume that F commutes with small limits, and the category $\mathcal{I}$ of pairs (x, f) where $x \in \mathcal{C}, f \in F(x)$ has a cofinal family of objects indexed by a set I, then F is representable, i.e. there is an object x that $F(y) = \mathrm{Mor}_{\mathcal{C}}(x, y)$, functorial in y. ⌟

Proof: Because $\mathcal{C}$ has small limits, let $\mathcal{I}'$ be the full subcategory of $\mathcal{I}$ generated by (x_i, f_i), set $x = \varprojlim_{(x_i, f_i) \in \mathcal{I}'} x_i$. As F commutes with limits, $F(x) = \varprojlim_{(x_i, f_i) \in \mathcal{I}} F(x_i)$. Hence there is a universal element $f \in F(x)$ that maps to f_i under $F(x \to x_i)$. f induces a natural transformation $\xi : \mathrm{Mor}_{\mathcal{C}}(x, -) \to F(-)$.

The assumption shows ξ is surjective. Now let $x' \to x$ be the equalizer of all maps $\varphi : x \to x$ that $F(\varphi)f = f$, then there is a $f' \in F(x')$ mapping to f. then the transformation ξ' defined by f' is also surjective. Now we also want to show it is injective: if $a, b \in \mathrm{Mor}_{\mathcal{C}}(x', y)$ mapsto the same element, then we consider the equalizer $e' : x'' \to x'$ of a, b, then the assumption and the fact F commutes with equalizer shows there is a $f'' \in F(x'')$ mapping to f'.

By universality consider a morphism $\psi : x \to x''$ that $F(\psi)f = f''$, then $e \circ e' \circ \psi$ is a morphism $x \to x$ that fixes f, thus by construction $ee'\psi e = e$, so $e'\psi e = \mathrm{id}$, because e is a monomorphism. Then e' is an epimorphism, thus $a = b$. □

Adjunctions

Def. (4.1.1.28) [Adjunction Pairs]. A pair of functors (f, g) where $f : \mathcal{C} \to \mathcal{D}, g : \mathcal{D} \to \mathcal{C} \in \mathcal{C}at$ are called an **adjunction pair** iff there is natural isomorphism of functors:

$$\mathcal{C}^{\mathrm{op}} \times \mathcal{D} \to \mathcal{S}et : \mathrm{Hom}(f(-), -) \cong \mathrm{Hom}(-, g(-)).$$

Equivalently this means that for any $X_1 \to X_2 \in \mathcal{C}, Y_1 \to Y_2 \in \mathcal{D}$,

$$\begin{array}{ccc} f(X_1) & \longrightarrow & Y_1 \\ \downarrow & & \downarrow \\ f(X_2) & \longrightarrow & Y_2 \end{array}$$

is commutative iff its corresponding map

$$\begin{array}{ccc} X_1 & \longrightarrow & g(Y_1) \\ \downarrow & & \downarrow \\ X_2 & \longrightarrow & g(Y_2) \end{array}$$

is commutative.

Denoted an adjunction pair by $(f,g) : \mathcal{C} \rightleftarrows \mathcal{D}$. ⌟

Prop. (4.1.1.29) [Units and Counits]. If f, g are adjoints, then there are natural transformations $u : \mathrm{id} \to gf$, and $v : fg \to \mathrm{id}$, called the **unit/counit maps**. They satisfies $f \xrightarrow{u} fgf \xrightarrow{v} f$ is id, and $g \xrightarrow{u} gfg \xrightarrow{v} f$ is id.

Conversely, if there are natural morphisms u, v satisfying these two identities, then (f,g) is an adjuntion, by

$$\mathrm{Hom}(fX,Y) \to \mathrm{Hom}(gfX,gY) \to \mathrm{Hom}(X,gY) \to \mathrm{Hom}(fX,fgY) \to \mathrm{Hom}(fX,Y).$$

⌟

Proof: □

Lemma (4.1.1.30). Let (f,g) be an adjunction pair, then

- If $g \circ f$ is fully faithful, then f is fully faithful.
- If $f \circ g$ is fully faithful, then g is fully faithful.

⌟

Proof: Cf.[Sta]0FWV. □

Prop. (4.1.1.31). Let (f,g) be an adjunction pair, then

- f is fully faithful iff $u : \mathrm{id} \to gf$ is an isomorphism.
- g is fully faithful iff $v : fg \to \mathrm{id}$ is an isomorphism.

⌟

Proof: 1: If $\mathrm{id} \cong gf$, then gf is fully faithful, so f is fully faithful by(4.1.1.30). If f is fully faithful, then for any X, Y,

$$\mathrm{Hom}(X,Y) \xrightarrow{u} H(X, gfY) \cong H(fX, fY) \cong H(X,Y)$$

is a canonical isomorphism, so u is an isomorphism.

2 is dual to 1. □

Cor. (4.1.1.32) [Units and Equivalences]. Let (F,G) be an adjunction pair, then the following are equivalent:

- F, G are both fully faithful.
- the unit and counit are both isomorphisms.
- F, G defines an equivalence of categories.

⌟

Proof: $1 \to 2 \to 3$ follow from(4.1.1.31). And $3 \to 1$ is clear. □

Prop. (4.1.1.33) [Adjunction Preserves (Co)Limits]. A right adjoint functor is left exact and it preserves injectives if its left adjoint is exact.

A left adjoint functor is right exact and it preserves projectives if its right adjoint is exact. ⌟

Prop. (4.1.1.34) [Adjoint Functor Theorem]. Let $G : \mathcal{C} \to \mathcal{D} \in \mathcal{C}\mathrm{at}$, assume $\mathcal{C}$ is complete and G commutes with small limits. Assume for every $y \in \mathcal{D}$, the category of pairs (x, f) where $x \in \mathcal{C}$ and $f \in \mathrm{Mor}_{\mathcal{D}}(y, G(x))$ has a cofinal family of objects indexed by a set I, then G has a left adjoint.

Similarly the dual statement holds. ⌟

Proof: The assumption shows that for any $y \in \mathcal{D}$, the functor $x \mapsto \mathrm{Mor}_{\mathcal{D}}(y, G(x))$ satisfies the condition of(4.1.1.27), thus it is representable by an object denoted by $F(y)$. By Yoneda lemma, F underlies a functor, and this functor is a left adjoint of G. □

Prop. (4.1.1.35) [Groupoidification]. There is a functor $\mathcal{G}\mathrm{rpd} : \mathcal{C}\mathrm{at} \to \mathcal{G}\mathrm{rpd}$ that is left adjoint to the inclusion functor, called the **groupoidification functor**. ⌟

Proof: □

Prop. (4.1.1.36) [Examples of Adjunction pairs].

- The valuation at k-th coordinate is left adjoint to the functor $k_*(A)(i) = \prod_{\mathrm{Hom}\, i,k} A$ and is exact. So k_* preserves injectives.
- The sheaf Γ functor is right adjoint to the constant sheaf functor over arbitrary site.
- The inclusion functor is right adjoint to the shifification functor over arbitrary site.
- The forgetful functor is right adjoint to the Shifification functor, and shifification is exact, so it preserves injectives.
- The stalk functor is left adjoint to the skyscraper sheaf operator.

⌟

Limits and Colimits

Prop. (4.1.1.37) [Products and Equalizers Implies Limits]. If a category admits arbitrary(resp. finite) products and equalizers, then it admits arbitrary(resp. finite) limits. Dually a category that admits coproducts and coequalizers admits all colimits. ⌟

Proof: The limits over a category $\mathcal{C}$ is an equalizer of products over the category of arrows in $\mathcal{C}$. □

Def. (4.1.1.38) [Exact Functors]. A functor $F : \mathcal{C} \to \mathcal{D}$ is called a **left exact functor** if it maps finite limits to finite limits. It is called a **right exact functor** if it maps finite colimits to finite colimits. It is called an **exact functor** if it is both left exact and right exact. ⌟

Def. (4.1.1.39) [(Co)Complete Category]. A category is called **(co)complete** if it has all small (co)limits, i.e. (co)limits over small categories(4.1.2.1). ⌟

Def. (4.1.1.40) [Inverse Systems]. An **inverse system** in $\mathcal{C}$ is a diagram $\mathbb{Z}_+^{\mathrm{op}} \to \mathcal{C}$, where $\mathbb{Z}_+$ is the category of non-negative integers with a unique morphism $n \to m$ iff $n \le m$. ⌟

Prop. (4.1.1.41) [Equivalent Inverse System]. Two inverse systems $\{A_n\}, \{B_n\}$ are called equivalent if there are two non-decreasing unbounded maps $\alpha, \beta : \mathbb{Z}_+ \to \mathbb{Z}_+$ and maps $\alpha : A_n \to B_{\alpha(n)}, \beta : B_n \to A_{\beta(n)}$ that is compatible with the transition maps and for any n, there is a m large that $A_m \to A_{\beta\alpha(m)} \to A_n$ coincide with the transition map $A_m \to A_n$, and similar for B_n. And similarly for colimits.

The limit for two inverse systems are the same, and similarly for colimits. ⌟

Prop. (4.1.1.42) [Filtered Colimit of Sets]. Filtered colimits in $\mathcal{S}\mathrm{et}$ commutes with finite limits. ⌟

Proof: Cf.[Sta]002W. □

Prop. (4.1.1.43) [Cofiltered Limits of Sets]. A cofiltered limit of nonempty sets is nonempty. ⌟

Proof: Cf.[Sta]086J. □

Def. (4.1.1.44) [Mittag-Leffler]. If (A_i, φ_{ji}) is a directed inverse system of sets over I, then it is said to satisfy the **Mittag-Leffler condition** if $\varphi_{ji}(A_j) \in A_i$ stabilizes. This is clearly true if φ_{ji} is surjective for any i, j. ⌟

Prop. (4.1.1.45). If (A_n) where $n \in \mathbb{Z}$ is a Mittag-Leffler inverse system of nonempty sets, then $\lim A_i$ is also nonempty. ⌟

Proof: Let $A'_j = \cap_{j \ge i} \varphi_{ji} A_j$, then (A'_j) is a filtered system that the transition maps are all surjective, and clearly $\lim A_j = \lim A'_j$, so it is nonempty by(4.1.1.43). □

Prop. (4.1.1.46). $\mathcal{C}\mathrm{at}$ is complete and cocomplete. ⌟

Proof: □

Fiber Product

Prop. (4.1.1.47). For a category C, the following are equivalent:

- It has arbitrary limits.
- it has arbitrary products and equalizer.
- it has arbitrary products and fibered products.

⌟

Proof: $1 \to 2, 1 \to 3$ is trivial. $3 \to 2$: The equalizer for $f, g : X \to Y$ can be constructed as the base change of $Y \to Y \otimes Y$ along $(f, g) : X \to Y \times Y$. $2 \to 1$: for any diagram $F : I \to C$, the fibered pullback can be constructed as the equalizer of two morphisms:

$$s, t : \prod_{i \in \mathrm{Ob}(I)} F(i) \to \prod_{f : j \to k \in \mathrm{Mor}(I)} F(k)$$

where $\pi_{(f:j \to k)} s = \pi_k$, and $\pi_{(f:j \to k)} t = (Ff)\pi_j$. □

Prop. (4.1.1.48) [Diagonal Base Change]. The diagonal commutes with base change:

$$\begin{array}{ccc} X\times_Y Z & \xrightarrow{\Delta} & (X\times_Y Z)\times_Z(X\times_Y Z)\\ \downarrow & & \downarrow\\ X & \xrightarrow{\Delta} & X\times_Y X\end{array}$$

⌟

Proof: □

Prop. (4.1.1.49). $(X\times_E Y)\times_S(Z\times_F W)=(X\times_S Z)\times_{E\times_S F}(Y\times_S W)$. ⌟

Proof: □

Prop. (4.1.1.50). For $f:X\to T$ and $g:Y\to T$ and $h:T\to S$, $X\times_T Y=T\times_{T\times_S T}(X\times_S Y)$. In particular, $X\times_T Y\to X\times_S Y$ is a base change of $T\to T\times_S T$. ⌟

Proof: For any object U,

$$\mathrm{Hom}(U,X\times_T Y)=\{s:U\to X,t:U\to Y|f\circ s=g\circ t\},$$

$$\mathrm{Hom}(U,T\times_{T\times_S T}(X\times_S Y))=\{r:U\to T,s:U\to X,t:U\to Y|h\circ f\circ s=h\circ g\circ t,r=g\circ t,r=f\circ s\},$$

so they are functorially isomorphic. Then by Yoneda lemma we have the desired isomorphism. □

Prop. (4.1.1.51). The diagonal map $X\to X\times_Y X$ is an isomorphism iff $X\to Y$ is monomorphism. (Because this is equivalent to $\mathrm{pr}_1=\mathrm{pr}_2$). ⌟

Def. (4.1.1.52) [Mapping graph]. Let $f:X\to Y$ be a morphism in a category with fiber products and finite products, then the **mapping graph** Γ_f of f is defined to be the pullback

$$\begin{array}{ccc} \Gamma_f & \longrightarrow & X\times Y\\ \downarrow & & \downarrow\\ Y & \xrightarrow{\Delta} & Y\times Y\end{array}.$$

it can be seen that Γ_f is isomorphic to X. ⌟

Localizations

Def. (4.1.1.53) [Localized Categories]. Let $\mathcal{C}\in\mathcal{C}\mathrm{at}$ and $S\subset\mathrm{Mor}(\mathcal{C})$, then a functor $F:\mathcal{C}\to\mathcal{D}$ is called a **Localized category** of $\mathcal{C}$ w.r.t S if it maps morphisms in S to isomorphisms, and any other functor with this property factors uniquely through F. ⌟

Def. (4.1.1.54) [Localizing Systems]. For $\mathcal{C}\in\mathcal{C}\mathrm{at}$, a class of morphisms S in $\mathcal{C}$ is called a left(resp. right) **localizing system** if:

(LS1): S is closed under composition and contains all the identities.

(LS2): for every $s\in S$ and f with the same source(resp. target), there exists $t\in S,g\in\mathrm{Mor}(\mathcal{C})$ s.t. $t\circ f=g\circ s$(resp. $f\circ t=s\circ g$).

(LS3): For $f,g\in\mathrm{Mor}(\mathcal{C})$ with the same source and target, the existence of a $t\in S$ s.t. $ft=gt$ implies(resp. is implied by) the existence of a $s\in S$ s.t. $sf=sg$.

It is called **localizing system** if it is both left localizing and right localizing. ⌟

Def. (4.1.1.55) [Saturated Localizing Systems]. Let S be a localizing system, then it is called a **saturated localizing system** is moreover it satisfies

- if $f, g, h \in S$ and $fg, gh \in S$, then $g \in S$.

⌟

Def. (4.1.1.56)[Gabriel-Zisman Localization]. If $\mathcal{C} \in \mathcal{C}\mathrm{at}$ and $S \subset \mathrm{Mor}(\mathcal{C})$, we construct a category $S^{-1}\mathcal{C}$ as follows:

- $\mathrm{Ob}(S^{-1}\mathcal{C}) = \mathrm{Ob}(\mathcal{C})$.
- For $X, Y \in \mathrm{Ob}(S^{-1}\mathcal{C})$, $\mathrm{Mor}(X,Y) = \{(f,s) | f : X \to Y', s : Y \to Y', s \in S\}/\sim$, where the equivalence relation is generated by the following relations: $(f_1, s_1), (f_2, s_2) \in \mathrm{Mor}_{S^{-1}\mathcal{C}}(X,Y)$ are equivalent if there exists some commutative diagram in $\mathcal{C}$:

$$\begin{array}{ccccc} X & \xrightarrow{f_1} & Y' & \xleftarrow{s_1} & Y \\ & {\scriptstyle f_2}\searrow & \downarrow{\scriptstyle u} & \swarrow{\scriptstyle s_2} & \\ & & Y'' & & \end{array}.$$

  the pair (f,s) is also denoted by $s^{-1}f$.
- The composition of two morphisms $(f : X \to Y', s : Y \to Y')$ and $(g : Y \to Z', t : Z \to Z')$ is defined to be the equivalence class of $(hf : X \to Z'', ut : Z \to Z'')$, where h and $u \in S$ are chosen to fit in the commutative diagram

$$\begin{array}{ccc} Y & \xrightarrow{g} & Z \\ \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle u} \\ Y' & \xrightarrow{h} & Z'' \end{array}.$$

- The identity elements $\mathrm{id}_X \in \mathrm{Mor}(S^{-1}\mathcal{C})$ is defined to be the equivalence class of $(\mathrm{id}_X, \mathrm{id}_X)$.

Then there definitions are well-defined and makes $S^{-1}\mathcal{C}$ a category.

And dually we can define $S^{-1}\mathcal{C}$ for a right localizing system. ⌟

Proof: Cf.[Sta]04VG, □

Cor. (4.1.1.57) [Comparing Morphisms in $S^{-1}\mathcal{C}$]. Suppose $\mathcal{C} \in \mathcal{C}\mathrm{at}$ and $S \subset \mathrm{Mor}(\mathcal{C})$, then given any finite set of morphism $g_i : x \to y$ in $S^{-1}\mathcal{C}$ with the same target, we can find their representatives (f_i, s) with common $s \in S$.

And two morphisms $(f_1 : X \to Y', s : Y \to Y')$ and $(f_2 : X \to Y', s : Y \to Y')$ are equivalent iff there exists $a : Y' \to Y''$ s.t. $a \circ s \in S$ and $a \circ f_1 = a \circ f_2$. ⌟

Proof: These follow from LS1 and LS2 in the definition(4.1.1.54). □

Cor. (4.1.1.58) [$S^{-1}\mathcal{C}$ is the Localized Category]. If $\mathcal{C} \in \mathcal{C}\mathrm{at}$ and $S \subset \mathrm{Mor}(\mathcal{C})$ is a left localizing system, then the rule

$$X \mapsto X, (f : X \to Y) \mapsto \mathrm{id}_Y^{-1} f$$

defines a functor $Q : \mathcal{C} \to S^{-1}\mathcal{C}$ that represents $S^{-1}\mathcal{C}$ as a localizing category of $\mathcal{C}$ w.r.t S(4.1.1.53). And Q preserves finite colimits.

The dual statement is true for a right localizing system S. ⌟

Proof: It is clearly a functor, and for any $s\in S$, $Q(s)$ is an isomorphism with inverse (id_Y, s). To show that it preserves finite colimits, notice

$$\begin{aligned}\mathrm{Mor}_{S^{-1}\mathcal{C}}(\mathrm{colim}_i X_i, Y) &= \mathrm{colim}_{s:Y\to Y'\in S}\mathrm{Mor}_{\mathcal{C}}(\mathrm{colim}_i X_i, Y')\\ &= \mathrm{colim}_{s:Y\to Y'\in S}\lim_i \mathrm{Mor}_{\mathcal{C}}(X_i, Y')\\ (4.1.1.42) &= \lim_i \mathrm{colim}_{s:Y\to Y'\in S}\mathrm{Mor}_{\mathcal{C}}(X_i, Y')\\ &= \lim_i \mathrm{Mor}_{S^{-1}\mathcal{C}}(X_i, Y)\end{aligned}$$

To show it is the localized category, suppose $G:\mathcal{C}\to\mathcal{D}$ is a functor s.t. $G(s)$ are all isomorphisms for $s\in S$, then we can define $H: S^{-1}\mathcal{C}\to\mathcal{D}: H(x)=x$, and $H((f,s))=G(s)^{-1}\circ G(f)$. Then it can be checked that this is well-defined and $G=H\circ Q$. □

Cor. (4.1.1.59). If $\mathcal{C}\in\mathcal{C}at$ and $S\subset\mathrm{Mor}(\mathcal{C})$ is a localizing system, then the left localizing category and the right localizing category is canonically isomorphic, by the universal property(4.1.1.53). ⌟

Prop. (4.1.1.60) [Saturation]. If $\mathcal{C}\in\mathcal{C}at$ and $S\subset\mathrm{Mor}(\mathcal{C})$ is a localizing system, then the morphisms in $\mathcal{C}$ that is mapped to an isomorphism in $S^{-1}\mathcal{C}$ is the smallest saturated localizing system containing S, called the **saturation of** S. Moreover, it consists of morphisms $f\in\mathrm{Mor}(\mathcal{C})$ s.t. there exists $g,h\in S$ s.t. $gf,gh\in S$. ⌟

Proof: Cf.[Sta]05Q9. □

Prop. (4.1.1.61) [Full Subcategories of Localized Categories]. If S is a left localizing system in a category $\mathcal{C}$, $\mathcal{C}'$ is a full subcategory of $\mathcal{C}$ and S' is a left localizing system of $\mathcal{C}'$ that $S'\subset S$. If for any $s:X\to Y\in S$ and $X\in\mathcal{C}'$, there is a morphism $t:Y\to Z$ that $Z\in\mathcal{C}'$ and $t\circ s\in S'$, then the natural functor $(S')^{-1}\mathcal{C}'\to S^{-1}\mathcal{C}$ is fully faithful. And the dual is true for right localizing systems. ⌟

Proof: This is not hard from the Gabriel-Zisman localization description(4.1.1.56). □

Def. (4.1.1.62) [Reflective Localizations]. A **reflective localization** is an adjunction $(L,R):\mathcal{C}\rightleftarrows\mathcal{D}$ s.t. R is fully faithful. ⌟

Prop. (4.1.1.63) [Reflective Localizations as Localizations]. Let $(L,R):\mathcal{C}\rightleftarrows\mathcal{D}$ be a reflective localization(4.1.1.62), then $\mathcal{D}$ is equivalent to the localization $\mathcal{C}[S^{-1}]$, where S is the class of morphisms of $\mathcal{C}$ that are sent to isomorphisms by L ⌟

Proof: Cf.[Bor94]P190. □

Def. (4.1.1.64) [S-Local Equivalences]. Let $\mathcal{C}\in\mathcal{C}at$ and S a class of morphisms in $\mathcal{C}$.

- $c\in\mathcal{C}$ is called S**-local** if $\mathrm{Hom}(c_2,c)\to\mathrm{Hom}(c_1,c)$ is a bijection for any $c_1\to c_2\in S$.
- $f:c_1\to c_2\in\mathcal{C}$ is called an S**-local equivalence** if for any S-local object $c\in\mathcal{C}$, $\mathrm{Hom}(c_2,c)\to\mathrm{Hom}(c_1,c)$ is a bijection.

⌟

Prop. (4.1.1.65). Let $(L,R):\mathcal{C}\rightleftarrows\mathcal{D}$ is a reflective localization, and let S be the class of morphisms in $\mathcal{C}$ that is mapped sent to isomorphisms by L, then

- The essential image of R consists precisely of S-local objects.
- The S-local

⌟

Group Objects

Def. (4.1.1.66) [Group Object]. In a category $C \in \mathcal{C}\mathrm{at}$ with finite products and a final object e, a(n) **(Abelian)group object** is an object G that h_G is a functor from C to $\mathcal{G}\mathrm{rp}$(resp. $\mathcal{A}\mathrm{b}$). And a homomorphism of group objects is a natural transformation as a functor from C to $\mathcal{G}\mathrm{rp}$.

This is in fact equivalent to a morphism $m_G : G \times G \to G$ and $i_G : G \to G$, $e_G : e \to G$ that satisfy the desired commuting diagrams. ⌟

Def. (4.1.1.67) [Group Action]. A **(left)action** of a group object G on an object X is a map of presheaves $h_G \times h_X \to h_X$ that for any U, $h_G(U) \times h_X(U) \to h_X(U)$ is a group action. This is equivalent to a morphism $\mu : G \times X \to X$ that satisfies the desired commuting diagrams. ⌟

Prop. (4.1.1.68). Let $\mu : G \times X \to X$ be an action of a group object G on an object X, there is a commutative diagram

$$\begin{array}{ccc} G \times X & \xrightarrow{(g,x)\mapsto(g,gx)} & G \times X \\ \downarrow{\scriptstyle (g,x)\mapsto gx} & & \downarrow{\scriptstyle \pi_2} \\ X & \xrightarrow{\quad id \quad} & X \end{array}$$

and the horizontal maps are isomorphisms. ⌟

Cor. (4.1.1.69). Considering the action of G on itself, we get

$$\begin{array}{ccc} G \times G & \xrightarrow{(g,h)\mapsto(g,gh)} & G \times G \\ \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle \pi_2} \\ G & \xrightarrow{\quad \mathrm{id} \quad} & G \end{array}$$

and the horizontal maps are isomorphisms. ⌟

Prop. (4.1.1.70). A unital magma object G in the category of groups is an Abelian group. ⌟

Proof: A unital magma object structure endows G with maps $(\widetilde{m}, \widetilde{e})$, and $\widetilde{m}(ab, cd) = \widetilde{m}(a, c)\widetilde{m}(b, d)$, because $\widetilde{m}$ is a morphism of groups. So we can use Eckmann-Hilton argument2 to show the category multiplication is the same as the group multiplication. So the commutativity of $\widetilde{m}$ with the inverse i implies that it is Abelian. □

Prop. (4.1.1.71). A right-lax monoidal functor(4.1.5.11) between Cartesian monoidal structures maps a unital magma object to a unital magma object. ⌟

Def. (4.1.1.72) [Categorical Quotient]. Let C be a category with finite products, G be a group object in C, $G \times X \to X$ is a left action(4.1.1.67), then a morphism $X \to Y$ is called the **categorical quotient** of X iff Y is the coequalizer of $G \times X \underset{pr_2}{\overset{\rho}{\rightrightarrows}} X$. It is called the **universal categorical quotient** of X iff its product with S is the categorical quotient for each element $S \in C$, in the category $C_{/S}$. ⌟

2 Presentable Categories

Main references are [Locally presentable and accessible categories].

Def. (4.1.2.1) [Small Categories]. Given a regular cardinal κ(2.2.12.2), $S \in \mathcal{S}\mathrm{et}$ is called **κ-small** if it has cardinality smaller than κ. $\mathcal{C} \in \mathcal{C}\mathrm{at}$ is called **κ-small** if $\mathrm{Ob}(\mathcal{C})$ is κ-small, and the set of all morphisms of $\mathcal{C}$ is κ-small.

Through out the whole book, we will fix a strongly inaccessible cardinal κ and call a set or category **small** if it is κ-small. And a category is called **essentially small** if it is equivalent to a small category. ⌟

Prop. (4.1.2.2). Any small cocomplete category is a poset. ⌟

Proof: [MacLane]P114. □

Def. (4.1.2.3) [Compact Objects]. For a regular cardinal κ. Let $\mathcal{C} \in \mathcal{C}\mathrm{at}$ be a category that admits small colimits, and J be a κ-filtered poset and a diagram $\{Y_\alpha\}$ indexed by J, then for $X \in \mathcal{C}$, there is a natural map

$$\varinjlim \mathrm{Hom}(X, Y_j) \to \mathrm{Hom}(X, \varinjlim Y_j).$$

X is called **κ-compact** if this is an isomorphism for any κ-filtered diagram J. X is called **small** if it is κ-compact for some small(4.1.2.1) regular cardinal κ. ⌟

Def. (4.1.2.4) [κ-Accessible Categories]. For a regular cardinal κ, a **κ-accessible category** is a locally small category(4.1.2.1) $n\,\mathcal{C}\mathrm{at}$ that satisfies:

- $\mathcal{C}$ admits all κ-filtered colimits.
- $\mathcal{C}$ is generated by a κ-small set S consisting of κ-compact objects of $\mathcal{C}$ under κ-filtered colimits.

$\mathcal{C}$ is called **accessible** if it is κ-accessible for some small regular cardinal κ. A **κ-accessible functor** is a functor $F : \mathcal{C} \to \mathcal{D}$ between κ-cocomplete categories that preserves κ-filtered colimits. And a functor is called a **accessible functor** if it is κ-accessible for some small regular cardinal κ. ⌟

Def. (4.1.2.5) [Locally Presentable Categories]. A **locally presentable category** is a category that is both cocomplete and accessible(4.1.2.4). ⌟

Prop. (4.1.2.6). Any locally presentable category is complete. ⌟

Proof:

□

Example (4.1.2.7) [Locally Presentable Categories].

- $\mathcal{S}\mathrm{et}$ is locally presentable.
- If $\mathcal{C}$ is a small category, then $\mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C})$ is locally presentable.
- For $R \in \mathcal{CR}\mathrm{ing}$, $\mathcal{M}\mathrm{od}_R$ and $\mathrm{Ch}(R)$ are locally presentable.
- If $T : \mathcal{C} \to \mathcal{C}$ is an accessible monad on a locally presentable category, then the category of T-algebras is locally presentable.
- Every Grothendieck topos is locally presentable.
- If $\mathcal{M}$ is a locally presentable symmetric monoidal category, then $\mathcal{C}\mathrm{at}_{\mathcal{M}}$ is locally presentable.
- $\mathcal{T}\mathrm{op}$ is not locally presentable, but $\mathcal{CG}$ is locally presentable.

⌟

Proof: □

Cor. (4.1.2.8). $\mathcal{C}$at is locally presentable. ⌟

Prop. (4.1.2.9)[Adjoint Functor Theorem]. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor between locally presentable categories, then

- F is a left adjoint iff it preserves small colimits.
- F is a right adjoint iff it is accessible and preserves small limits.

⌟

Proof: □

Def. (4.1.2.10)[Accessible Reflective Localizations]. An **accessible reflective localization** is a reflective localization(4.1.1.62) $(L, R) : \mathcal{C} \rightleftarrows \mathcal{D}$ s.t. R is accessible(4.1.2.4). ⌟

Prop. (4.1.2.11)[Classifying Locally Presentable Categories]. A category is locally presentable iff it is equivalent to an accessible reflective localization(4.1.2.10) of $\mathcal{PSh}^{\mathrm{Set}}(\mathcal{A})$ for some small category A. ⌟

Proof: Cf.[Locally presentable and accessible categories]. □

3 Ends and Coends

Def. (4.1.3.1)[Dinatural Transformation]. Given categories $\mathcal{C}, \mathcal{D}$ and functor $P, Q : \mathcal{C}^{\mathrm{op}} \times \mathcal{C} \to \mathcal{D}$, then a **dinatural transformation** $\alpha : P \to Q$ is a family of arrows $\alpha_C : P(C, C) \to Q(C, C)$ where $C \in \mathcal{C}$ that for any arrow $C \to C' \in \mathcal{C}$, there is a commutative diagram

$$\begin{array}{ccccc} P(C', C) & \longrightarrow & P(C, C) & \xrightarrow{\alpha_C} & Q(C, C) \\ \downarrow & & & & \downarrow \\ P(C', C') & \xrightarrow{\alpha_{C'}} & Q(C', C') & \longrightarrow & Q(C, C') \end{array}$$

⌟

Def. (4.1.3.2)[Wedge and Cowedge]. Let $P : \mathcal{C}^{\mathrm{op}} \times \mathcal{C} \to \mathcal{D}$ be a functor, then a **wedge** for P is a binatural functor $\Delta_D \to P$, where D is an object of $\mathcal{C}$. Similarly a **cowedge** is a binatural functor $P \to \Delta_D$. ⌟

Def. (4.1.3.3)[End and Coend]. For a functor $P : \mathcal{C}^{\mathrm{op}} \times \mathcal{C} \to \mathcal{D}$, the wedges and cowedges of P form categories, and we define **end** of P is just a terminal wedge, denoted by $\int_C F(C, C)$, and the **coend** of P is the initial cowedge, denoted by $\int^C F(C, C)$.

Ends and coends are functorial w.r.t natural transformations. ⌟

Prop. (4.1.3.4)[Ends as Colimits]. There is a morphism

$$F \mapsto \overline{F} : \mathrm{Fun}(\mathcal{C}^{\mathrm{op}} \times \mathcal{C}, \mathcal{D}) \to \mathrm{Fun}(Tw(\mathcal{C}), \mathcal{D})(4.1.1.19)$$

where we maps $f : C \to C'$ to $F(C, C')$. Then it can be checked that

$$\int_C F(C, C) = \lim_{Tw(\mathcal{C})} \overline{F}, \quad \int^C F(C, C) = \mathrm{colim}_{TW(\mathcal{C})} \overline{F}.$$

⌟

Cor. (4.1.3.5). A functor that preserves (co)limits preserves (co)ends. ⌟

Cor. (4.1.3.6). For an object $D \in \mathcal{D}$, we have isomorphisms:

$$\mathrm{Hom}(\int^C F(C,C), D) \cong \int_C \mathrm{Hom}(F(C,C), D),$$
$$\mathrm{Hom}(D, \int_C F(C,C)) \cong \int_C \mathrm{Hom}(D, F(C,C)).$$

⌟

Prop. (4.1.3.7) [Fubini]. Cf.[Coend Calculus, P20]. ⌟

Prop. (4.1.3.8) [Natural Transformation as Ends]. Let $F, G : \mathcal{C} \to \mathcal{D}$ be functors, then the set of natural transformations is an coend.

$$\mathrm{Map}(F, G) \cong \int_C \mathrm{Hom}_{\mathcal{D}}(FC, GC)$$

⌟

Kan Extension

Cf.[All Concepts are Kan Extensions].

Def. (4.1.3.9)[Kan Extensions]. Given functors $F : \mathcal{C} \to \mathcal{E}$ and $K : \mathcal{C} \to \mathcal{D}$, a **left Kan extension** of F along K is a functor $Lan_K F : \mathcal{D} \to \mathcal{E}$ together with a natural transformation $\eta : F \to Lan_K F \circ K$ that for any other pair $(G : \mathcal{D} \to \mathcal{E}, \gamma : F \to G \circ K)$, γ factors uniquely through η.

Dually, a **right Kan extension** of F over K is equivalent to a left Kan extension of F^{op} over K^{op}. ⌟

Prop. (4.1.3.10) [(Co)Limits as Kan Extensions]. If $\mathcal{D}$ is the final category 1, then the left Kan extension is just the colimit of the diagram defined by F, and the right Kan extension is just the limit of the diagram defined by F. ⌟

Prop. (4.1.3.11) [Yoneda Lemma]. $h_X : Y \mapsto \mathrm{Hom}(Y, X)$ is a presheaf, and $\mathrm{Hom}(h_X, \mathcal{F}) \cong \mathcal{F}(X)$ for any presheaf $\mathcal{F}$.

So $X \to h_X$ is a fully faithful embedding よ $: \mathcal{C} \to \mathcal{PSh}^{\mathcal{S}\mathrm{et}}(\mathcal{C})$. In particular, if a $X \to Y$ induces isomorphism $\mathrm{Hom}(W, X) \to \mathrm{Hom}(W, Y)$ for every W, then $X \cong Y$.

So we can regard $\mathcal{C}$ as a fully faithful subcategory of $\mathcal{PSh}^{\mathcal{S}\mathrm{et}}(\mathcal{C})$. ⌟

Proof: The map $\mathrm{Hom}(h_X, \mathcal{F}) \to \mathcal{F}(X)$ maps a u to $u(X)(\mathrm{id}_X)$. And the inverse map is defined to be $x \in \mathcal{F}(X) \mapsto (s \in \mathrm{Hom}(Y, X) \mapsto s^*(x) \in \mathcal{F}(Y)) \in \mathrm{Hom}(h_X, \mathcal{F})$. □

Cor. (4.1.3.12). A **universal object** for a presheaf $\mathcal{F}$ is a pair (X, ζ) that $\zeta \in F(X)$ with the property that for any U and a $\sigma \in \mathcal{F}(U)$, there is a unique arrow $U \to X$ that $Ff(\zeta) = \sigma$.

In fact, a universal object is equivalent to an isomorphism $h_X \cong \mathcal{F}$. ⌟

Prop. (4.1.3.13)[Presheaves as Colimits of Presentable Presheaves]. For $\mathcal{C} \in \mathcal{C}\mathrm{at}$, any presheaf of sets on $\mathcal{C}$ is a colimit of presentable presheaves on $\mathcal{C}$. More precisely, there is an isomorphism

$$\mathcal{F} \cong \varinjlim_{h_X \to \mathcal{F}} h_X.$$

From this we see that any functor $\mathcal{PSh}^{\mathcal{S}\mathrm{et}}(\mathcal{C}) \to \mathcal{D}$ compatible with colimits is determined by its restriction on $\mathcal{C}$. ⌟

Proof: For any presheaf $\mathcal{G}$, there is a morphism $\mathrm{Hom}(\mathcal{F},\mathcal{G}) \to \mathrm{Hom}(\varinjlim_{h_X \to \mathcal{F}} h_X, \mathcal{G})$, i.e. a set of sections $f_s \in \mathcal{G}(X)$ for every $h_X \xrightarrow{s} \mathcal{F}$, that if $t \circ u = s$, then $u^*(f_t) = f_s$. Conversely, by Yoneda lemma, this just says that there is a morphism of presheaves $\mathcal{F} \to \mathcal{G} : F(X) \to G(X) : s \mapsto f_s$. □

Cor. (4.1.3.14) [Yoneda Extensions]. For any $\mathcal{C} \in \mathcal{C}\mathrm{at}$ and a cocomplete category $\mathcal{D}$, then any functor $Q : \mathcal{C} \to \mathcal{D}$ extends to a functor $|\cdot|_Q : \mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C}) \to \mathcal{D}$ s.t.

$$\begin{array}{ccc} \mathcal{D} & \xrightarrow{Q} & \mathcal{D} \\ \downarrow {\small よ} & \nearrow_{|\cdot|_Q} & \\ \mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C}) & & \end{array}$$

is commutative. Moreover, there is a functor

$$\mathrm{Sing}_Q : \mathcal{C} \to \mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C}) : C \mapsto (X \mapsto \mathrm{Hom}_{\mathcal{D}}(QX, C)).$$

And there is an adjunction

$$|\cdot|_Q : \mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C}) \rightleftarrows \mathcal{D} : \mathrm{Sing}_Q .$$

Moreover, this assignment $Q \mapsto (|\cdot|_Q, \mathrm{Sing}_Q)$ induces an equivalence of categories:

$$\mathrm{Func}(\mathcal{C},\mathcal{D}) \cong \mathrm{Adj}(\mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C}),\mathcal{D}).$$

⌟

Proof: Define $|\cdot|_Q$ by colimit as in(4.1.3.13), then**?** □

Cor. (4.1.3.15). Any contravariant functor $Q : \mathcal{C} \to \mathcal{S}\mathrm{et}$ that take colimits to limits is representable. ⌟

Proof: Use Sing_Q as in the last proof, Q is representable by $\mathrm{Sing}_Q(\mathrm{pt})$. □

Def. (4.1.3.16) [$\mathcal{I}$-Free Diagram]. For a cocomplete category $\mathcal{C}$ and a small category $\mathcal{I}$, let $\mathcal{I}^\delta$ be the subcategory of $\mathcal{I}$ that has the same objects but only the identity morphisms, then an $\mathcal{I}$-diagram in $\mathcal{C}$ is called **$\mathcal{I}$-free** iff it is a left Kan extension of some diagram $\mathcal{I}^\delta \to \mathcal{C}$. ⌟

4 n-Categories

Remark (4.1.4.1) [2-Categories]. For $n \in \mathbb{N}$, n-categories are defined as in(4.7.1.28). ⌟

Prop. (4.1.4.2) [$\mathcal{C}\mathrm{at}$]. There is a 2-category $\mathcal{C}\mathrm{at}$ consisting of small categories and functors and natural transformations. ⌟

Def. (4.1.4.3) [(2, 1)-Categories]. A $(2,1)$**-category** is a 2-category that all the 2-morphisms(corresponding to a 2-simplex) are isomorphisms. ⌟

Prop. (4.1.4.4) [Final Objects]. An object in a $(2,1)$-category is a final object(4.7.3.2) iff for any y there is a morphism $y \to x$, and any two morphisms $y \to x$ are isomorphic by a unique 2-morphism. ⌟

Lemma (4.1.4.5) [2-Commutative diagrams]. Let $\mathcal{C}$ be a 2-category, and $g: y \to z, f: x \to z$ are arrows in $\mathcal{C}$, then the diagrams in $\mathcal{C}$:

$$\begin{array}{ccc} w & \xrightarrow{a} & x \\ \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle f} \\ y & \xrightarrow{g} & z \end{array}$$

together with a 2-morphism from gb to fa, naturally form a 2-category. A diagrams with invertible 2-morphisms are called **2-commutative digram** in $\mathcal{C}$. ⌟

Def. (4.1.4.6) [2-Fibered Products]. Let $\mathcal{C}$ be a 2-category, and $g: y \to z, f: x \to z$ are arrows in $\mathcal{C}$, a **2-fibered product** of f, g is a final object in the $(2,1)$-category of 2-commutative diagrams as defined in(4.1.4.5), and it is denoted by $x \times_z y$. ⌟

5 Monoidal Categories

Main references are [Tensor Categories, Etingof], [Lur09].

Def. (4.1.5.1) [Monoidal Categories]. A **monoidal category** is a category $\mathcal{C}$ with a functor $\otimes: \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ and a unit object 1 together with isomorphisms

$$\eta_{A,B,C}: (A \otimes B) \otimes C \to A \otimes (B \otimes C), \quad \alpha_A: A \otimes \mathbb{1} \to A, \quad \beta_A: \mathbb{1} \otimes A \to A$$

s.t.

- $\eta_{A,B,C}, \alpha_A, \beta_B$ are functorial in each coordinate.
- (MacLane Pentagon)The following diagram is commutative:

$$\begin{array}{ccccc} & & ((A \otimes B) \otimes C) \otimes D & & \\ & \swarrow{\scriptstyle \eta_{A,B,C} \otimes \mathrm{id}_D} & & \searrow{\scriptstyle \eta_{A\otimes B,C,D}} & \\ (A \otimes (B \otimes C)) \otimes D & & & & (A \otimes B) \otimes (C \otimes D) \\ \downarrow{\scriptstyle \eta_{A,B\otimes C,D}} & & & & \downarrow{\scriptstyle \eta_{A,B,C\otimes D}} \\ A \otimes ((B \otimes C) \otimes D) & & \xrightarrow{\mathrm{id}_A \otimes \eta_{B,C,D}} & & A \otimes (B \otimes (C \otimes D)) \end{array}$$

- The following diagram is commutative:

$$\begin{array}{ccc} (A \otimes \mathbb{1}) \otimes B & \xrightarrow{\eta_{A,\mathbb{1},B}} & A \otimes (\mathbb{1} \otimes B) \\ & \searrow{\scriptstyle \alpha_A \otimes \mathrm{id}_B} \quad \swarrow{\scriptstyle \mathrm{id}_A \otimes \beta_B} & \\ & A \otimes B & \end{array}$$

⌟

Def. (4.1.5.2) [Dual and Opposed Category]. Let $\mathcal{C}$ be a monoidal category, then the **opposed category** $\mathcal{C}^{opp}$ is the same category as $\mathcal{C}$ with the tensoring switched, which is also a monoidal category.

The dual category $\mathcal{C}^{\mathrm{op}}$ with the same tensoring is also a monoidal category. ⌟

Def. (4.1.5.3) [Strict Monoidal Categories]. A **strict monoidal category** is a monoidal category that the isomorphisms above(4.1.5.1) are all identities. ⌟

Prop. (4.1.5.4) [Mac Lane Coherence]. In a monoidal category, any two morphisms between two bracketings of a product $X_1 \otimes \ldots X_n$ constructed using the isomorphisms $\eta_{A,B,C}$ are equal. Also if some X_i are 1, then we can also use α_A and β_A. ⌟

Prop. (4.1.5.5) [Cartesian Monoidal Categories]. For a category with a final object and finite products, the product makes $\mathcal{C}$ a symmetric monoidal category, called the **Cartesian monoidal structure**. ⌟

Prop. (4.1.5.6). For any category $\mathcal{C}$, the category $[\mathcal{C},\mathcal{C}]$ of endofunctors has a natural monoidal structure. ⌟

Def. (4.1.5.7) [Closedness]. A monoidal category $(\mathcal{C},\otimes)$ is called **left-closed** if for every $A\in\mathcal{C}$, the functor $N\mapsto A\otimes N$ has a right adjoint $Y\mapsto {}^AY$(or denoted by $\mathcal{H}om(A,Y)$ when $\mathcal{C}$ is symmetric). Dually it is called **right-closed** if $\mathcal{C}^{opp}$ is left-closed. It is called **closed** if it is both left-closed and right-closed.

For a Cartesian monoidal category $\mathcal{C}$, $\mathcal{C}$ is called **Cartesian-closed** if it is closed for the Cartesian monoidal structure. ⌟

Prop. (4.1.5.8). $\mathcal{C}at$ is Cartesian closed, and for any $\mathcal{A},\mathcal{B},\mathcal{C}\in\mathcal{C}at$, there is an equivalence of categories

$$\mathrm{Func}(\mathcal{A},\mathrm{Func}(\mathcal{B},\mathcal{C}))\cong\mathrm{Func}(\mathcal{A}\times\mathcal{B},\mathcal{C}).$$

⌟

Proof: □

Def. (4.1.5.9) [Reflexive Objects]. Let $(\mathcal{C},\otimes)$ be a symmetric monoidal category that is closed, then we denote $\mathcal{H}om(Y,1)$ by $Y^\vee$, then there is a natural map $Y\to(Y^\vee)^\vee$. If such a map is reflexive, then Y is called a **reflexive object**. ⌟

Prop. (4.1.5.10). If $\mathcal{C}$ is closed, then

$$^{\varinjlim A_i}B\cong\varprojlim({}^{A_i}B)\quad {}^A(\varprojlim B_i)\cong\varprojlim({}^AB_i)$$

⌟

Proof: Because $\mathcal{C}$ is closed, left and right tensor $A\otimes-$ and $-\otimes A$ are both left adjoints thus commutes with colimits. Now $B\mapsto {}^AB$ is a right adjoint, thus it commutes with limits. And for any $C\in\mathcal{C}$,

$$\begin{aligned}\mathrm{Hom}(C,{}^{\varinjlim A_i}B)&\cong\mathrm{Hom}(C\otimes(\varinjlim A_i),B)\cong\mathrm{Hom}(\varinjlim C\otimes A_i,B)\\&\cong\varprojlim\mathrm{Hom}(C\otimes A_i,B)\cong\varprojlim\mathrm{Hom}(C,{}^{A_i}B)\cong\mathrm{Hom}(C,\varprojlim({}^{A_i}B))\end{aligned}$$

so $^{\varinjlim A_i}B\cong\varprojlim({}^{A_i}B)$ by Yoneda lemma. □

Def. (4.1.5.11) [Monoidal Functor]. Let $(\mathcal{C},\otimes),(\mathcal{D},\otimes)$ be monoidal categories, then a **right-lax monoidal functor** from $\mathcal{C}$ to $\mathcal{D}$ is a functor G together with morphisms $\gamma_{A,B}:G(A)\otimes G(B)\to G(A\otimes B)$ for any $A,B\in\mathcal{C}$ and a morphism $e:\mathbb{1}_{\mathcal{D}}\to G(\mathbb{1}_{\mathcal{C}})$ s.t.

- $\gamma_{A,B}$ is functorial in each coordinate.

- (Hexagon Diagram)The following diagram is commutative:

$$\begin{array}{ccc}
(G(A)\otimes G(B))\otimes G(C) & \xrightarrow{\eta_{G(A),G(B),G(C)}} & G(A)\otimes (G(B)\otimes G(C)) \\
\downarrow \gamma_{A,B} & & \downarrow \gamma_{B,C} \\
G(A\otimes B)\otimes G(C) & & G(A)\otimes G(B\otimes C) \\
\downarrow \gamma_{A\otimes B,C} & & \downarrow \gamma_{A,B\otimes C} \\
G((A\otimes B)\otimes C) & \xrightarrow{G(\eta_{A,B,C})} & G(A\otimes (B\otimes C))
\end{array}$$

- The following diagrams are commutative:

$$\begin{array}{ccccc}
G(A)\otimes \mathbb{1}_{\mathcal{D}} & \xrightarrow{\mathrm{id}_{G(A)}\otimes e} & G(A)\otimes G(\mathrm{id}_{\mathcal{C}}) & \xrightarrow{\gamma_{A,\mathbb{1}_{\mathcal{C}}}} & G(A\otimes \mathbb{1}_{\mathcal{C}}) \\
 & \searrow^{\alpha_{G(A)}} & & \swarrow_{G(\alpha_A)} & \\
 & & G(A) & &
\end{array}$$

$$\begin{array}{ccccc}
\mathbb{1}_{\mathcal{D}}\otimes G(B) & \xrightarrow{e\otimes \mathrm{id}_{G(B)}} & G(\mathrm{id}_{\mathcal{C}})\otimes G(B) & \xrightarrow{\gamma_{\mathbb{1}_{\mathcal{C}},B}} & G(B\otimes \mathbb{1}_{\mathcal{C}}) \\
 & \searrow^{\alpha_{G(B)}} & & \swarrow_{G(\beta_B)} & \\
 & & G(B) & &
\end{array}$$

Moreover, it is called a **monoidal functor** if $\gamma_{A,B}$ and e are all isomorphisms.

A **monoidal natural transformation** between right-lax monoidal functors is a natural transformation that commutes with the maps $\gamma_{A,B}$ and e. ⌟

Def. (4.1.5.12) [Equivalence of Monoidal Categories]. An equivalence of monoidal categories is a map that is an equivalence of categories as well as a monoidal functor. ⌟

Prop. (4.1.5.13) [Mac Lane Strictness]. Any monoidal category is equivalent to a strict monoidal category. ⌟

Proof: □

Prop. (4.1.5.14) [Examples]. For a monoidal category $(\mathcal{C},\otimes)$, the functor $X\mapsto \mathrm{Hom}(\mathbb{1},X)$ is a right-lax monoidal functor from $\mathcal{C}\to \mathcal{S}\mathrm{et}$(4.1.5.5).

The morphism $\pi_0 : A\mapsto \pi_0(A)$ is a monoidal functor from the category of topological spaces $\mathcal{T}\mathrm{op}$ to the category $\mathcal{S}\mathrm{et}$ because it commutes with products. ⌟

Proof: □

Symmetric Monoidal Categories

Def. (4.1.5.15) [Symmetric Monoidal Category]. A **symmetric monoidal category** is a monoidal category $(\mathcal{C},\otimes)$ together with a natural transformation ψ between $\otimes$ and $\otimes\circ\iota : \mathcal{C}\times\mathcal{C}\to\mathcal{C}$ that $\psi^2 = \mathrm{id}$ and the following commutative hexagon diagram is commutative:

A **symmetric monoidal functor** between symmetric monoidal categories are required to commutes with the braiding?. ⌟

Rigid Monoidal Categories

Def. (4.1.5.16) [Duals]. Let $\mathcal{C}$ be a monoidal category and $V \in \mathcal{C}$, a **left dual** of V is an element V^* together with maps

$$\mathrm{ev}_V : V^* \otimes V \to 1, \quad coev_V : 1 \mapsto V \otimes V^*$$

that satisfies

$$V \to V \otimes V^* \otimes V \to V, \quad V^* \to V^* \otimes V \otimes V^* \to V^*$$

are identities.

Similarly we can define right dual. if Y is a left/right dual to X, then X is right/left dual to Y. ⌟

Def. (4.1.5.17) [Dual Morphisms]. Let $f; X \to Y$ be a morphism and X^*, Y^* the left duals of X and Y, then there is a natural **left dual map**: $f^* : Y^* \to X^*$ given by

$$Y^* \to Y^* \otimes X \otimes X^* \to Y^* \otimes Y \otimes X^* \to X^*.$$

⌟

Prop. (4.1.5.18) [Monoidal Functor Preserves Duals]. Let $F : \mathcal{C} \to \mathcal{D}$ be a monoidal functor(4.1.5.11) between monoidal categories, $X \in \mathcal{C}$ is an object with left dual X^*. Then $F(X^*)$ is a left dual of $F(X)$ with evaluation and coevaluation maps

$$\mathrm{ev}_{F(X)} : F(X^*) \otimes F(X) \to F(X^* \otimes X) \to F(1_{\mathcal{C}}) \to 1_{\mathcal{D}},$$

$$coev_{F(X)} : 1_{\mathcal{D}} \to F(1_{\mathcal{C}}) \to F(X \otimes X^*) \to F(X) \otimes F(X^*).$$

and similarly for right duals. ⌟

Prop. (4.1.5.19) [Adjointness]. Let $\mathcal{C}$ be a monoidal category and $V \in \mathcal{C}$ with left dual V^*, then there are natural adjunction maps

$$\mathrm{Hom}(U \otimes V, W) \cong \mathrm{Hom}(U, W \otimes V^*), \quad \mathrm{Hom}(V^* \otimes U, W) \cong \mathrm{Hom}(U, V \otimes W).$$

⌟

Proof: The first adjunction map is given by $f \mapsto (f \otimes \mathrm{id}_{V^*}) \circ (\mathrm{id}_U \otimes coev_V)$, and the inverse given by $g \mapsto (W \otimes ev_V) \circ (g \otimes \mathrm{id}_V)$. The verification and the second one: □

Cor. (4.1.5.20). In particular, we can use Yoneda lemma to show the left/right adjoints are unique if they exist. ⌟

Invertible Objects and Grothendieck Categories

Def. (4.1.5.21) [Invertible Objects]. An **invertible object** in a monoidal category is a rigid object L that the evaluation maps and coevaluation maps are all isomorphisms.? ⌟

6 Tensor Categories

Notation (4.1.6.1).
- Let $k \in \texttt{Field}$.

⌟

Def. (4.1.6.2)[Tensor Categories]. A **tensor category** over a field k is an Artinian Abelian category over k together with a strict monoidal structure that is bilinear and satisfies $\mathrm{End}(\mathbb{1}) = k$.

A **tensor functor** is a functor between tensor categories that is additive and monoidal. ⌟

Prop. (4.1.6.3) [End(𝟙)]. If $\mathcal{C}$ is a rigid tensor category, then $\mathrm{End}(\mathbb{1})$ is a ring that acts on objects $X \in \mathcal{C}$ via $X \cong \mathbb{1} \otimes X$. The action of $\mathrm{End}(\mathbb{1})$ commutes with $\mathrm{End}(X)$, in particular, $\mathrm{End}(\mathbb{1})$ is commutative and $\mathcal{C}$ is $\mathrm{End}(\mathbb{1})$-linear. ⌟

Rigid Tensor Categories

Def. (4.1.6.4)[Rigid Tensor Categories]. Let $\mathcal{C}$ be a monoidal category, an element $X \in \mathcal{C}$ is called **rigid object** if it has left and right duals. A **rigid tensor category** is a tensor category(4.2.1.2) s.t. every object is rigid. In particular, by(4.1.5.19), a rigid tensor category is closed. ⌟

Prop. (4.1.6.5). If $\mathcal{C}$ is a rigid tensor category, then the functor

Equivalence of $\mathcal{C}^{\mathrm{op}}$ and $\mathcal{C}^{opp}$.**?** ⌟

Cor. (4.1.6.6). Any natural transformation of monoidal functors between rigid tensor categories is an isomorphism. ⌟

Proof: Cf.[Milne, Tannakian Categories, P13].**?** □

Prop. (4.1.6.7) [Trace and Rank]. Let $\mathcal{C}$ be a symmetric rigid tensor category, we can define a trace morphism

$$\mathrm{tr}_X : \mathrm{End}(X) \to \mathrm{End}(\mathbb{1}) : f \mapsto 1 \to X \otimes X^* \xrightarrow{f \otimes \mathrm{id}} X \otimes X^* \to X^* \otimes X \to 1$$

And the **dimension** of X is defined to be $\mathrm{tr}_X(\mathrm{id}_X) \in \mathrm{End}(1)$. ⌟

Prop. (4.1.6.8)[Abelian Rigid Tensor Categories Exact]. If $\mathcal{C}$ is an Abelian rigid tensor category, then $\otimes$ commutes with inverse limits and direct limits in each variable. ⌟

Proof: It commutes with direct limits because it is left adjoint to the Hom functor, and it commutes with inverse limits by considering the opposite category(4.2.1.5). □

Prop. (4.1.6.9). $\dim(X \otimes Y) = \dim X \cdot \dim Y$. If there is an exact sequence $0 \to X \to Z \to Y \to 0$, then $\dim(Z) = \dim(X) + \dim(Y)$. ⌟

Prop. (4.1.6.10) [Decompositions]. Let $(\mathcal{C}, \otimes)$ be a rigid Abelian tensor category and if U is a subobject of 1, then $1 = U \oplus U^\perp$ where $U^\perp = \ker(1 \to U^\vee)$. Consequently, 1 is a simple object iff $\mathrm{End}(1)$ is a field. And any rigid tensor category can be decomposed as rigid Abelian tensor categories $\mathcal{C}_I$ with $\mathrm{End}(1_i)$ being fields. ⌟

Proof: Let $V = \mathrm{Coker}(U \to 1)$, by tensoring $0 \to U \to 1 \to V \to 0$ with $U \hookrightarrow 1$, we get exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U & \longrightarrow & 1 & \longrightarrow & V & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & \overset{0}{\nearrow} & \uparrow & & \\ 0 & \longrightarrow & U\otimes U & \longrightarrow & U & \longrightarrow & V\otimes U & \longrightarrow & 0 \end{array}$$

thus $V \otimes U = 0$ and $U \otimes U = U$ via $1 \otimes 1 \cong 1$.

For the rest, Cf.[Tannakian Categories, Milne, P14]. □

Def. (4.1.6.11) [Associative Algebra in a Symmetric Tensor Category]. ⌟

<u>**Tannakian Categories**</u>

Def. (4.1.6.12) [Fiber Functor]. Let $\mathcal{C}$ be a k-linear tensor category, then a **fiber functor** on $\mathcal{C}$ with values in a k-algebra R is a k-linear exact faithful tensor functor $\eta : \mathcal{C} \to \mathcal{M}\mathrm{od}_R$ that takes values in the subcategory $\mathbf{Proj}_R$. ⌟

Def. (4.1.6.13) [Tannakian Category]. A **Tannakian category** is a symmetric rigid tensor category(4.2.1.4) $\mathcal{C}$ that $\mathrm{End}(\mathbb{1}) = k$ together with a fiber functor(4.2.1.12) with values in $R \in \mathcal{CR}\mathrm{ing}_k$. ⌟

Def. (4.1.6.14) [Neutral Tannakian Categories]. A **neutral Tannakian category** is a Tannakian category that the fiber functor is valued in k. By(18.5.2.9), such a category is equivalent to $\mathrm{Rep}_k(G)$ for some affine group scheme G, and such G is uniquely defined up to inner automorphisms.

In particular, a Tannakian category can be thought of as an abstract version of the category of representations of an affine group scheme that has no distinguished "forgetful"functor, just as a vector space is an abstract version of k^n that has no distinguished basis. ⌟

7 Enriched Category

Def. (4.1.7.1) [Enriched Categories]. Given a monoidal category $(\mathcal{C}, \otimes)$, an **enriched category** $\mathcal{D}$ over $\mathcal{C}$ consists of the following data:

- a collection of objects.
- For objects $X, Y \in \mathcal{D}$, a mapping object $\mathrm{Map}_{\mathcal{D}}(X, Y) \subset \mathcal{C}$.
- For objects $X, Y, Z \in \mathcal{D}$, a composite map $\mathrm{Map}_{\mathcal{D}}(X, Y) \otimes_{\mathcal{C}} \mathrm{Map}_{\mathcal{D}}(Y, Z) \to \mathrm{Map}_{\mathcal{D}}(X, Z)$ that is associative.
- For every $X \in D$, a morphism $1 \mapsto \mathrm{Map}_{\mathcal{D}}(X, X)$ that satisfies the commutative diagrams of the identity morphism.

⌟

Def. (4.1.7.2) [Category of Enriched Categories]. We can naturally define morphisms and natural transformations of categories enriched over a monoidal category $\mathcal{C}$. The resulting category is denoted by $\mathcal{C}\mathrm{at}_{\mathcal{C}}$. ⌟

Prop. (4.1.7.3) [Completeness and Cocompleteness]. Let $\mathcal{C}$ be a complete and cocomplete symmetric monoidal closed category, then $\mathcal{C}\mathrm{at}_{\mathcal{C}}$ is also complete and cocomplete. ⌟

Proof: Cf.[H. Wolff. V-cat and V-graph].? □

Prop. (4.1.7.4) [Transfer of Enriched Structure]. Given a right-lax monoidal functor between monoidal categories $F : \mathcal{C} \to \mathcal{C}'$ and a category $\mathcal{D}$ enriched over $\mathcal{C}$, we may obtain a category $F(\mathcal{D})$ enriched over $\mathcal{C}'$ by asserting $\mathrm{Map}_{F(\mathcal{D})}(X, Y) = F(\mathrm{Map}(X, Y))$. It is an enriched category just by the definition of right-lax monoidal functors. ⌟

Prop. (4.1.7.5) [Underlying Category]. For a category enriched $\mathcal{D}$ over $\mathcal{C}$, by(4.1.5.14), we can transfer the structure via $\mathcal{C} \to \mathcal{S}\mathrm{et} : X \mapsto \mathrm{Hom}(1, X)$, and the resulting category is called the underlying category of $\mathcal{D}$. ⌟

Prop. (4.1.7.6).

- A category enriched in $\mathcal{S}\mathrm{et}$ is just a usual category.
- A right-closed monoidal category is enriched over itself if we define $\mathrm{Map}(X, Y) = Y^X$.(Check).

⌟

Def. (4.1.7.7) [Tensored Category]. Let $\mathcal{C}$ be a right-closed monoidal category and $\mathcal{D}$ a category enriched over $\mathcal{C}$, then $\mathcal{D}$ is called **tensored over** $\mathcal{C}$ if for any $C \in \mathcal{C}$ and $X \in \mathcal{D}$, there is an isomorphism of functors

$$\eta : \mathrm{Map}_{\mathcal{D}}(X, -)^C \cong \mathrm{Map}_{\mathcal{D}}(X \otimes C, -).$$

for some element $X \otimes C \in \mathcal{D}$.

In particular, this implies $\mathrm{Hom}_{\mathcal{C}}(C, \mathrm{Map}(X, Y)) \cong \mathrm{Hom}_{\mathcal{D}}(X \otimes C, Y)$, thus $X \otimes C$ is determined up to a unique isomorphism, and the map $(X, C) \mapsto X \otimes C$ defines a functor $\mathcal{D} \times \mathcal{C} \to \mathcal{D}$ that there are natural morphisms

$$X \otimes (C \otimes D) \cong (X \otimes C) \otimes D.$$

Dually, if $\mathcal{C}$ is left-closed and there is an object ${}^C X$ that there is an isomorphism of functors

$${}^C\,\mathrm{Map}(-, X) \cong \mathrm{Map}(-, {}^C X)$$

then $\mathcal{D}$ is called **cotensored** over $\mathcal{C}$. ⌟

Proof:

□

Prop. (4.1.7.8). If $\mathcal{C}$ is a right-closed monoidal category, then it is naturally tensored over itself, as defined in(4.2.2.6). ⌟

Lifting Property and Small Object Argument

Def. (4.1.7.9) [lifting Properties]. Let $\mathcal{C}$ be a category and $p : A \to B, q : X \to Y$ be morphisms, then p is said to have **left lifting property** w.r.t q and q is said to have **right lifting property** w.r.t p if given any diagram $\begin{array}{ccc} A & \longrightarrow & X \\ \downarrow{\scriptstyle p} & \nearrow & \downarrow{\scriptstyle q} \\ B & \longrightarrow & Y \end{array}$, there is a dotted arrow completing the diagram.

For a set A of morphisms of $\mathcal{C}$, let $l(A)$ denote the morphisms that have left lifting property w.r.t A and $r(A)$ the morphisms that have right lifting property w.r.t A. ⌟

Def. (4.1.7.10) [Weakly Saturated Class]. Let $\mathcal{C}$ be a category with all small colimits, then a class of morphisms of $\mathcal{C}$ is called **weakly saturated** if it satisfies:

- Closed under pushout.

- Closed under transfinite composition: Let α be an ordinal and $\{D_\beta\}_{\beta<\alpha}$ be a system of objects in $\mathcal{C}_{C/}$ indexed by α. For $\beta<\alpha$, let $D_{<\beta}$ be the colimit of system $\{D_\gamma\}_{\gamma<\beta}$ in $\mathcal{C}_{C/}$, then if each $D_{<\beta}\to D_\beta$ is in S, then $C\to D_{<\alpha}$ is in S.
- Closed under Retraction: In the category of morphisms of $\mathcal{C}$, if there is a morphism $F: f\to g, G: g\to f$ that $G\circ F=\mathrm{id}$, and $g\in S$, then $f\in S$.

⌟

Cor. (4.1.7.11). The second condition implies all isomorphisms are in S, and S is closed under composition. ⌟

Prop. (4.1.7.12) [Lifting and Retraction]. For a diagram $\begin{array}{ccc} X & = & X \\ \downarrow i & \nearrow s & \downarrow p \\ Z & \xrightarrow{f} & Y \end{array}$ represents p as a retraction of u, as the diagram $\begin{array}{ccccc} X & \xrightarrow{i} & Z & \xrightarrow{s} & X \\ \downarrow p & & \downarrow f & & \downarrow p \\ Y & = & Y & = & Y \end{array}$ shows.

Dually a diagram $\begin{array}{ccc} X & \xrightarrow{i} & Y \\ \downarrow q & \nearrow s & \downarrow f \\ Z & = & Z \end{array}$ represents q as a retraction of i. ⌟

Prop. (4.1.7.13) [Small Object Argument]. Let $\mathcal{C}$ be a presentable category and $A_0=\{\varphi_i: C_i\to D_i\}$ be a small collection of morphisms in $\mathcal{C}$, then there is a morphism $T:\mathcal{C}^{[1]}\to\mathcal{C}^{[2]}$ taking morphisms $f: X\to Z$ in $\mathcal{C}$ to the diagram

$$\begin{array}{ccccc} & & Y & & \\ & \nearrow f' & & \searrow f'' & \\ X & & \xrightarrow{\quad f \quad} & & Z \end{array}$$

That f' belongs to the weakly saturated class generated by A_0 and $f''\in r(A_0)$.

Moreover, if κ is a regular cardinal that each C_i, D_i is κ-compact, then T commutes with κ-filtered colimits. ⌟

Proof: Cf.[HTT, P788]. □

Lemma (4.1.7.14). $l(A)$ is weakly saturated for any set of morphisms A(Clear). ⌟

Cor. (4.1.7.15) [Generated Weakly Saturated Class]. For any presentable category $\mathcal{C}$ and A a set of morphisms in $\mathcal{C}$, $l(r(A))$ is the smallest weakly saturated class of morphisms containing A. ⌟

Proof: One direction of inclusion is by(4.2.2.14), for the other, if $f: X\to Z\in l(r(A))$, then there is a factorization $X\xrightarrow{f'}Y\xrightarrow{f''}Z$, where $f'\in\overline{A}$ and $f''\in r(A)$, thus $f\in l(f'')$, thus f is retraction of f':

$$\begin{array}{ccc} X & \xrightarrow{f'} & Y \\ \downarrow f & \overset{g}{\nearrow} & \downarrow f'' \\ Z & \longrightarrow & Z \end{array} \Rightarrow \begin{array}{ccccc} X & \longrightarrow & X & \longrightarrow & X \\ \downarrow f & & \downarrow f' & & \downarrow f \\ Z & \xrightarrow{g} & Y & \xrightarrow{f''} & Z \end{array}$$

Thus $f\in\overline{A}$. □

Trees

Cf.[HTT, Appendix]

8 Fibered Categories

Notation (4.1.8.1).
- Let $\mathcal{C} \in \mathcal{C}\mathrm{at}$.

⌟

Categories of Categories

Def. (4.1.8.2) [2-Category of Categories over Categories]. There is a 2-category of categories over $\mathcal{C}$, where the 1-morphisms are morphisms of categories over $\mathcal{C}$ and the 2-morphisms are base-preserving natural transformations.

Two categories over $\mathcal{C}$ are called **equivalent** if they are equivalent in this 2-category. ⌟

Prop. (4.1.8.3) [2-Fibered Products in the Categories of Categories]. 2-fibered products exists in the categories of categories. ⌟

Proof: Let $F : \mathcal{A} \to \mathcal{C}, G : \mathcal{B} \to \mathcal{C}$ be functors, then we can define a category $\mathcal{A} \times_{\mathcal{C}} \mathcal{B}$ as follows:
- Objects are the triples (A, B, f) where $A \in \mathcal{A}, B \in \mathcal{B}$ and $f : F(A) \to G(B)$ is an isomorphism in $\mathcal{C}$.
- Morphisms from (A, B, f) to (A', B', f') are pairs (a, b) where $a : A \to A', b : B \to B'$ s.t. the diagram

$$\begin{array}{ccc} F(A) & \xrightarrow{f} & G(B) \\ \downarrow{\scriptstyle F(a)} & & \downarrow{\scriptstyle G(b)} \\ F(A') & \xrightarrow{f'} & G(B') \end{array}$$

is commutative.

$\mathcal{A} \times_{\mathcal{C}} \mathcal{B}$ is a category both over $\mathcal{A}$ and over $\mathcal{B}$, and it fits into a 2-fiber products diagram

$$\begin{array}{ccc} \mathcal{A} \times_{\mathcal{C}} \mathcal{B} & \longrightarrow & \mathcal{B} \\ \downarrow & & \downarrow \\ \mathcal{A} & \longrightarrow & \mathcal{C} \end{array}$$

where the invertible 2-morphism is given by $\psi_{(A,B,f)} = f : F(A) \to G(B)$.

The verification that this defines a final object in the 2-category of 2-commutative diagrams is in[Sta]02X9. □

Cor. (4.1.8.4). The 2-fibered product $\mathcal{A} \times_{\mathcal{C}} \mathcal{B}$ is a groupoid iff $\mathcal{A}, \mathcal{B}$ are all groupoids. ⌟

Prop. (4.1.8.5). Let $\mathcal{A} \to \mathcal{C}, \mathcal{B} \to \mathcal{C}, \mathcal{C} \to \mathcal{D}$ be functors between categories, then there is a 2-fiber product diagram

$$\begin{array}{ccc} \mathcal{A} \times_{\mathcal{C}} \mathcal{B} & \longrightarrow & \mathcal{A} \times_{\mathcal{D}} \mathcal{B} \\ \downarrow & & \downarrow \\ \mathcal{C} & \xrightarrow{\Delta_{\mathcal{C}/\mathcal{D}}} & \mathcal{C} \times_{\mathcal{D}} \mathcal{C} \end{array}$$

⌟

Proof: □

Prop. (4.1.8.6) [2-Fibered Products of Categories]. The $(2,1)$-category of categories over $\mathcal{C}$ has 2-fiber products(4.1.4.6). More explicitly, suppose $F : \mathcal{X} \to \mathcal{S}, \mathcal{Y} \to \mathcal{S}$ be morphisms of categories over $\mathcal{C}$, $\mathcal{X} \times_{\mathcal{S}} \mathcal{Y}$ is given as follows:

- Objects of $\mathcal{X} \times_{\mathcal{C}} \mathcal{Y}$ are quadruples (U, x, y, f), where $U \in \mathcal{C}, x \in \mathcal{X}_U, y \in \mathcal{Y}_U$, and $f : F(x) \to G(y)$ is an isomorphism in $\mathcal{S}_U$.
- A morphism $(U, x, y, f) \to (U', x', y', f')$ is given by a pair (a, b), where $a : x \to x'$ is a morphism in $\mathcal{X}$ and $y \to y'$ is a morphism in $\mathcal{Y}$ that
  - a, b induce the same morphism $U \to U'$.
  - the diagram

$$\begin{array}{ccc} F(x) & \xrightarrow{f} & G(y) \\ \downarrow{\scriptstyle F(a)} & & \downarrow{\scriptstyle G(b)} \\ F(x') & \xrightarrow{f'} & G(y') \end{array}$$

    is an isomorphism.

$\mathcal{X} \times_{\mathcal{S}} \mathcal{Y}$ is endowed with morphisms to $\mathcal{X}$ and $\mathcal{Y}$ over $\mathcal{C}$ that the invertible 2-morphism giving the 2-commutativity is $\psi_{(U,x,y,f)} : F(x) \to G(y)$.

The verification of the universal properties are similar to that of(4.2.3.2). ⌟

Cor. (4.1.8.7). There is an equivalence of fibre categories:

$$(\mathcal{X} \times_{\mathcal{S}} \mathcal{Y})_U \cong \mathcal{X}_U \times_{\mathcal{S}_U} \mathcal{Y}_U.$$

⌟

Fibered Categories

Def. (4.1.8.8) [(Co)Cartesian Arrows]. Let $p : \mathcal{F} \to \mathcal{C}$ be a morphism, then a **Cartesian arrow** is an arrow $\varphi : C' \to C$ in $\mathcal{F}$ that for any object $C'' \in \mathcal{F}$ the map

$$\mathrm{Hom}(C'', C') \to \mathrm{Hom}(C'', C) \times_{\mathrm{Hom}(p(C''), p(C))} \mathrm{Hom}(p(C''), p(C'))$$

is a bijection. A **coCartesian arrow** is an arrow that corresponds to a Cartesian diagram in $\mathcal{F}^{op} \to \mathcal{C}^{\mathrm{op}}$. ⌟

Prop. (4.1.8.9).

- If f is Cartesian, then $f \circ g$ is Cartesian iff g is Cartesian.
- An arrow in $\mathcal{F}$ whose image is an isomorphism is Cartesian iff it is itself an isomorphism.

⌟

Proof: Easy. □

Def. (4.1.8.10)[Quasi-Fibrantion]. A functor $F : \mathcal{C} \to \mathcal{D}$ is called a **quasi-fibration** if for any $X \in \mathcal{C}$ and an isomorphism $f : F(X) \cong Y$, there is an isomorphism $\overline{f} : X \to \overline{Y}$ mapping to f. ⌟

Def. (4.1.8.11) [2-Category of Fibered Categories]. A **fibered category** over $\mathcal{C}$ is a category over $\mathcal{C}$ $p : \mathcal{F} \to \mathcal{C}$ that for any $\eta \in \mathcal{F}$ and an arrow $f : U \to p(\eta)$, there is a Cartesian arrow $\xi \to \eta$ in $\mathcal{F}$ lifting f. A **cofibered category** over $\mathcal{C}$ is a category $p : \mathcal{F} \to \mathcal{C}$ that the dual category $p^{\mathrm{op}} : \mathcal{F}^{\mathrm{op}} \to \mathcal{C}^{\mathrm{op}}$ is a fibered category.

A morphism of fibered categories over $\mathcal{C}$ is a morphism of categories over $\mathcal{C}$ that maps Cartesian morphisms to Cartesian morphisms. A 2-morphism of fibered categories is the same as a 2-morphism of categories over categories.

The 2-category of categories fibered over $\mathcal{C}$ is denoted by $\mathfrak{FibCat}/\mathcal{C}$ or $\mathfrak{FibCat}(\mathcal{C})$. ⌟

Def. (4.1.8.12) [Split Fibered Categories]. A **split fibered category** is a fibered category $\mathcal{F} \to \mathcal{C}$ that comes from a functor $\mathcal{C}^{\mathrm{op}} \to \mathfrak{Cat}$. ⌟

Def. (4.1.8.13) [Cleavage]. A **cleavage** of a fibered category $\pi : \mathcal{F} \to \mathcal{C}$ is a choice of Cartesian arrow f^* lifting f for any $f \in \mathcal{A}\mathrm{rr}(\mathcal{C})$. ⌟

Lemma (4.1.8.14). Let $F : \mathcal{F} \to \mathcal{G}$ be a morphism of fibered categories over $\mathcal{C}$ that $\mathcal{F}(U) \to \mathcal{G}(U)$ are fully faithful for any $U \in \mathcal{C}$, then F is fully faithful. ⌟

Proof: To show F is fully faithful, it suffices to show for objects X, Y lying over U, V, F induces a bijection of morphisms from x to y lying over a fixed $f : U \to V$. Choose a Cartesian morphism $f^*y \to y$ in $\mathcal{S}_1$ lying over f, then this induces a bijection between morphisms from x to y lying over f and $\mathrm{Hom}_{\mathcal{S}_{1,U}}(x, f^*y)$. Similarly, because F preserves Cartesian morphisms, we get a bijection between morphisms $F(x) \to F(y)$ lying over f and $\mathrm{Hom}_{\mathcal{S}_{2,U}}(F(x), F(f^*y))$. Then the desired bijection follows from the hypothesis. □

Prop. (4.1.8.15) [Equivalence of Fibered Categories]. Let $F : \mathcal{F} \to \mathcal{G}$ be a morphism of fibered categories. Then F is an equivalence iff the restriction $F_U : \mathcal{F}(U) \to \mathcal{G}(U)$ is an equivalence of categories for any object U of $\mathcal{C}$. ⌟

Proof: One direction is trivial, for the other, the proof is similar to the fact essentially surjective+fully faithful implies equivalence.

Because $F(U)$ are equivalences, for any object ξ of $\mathcal{G}$ over U, pick an object $G\xi$ in $\mathcal{F}(U)$ together with an isomorphism $\alpha_\xi : \xi \cong F(G\xi)$. And for any morphism $\xi \to \eta$, by(4.2.3.13), there is a unique arrow $G\varphi : G\xi \to G\eta$ that $F(G\varphi) = \alpha_\eta \circ \varphi \circ \alpha_\xi^{-1}$.

Thus clearly there is a 2-isomorphism $\mathrm{id}_{\mathcal{G}} \cong F \circ G$. It remains to construct an 2-isomorphism $\mathrm{id}_{\mathcal{F}} \cong G \circ F$: For any object ξ' over U, since $F(U)$ is fully faithful, there is a unique isomorphism $\beta_{\xi'} : \xi' \cong G \circ F(\xi)$ in $\mathcal{F}(U)$ that $F\beta_{\xi'} = \alpha_{F\xi'}$. Then this is easily checked to be an 2-isomorphism $\beta : \mathrm{id}_{\mathcal{F}} \cong F \circ G$. □

Prop. (4.1.8.16) [2-Fiber Products of Fibered Categories]. 2-fiber products exists in the category of fibered categories, and it coincides with that defined in(4.2.3.5). ⌟

Proof: it suffices to show for fibered categories $\mathcal{X}, \mathcal{Y}$ over $\mathcal{C}$, $\mathcal{X} \times_{\mathcal{C}} \mathcal{Y}$ is also fibered over $\mathcal{C}$. Let (x, y, φ) be an object of $\mathcal{X} \times_{\mathcal{C}} \mathcal{Y}$ mapping to $U \in \mathcal{C}$ and $f : V \to U$ is a morphism in $\mathcal{C}$, choose Cartesian morphisms $a : f^*x \to x$, $b : f^*y \to y$ lying over f, then $F(a)$ and $G(b)$ are Cartesian. Since $\varphi : F(x) \to G(y)$ is an isomorphism, by the property of Cartesian morphisms, there exists a unique isomorphism $f^*\varphi : F(f^*x) \to G(f^*y) \in \mathcal{S}_V$ that $G(b) \circ f^*\varphi = \varphi \circ F(a)$. In other words, $(F(a), F(b)) : (V, f^*x, f^*y, f^*\varphi) \to (U, x, y, \varphi)$ is a morphism in $\mathcal{X} \times_{\mathcal{S}} \mathcal{Y}$.

The verification that this morphism is Cartesian is omitted**?**. □

Lemma (4.1.8.17). Let $\mathcal{S} \to \mathcal{C}$ be a fibered category that factors through $\mathcal{C}/U$ where $U \in \mathcal{C}$, then $\mathcal{S} \to \mathcal{C}/U$ is also a fibered category. ⌟

Proof: Cf.[[Sta]02XR]. □

Def. (4.1.8.18) [G-Equivariant Object]. Let $G : \mathcal{C}^{op} \to (Grp)$ be a group functor and $p_{\mathcal{F}} : \mathcal{F} \to \mathcal{C}$ a fibered category, and X an object of $\mathcal{C}$ with an action of G. A **G-equivariant object** of $\mathcal{F}(X)$ is an object ρ of $\mathcal{F}(X)$ that there is an action of $G \circ p_{\mathcal{F}}$ on ρ and for any object U and $\xi \in \mathcal{F}(U)$, the function $p_{\mathcal{F}} : \mathrm{Hom}_{\mathcal{F}}(\xi, \rho) \to \mathrm{Hom}_{\mathcal{C}}(U, X)$ is $G(U)$-equivariant.

The category $\mathcal{F}^G(X)$ of G-equivariant objects of $\mathcal{F}(X)$ consisting of $G \circ p_{\mathcal{F}}$-equivariant morphism of G-equivariant objects. ⌟

Prop. (4.1.8.19). Let π_2 is the projection $G \otimes X \to X$, ρ be an object of $\mathcal{F}(X)$, then a G-equivariant structure on ρ is the same as a Cartesian arrow $\beta : \pi_2^* \rho \to \rho$ that $p_{\mathcal{F}}\beta = \alpha$, and satisfies the desired commutative diagram corresponding to $(gh)x = g(h(x))$. And a morphism of G-equivariant objects just corresponds to a morphism of pairs (ρ, β). ⌟

Proof: Cf.[Vistoli, P68]. □

Def. (4.1.8.20) [Presheaf of Arrows]. Let $\mathcal{F}$ be a fibered category over $\mathcal{C}$, and $\xi, \eta \in \mathcal{F}(S)$, then we can define a quasi-functor $\mathcal{H}om_S(\xi, \eta) \to (\mathcal{C}/S)$, where

$$\mathcal{H}om_S(\xi, \eta)(U/S) = \{(\xi_1 \to \xi, \eta_1 \to \eta, \varphi)\}$$

where $\xi_1 \to \xi, \eta_1 \to \eta$ are Cartesian arrows over $U \to S$, and $\varphi : \xi_1 \to \eta_1 \in \mathcal{F}(U)$. The arrows in $\mathrm{Hom}_S(\xi, \eta)$ are uniquely defined by the property of Cartesian arrows. Then it is a quasi-functor, by(4.2.3.30).

Then it is equivalence to a presheaf $\underline{\mathrm{Hom}}_S(\xi, \eta)$, by(4.2.3.31). Equivalently, this presheaf can be defined by designating a choice of Cartesian arrows. ⌟

Prop. (4.1.8.21) [Splitting a Fibered Category]. Let $\mathcal{F} \to \mathcal{C}$ be a fibered category, then there exists a canonically defined split fibered category $\widetilde{\mathcal{F}} \to \mathcal{C}$ with a canonical equivalence of fibered categories $\widetilde{\mathcal{F}} \to \mathcal{F}$ over $\mathcal{C}$. ⌟

Proof: There is a functor $\mathcal{C}^{op} \to \mathcal{C}at : U \mapsto \mathrm{Hom}(h_U, \mathcal{F})$, with corresponds to a split fibered category $\widetilde{\mathcal{F}}$. There is an obvious morphism $\widetilde{\mathcal{F}} \to \mathcal{F}$, sending an object $\varphi : h_U \to \mathcal{F}$ to $\varphi(\mathrm{id}_U) \in \mathcal{F}(U)$. And for any $f : U \to V \in \mathcal{C}$ and a $\varphi : h_U \to \mathcal{F}$, we send $f^*\varphi \to \varphi \in \widetilde{\mathcal{F}}$ to $\varphi(f : V/U \to U/U) \in \mathcal{F}$, Then we get a canonical map of fibered categories $\widetilde{\mathcal{F}} \to \mathcal{F}$ over $\mathcal{C}$. It is an equivalence of categories by(4.2.3.14) and(4.2.3.33). □

Categories Fibered in Groupoids, Sets and Equivalence Relations

Def. (4.1.8.22) [Category Fibered in Groupoids]. A **category (co)fibered in groupoids/sets/equivalence relations** over $\mathcal{C}$ is a category $\mathcal{F}$ (co)fibered over $\mathcal{C}$ that $\mathcal{F}(U)$ is a groupoid/setoids/equivalence relations(4.1.1.14) for any $U \in \mathcal{C}$. Also we call a category fibered in equivalence relations over $\mathcal{C}$ a **quasi-functor**.

The 2-category of categories fibered in groupoids is denoted by $\mathcal{F}ib\mathcal{C}at^{\mathcal{G}rpd}/\mathcal{C}$. ⌟

Prop. (4.1.8.23) [Characterization of Category Fibered in Groupoids]. Let $\mathcal{F}$ be a category over $\mathcal{C}$, then $\mathcal{F}$ is fibered over groupoids over $\mathcal{C}$ iff

- Every morphism in $\mathcal{F}$ is Cartesian.

- Given any $\eta \in \mathcal{F}, U \in \mathcal{C}$ and a morphism $f : U \to p_{\mathcal{F}}(\eta)$, there is an arrow $\varphi : \xi \to \eta \in \mathcal{F}$ mapping to f.

And dually for cofibered categories. ⌟

Proof: If these two holds, then $\mathcal{F}$ is clearly fibered over $\mathcal{C}$, and for any arrow $f : \xi \to \eta$ in $\mathcal{F}(U)$, there is a morphism $g : \eta \to \xi$ that is right inverse to f, then clearly it is the inverse.

Conversely, if $\mathcal{F}$ is fibered over $\mathcal{C}$, it suffices to check1: for any arrow f, the image in $\mathcal{C}$ can be lifted to a Cartesian diagram in $\mathcal{F}$, and differs f by an isomorphism, thus f is also Cartesian by(4.2.3.8). □

Cor. (4.1.8.24). if $\mathcal{A}$ is a category fibered in groupoids over $\mathcal{B}$ and $\mathcal{B}$ is a category fibered in groupoids over $\mathcal{C}$, then $\mathcal{A}$ is a category fibered in groupoids over $\mathcal{C}$. ⌟

Prop. (4.1.8.25) [Associated Category Fibered in Groupoids]. Let $\mathcal{F} \to \mathcal{C}$ be a fibered category, then the **associated category fibered in groupoids** $\mathcal{F}_{cart}$ is the category obtained by deleting all the non-Cartesian arrows. Then $\mathcal{F}_{cart}$ is a category fibered in groupoids over $\mathcal{C}$. ⌟

Proof: Firstly $\mathcal{F}_{cart}$ is a category by(4.2.3.8), and it is a category fibered in groupoids by(4.2.3.22). □

Def. (4.1.8.26) [RIgid Fibered Categories]. A **rigid fibered category** is a fibered category whose associated category fibered groupoids is fibered in setoids. Equivalently, there are no isomorphisms above any id_U. ⌟

Prop. (4.1.8.27) [2-Fibered Products of Categories Fibered in Groupoids]. The 2-fibered products of categories fibered in groupoids over $\mathcal{C}$ is a category fibered in groupoids over $\mathcal{C}$. ⌟

Proof: The 2-fibered products exist by(4.2.3.15), and using (4.2.3.6), it is fibered in groupoids because the 2-fibered products of groupoids is a groupoid by(4.2.3.3). □

Prop. (4.1.8.28) [Characterization of Categories Fibered in Setoids]. Let $\mathcal{F}$ be a category over $\mathcal{C}$, then $\mathcal{F}$ is fibered in setoids over $\mathcal{C}$ iff for any object η of $\mathcal{F}$ and an arrow $f : U \to p_{\mathcal{F}}\eta \in \mathcal{C}$, there is a unique arrow $\xi \to \eta$ mapping to f. ⌟

Proof: Let $\mathcal{F}$ be a category fibered in sets, then pick a Cartesian arrow $\widetilde{f}$ over f, then any other lifting factors through this lifting by the property of Cartesian, then it is identity, because $\mathcal{F}(U)$ is a setoid.

Conversely, if the hypothesis holds, then clearly $\mathcal{F}(U)$ is a setoid, and the fibered category condition holds, because of the uniqueness. □

Cor. (4.1.8.29) [Presheaves and Categories Fibered in Setoids]. Let $\mathcal{C}$ be a category, then categories fibered in setoids over $\mathcal{C}$ are exactly those equivalent to a presheaf over $\mathcal{C}$. ⌟

Cor. (4.1.8.30). In particular, for any object $X \in \mathcal{C}$, the presheaf h_X determines a category fibered in sets, which is just the comma category $\mathcal{C}/X \to \mathcal{C}$. ⌟

Prop. (4.1.8.31) [Characterization of Quasi-Functors]. A category $\mathcal{F}$ over $\mathcal{C}$ is a quasi-functor iff:

- Given any object $\eta \in \mathcal{F}$ and an arrow $f : U \to p_{\mathcal{F}}\eta$, there is a lifting $\xi \to \eta$ mapping to f. And given any two such extensions, there is a morphism $\xi' \to \xi$ commuting them.
- Given any two objects $\xi, \eta \in \mathcal{F}$ and an arrow $f : p_{\mathcal{F}}\xi \to p_{\mathcal{F}}\eta$, there is at most one arrow $\widetilde{f} : \xi \to \eta$ lifting f.

⌟

Proof: □

Prop. (4.1.8.32). A fibered category over $\mathcal{C}$ is a quasi-functor iff it is equivalent to a presheaf. ⌟

Proof: If it is equivalent to a functor, then $\mathcal{F}(U)$ is equivalent to a setoid, thus it is an equivalent relation, by(4.1.1.15). Conversely, if $\mathcal{F}$ is a quasi-functor, then it is fibered in groupoids, thus by(4.2.3.22) every morphism is Cartesian, and if we denote $\Phi(U)$ the equivalence classes of $\mathcal{F}(U)$, then a morphism $U \to V$ will induce a morphism $\Phi(V) \to \Phi(V)$ by the property of Cartesian arrows. Then clearly this defines a presheaf that is equivalent to $\mathcal{F}$. □

Representability

Def. (4.1.8.33) [Representable Fibered Category]. A fibered category is called **representable** if it is equivalent to the fibered category $\mathcal{C}/X$ defined in(4.2.3.29) for some $X \in \mathcal{C}$. ⌟

Prop. (4.1.8.34) [2-Categorical Yoneda Lemma]. Let $\mathcal{F}$ be a fibered category over $\mathcal{C}$ and $X \in \mathcal{C}$, there is an equivalence of categories:

$$\mathrm{Hom}_{\mathcal{C}}((\mathcal{C}/X), \mathcal{F}) \cong \mathcal{F}(X) : \varphi \mapsto \varphi(\mathrm{id}_X)$$

⌟

Proof: To show this functor is essentially surjective, choose a choice of pullbacks of $\mathcal{F}$, for any $\xi \in \mathcal{F}(X)$, we define a $F : \mathcal{C}/X \to \mathcal{F}$ that maps a $\varphi : U \to X$ to $\varphi^*\xi$, and to any morphism in $\mathcal{C}/X$ an arrow in $\mathcal{F}$ induced by Cartesian property.

To show it is fully faithful, notice a natural transformation of $\varphi, \psi \in \mathrm{Hom}_{\mathcal{C}}((\mathcal{C}/X), \mathcal{F})$ is determined by their value on id_X, and any map $\varphi(\mathrm{id}_X) \to \psi(\mathrm{id}_X)$ induces a natural transformation, by Cartesian properties. □

Cor. (4.1.8.35) [Characterization of Representability]. Translating the 2-Yoneda lemma and(4.2.3.14), we see that a fibered category $\mathcal{F}$ is representable by $X \in \mathcal{C}$ iff $\mathcal{F}$ is fibered in groupoids, and there is an object $\xi \in \mathcal{F}(X)$ that for any object $\rho \in \mathcal{F}$, there is a unique arrow $\rho \to \xi$. ⌟

Cor. (4.1.8.36). If $\mathcal{X}, \mathcal{Y}$ are fibered categories over $\mathcal{C}$ representable by U, V resp., then there is an isomorphism of sets

$$\mathrm{Hom}_{\mathcal{C}}(\mathcal{X}, \mathcal{Y})/2 - \text{isomorphisms} \cong \mathrm{Hom}_{\mathcal{C}}(U, V)$$

⌟

Proof: By Yoneda lemma there is an equivalence $\mathrm{Hom}_{\mathcal{C}}(\mathcal{X}, \mathcal{Y}) \cong \mathrm{Hom}_{\mathcal{C}}(U, V)$, and then $\mathrm{Hom}_{\mathcal{C}}(\mathcal{X}, \mathcal{Y})$ is an equivalence relation by(4.1.1.15), so the isomorphism is clear. □

Def. (4.1.8.37) [Representable 1-Morphisms]. Let $\mathcal{C}$ be a category and $F : \mathcal{X} \to \mathcal{Y}$ be a morphism of categories fibered over $\mathcal{C}$, then F is called **representable** if for any $U \in \mathcal{C}$ and a morphism $\mathcal{C}/U \to \mathcal{Y}$, the fibered category $(\mathcal{C}/U) \times_{\mathcal{Y}} \mathcal{X} \to \mathcal{C}/U$ is representable(4.2.3.32)(Notice it is a fibered category by(4.2.3.15) and(4.2.3.16)). ⌟

Prop. (4.1.8.38) [Diagonal and Representability]. Let $\mathcal{S}$ be a category fibered in groupoids over $\mathcal{C}$. Assume $\mathcal{C}$ has fibered product, then the following are equivalent:

- $\Delta_S : \mathcal{S} \to \mathcal{S} \times_{\mathcal{C}} \mathcal{S}$ is representable.

- For every $U \in \mathcal{C}$, any $G : \mathcal{C}/U \to \mathcal{S}$ is representable.

⌟

Proof: Cf.[Sta]02YA.

The key to this proposition is the fibered product diagram(4.2.3.15)(4.1.1.48)

$$\begin{array}{ccc} X \times_{\mathcal{F}} Y & \longrightarrow & \mathcal{F} \\ \downarrow & & \downarrow \Delta \\ X \times_S Y & \xrightarrow{f \times g} & \mathcal{F} \times_S \mathcal{F} \end{array}$$

which still holds in the 2-commutative sense.

So if $\Delta_{\mathcal{F}}$ is schematic, then $X \times_{\mathcal{F}} Y$ is a scheme, so $X \to \mathcal{F}$ is schematic, for any scheme X. Conversely, consider the fibered products

$$\begin{array}{ccccc} \mathcal{F} \times_{\mathcal{F} \times_S \mathcal{F}} X & \longrightarrow & X \times_{\mathcal{F}} X & \longrightarrow & \mathcal{F} \\ \downarrow & & \downarrow & & \downarrow \Delta \\ X & \xrightarrow{\Delta} & X \times_S X & \xrightarrow{f \times g} & \mathcal{F} \times_S \mathcal{F} \end{array}$$

induced by $h = f \times g : X \mapsto \mathcal{F} \times_S \mathcal{F}$. So in order to prove $\Delta_{\mathcal{F}}$ is schematic, it suffices to prove $\mathcal{F} \times_{\mathcal{F} \times_S \mathcal{F}} X$ is a scheme, and for this, it suffices to prove $X \times_{\mathcal{F}} X$ is a scheme. But $X \times_{\mathcal{F}} X \to X$ is a pullback of $X \to \mathcal{F}$, so it is a scheme. □

4.2 Categories II

Main references are [Mac98], [Bor94], [Coend Calculus, Fosco Loregian].

1 Tensor Categories

Notation (4.2.1.1).

- Let $k \in \texttt{Field}$.

⌟

Def. (4.2.1.2)[Tensor Categories]. A **tensor category** over a field k is an Artinian Abelian category over k together with a strict monoidal structure that is bilinear and satisfies $\mathrm{End}(\mathbb{1}) = k$.

A **tensor functor** is a functor between tensor categories that is additive and monoidal. ⌟

Prop. (4.2.1.3) [End($\mathbb{1}$)]. If $\mathcal{C}$ is a rigid tensor category, then $\mathrm{End}(\mathbb{1})$ is a ring that acts on objects $X \in \mathcal{C}$ via $X \cong \mathbb{1} \otimes X$. The action of $\mathrm{End}(\mathbb{1})$ commutes with $\mathrm{End}(X)$, in particular, $\mathrm{End}(\mathbb{1})$ is commutative and $\mathcal{C}$ is $\mathrm{End}(\mathbb{1})$-linear. ⌟

Rigid Tensor Categories

Def. (4.2.1.4)[Rigid Tensor Categories]. Let $\mathcal{C}$ be a monoidal category, an element $X \in \mathcal{C}$ is called **rigid object** if it has left and right duals. A **rigid tensor category** is a tensor category(4.2.1.2) s.t. every object is rigid. In particular, by(4.1.5.19), a rigid tensor category is closed. ⌟

Prop. (4.2.1.5). If $\mathcal{C}$ is a rigid tensor category, then the functor

Equivalence of $\mathcal{C}^{\mathrm{op}}$ and $\mathcal{C}^{opp}$.**?** ⌟

Cor. (4.2.1.6). Any natural transformation of monoidal functors between rigid tensor categories is an isomorphism. ⌟

Proof: Cf.[Milne, Tannakian Categories, P13].**?** □

Prop. (4.2.1.7) [Trace and Rank]. Let $\mathcal{C}$ be a symmetric rigid tensor category, we can define a trace morphism

$$\mathrm{tr}_X : \mathrm{End}(X) \to \mathrm{End}(\mathbb{1}) : f \mapsto 1 \to X \otimes X^* \xrightarrow{f \otimes \mathrm{id}} X \otimes X^* \to X^* \otimes X \to 1$$

And the **dimension** of X is defined to be $\mathrm{tr}_X(\mathrm{id}_X) \in \mathrm{End}(1)$. ⌟

Prop. (4.2.1.8)[Abelian Rigid Tensor Categories Exact]. If $\mathcal{C}$ is an Abelian rigid tensor category, then $\otimes$ commutes with inverse limits and direct limits in each variable. ⌟

Proof: It commutes with direct limits because it is left adjoint to the Hom functor, and it commutes with inverse limits by considering the opposite category(4.2.1.5). □

Prop. (4.2.1.9). $\dim(X \otimes Y) = \dim X \cdot \dim Y$. If there is an exact sequence $0 \to X \to Z \to Y \to 0$, then $\dim(Z) = \dim(X) + \dim(Y)$. ⌟

Prop. (4.2.1.10) [Decompositions]. Let $(\mathcal{C}, \otimes)$ be a rigid Abelian tensor category and if U is a subobject of 1, then $1 = U \oplus U^\perp$ where $U^\perp = \ker(1 \to U^\vee)$. Consequently, 1 is a simple object iff $\mathrm{End}(1)$ is a field. And any rigid tensor category can be decomposed as rigid Abelian tensor categories $\mathcal{C}_I$ with $\mathrm{End}(1_i)$ being fields. ⌟

Proof: Let $V = \mathrm{Coker}(U \to 1)$, by tensoring $0 \to U \to 1 \to V \to 0$ with $U \hookrightarrow 1$, we get exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U & \longrightarrow & 1 & \longrightarrow & V & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & \overset{0}{\nearrow} & \uparrow & & \\ 0 & \longrightarrow & U\otimes U & \longrightarrow & U & \longrightarrow & V\otimes U & \longrightarrow & 0 \end{array}$$

thus $V \otimes U = 0$ and $U \otimes U = U$ via $1 \otimes 1 \cong 1$.

For the rest, Cf.[Tannakian Categories, Milne, P14]. □

Def. (4.2.1.11) [Associative Algebra in a Symmetric Tensor Category]. ⌟

<u>**Tannakian Categories**</u>

Def. (4.2.1.12) [Fiber Functor]. Let $\mathcal{C}$ be a k-linear tensor category, then a **fiber functor** on $\mathcal{C}$ with values in a k-algebra R is a k-linear exact faithful tensor functor $\eta : \mathcal{C} \to \mathcal{M}\mathrm{od}_R$ that takes values in the subcategory $\mathbf{Proj}_R$. ⌟

Def. (4.2.1.13) [Tannakian Category]. A **Tannakian category** is a symmetric rigid tensor category(4.2.1.4) $\mathcal{C}$ that $\mathrm{End}(\mathbb{1}) = k$ together with a fiber functor(4.2.1.12) with values in $R \in \mathcal{CR}\mathrm{ing}_k$. ⌟

Def. (4.2.1.14) [Neutral Tannakian Categories]. A **neutral Tannakian category** is a Tannakian category that the fiber functor is valued in k. By(18.5.2.9), such a category is equivalent to $\mathrm{Rep}_k(G)$ for some affine group scheme G, and such G is uniquely defined up to inner automorphisms.

In particular, a Tannakian category can be thought of as an abstract version of the category of representations of an affine group scheme that has no distinguished "forgetful"functor, just as a vector space is an abstract version of k^n that has no distinguished basis. ⌟

2 Enriched Category

Def. (4.2.2.1) [Enriched Categories]. Given a monoidal category $(\mathcal{C}, \otimes)$, an **enriched category** $\mathcal{D}$ over $\mathcal{C}$ consists of the following data:

- a collection of objects.
- For objects $X, Y \in \mathcal{D}$, a mapping object $\mathrm{Map}_{\mathcal{D}}(X, Y) \subset \mathcal{C}$.
- For objects $X, Y, Z \in \mathcal{D}$, a composite map $\mathrm{Map}_{\mathcal{D}}(X, Y) \otimes_{\mathcal{C}} \mathrm{Map}_{\mathcal{D}}(Y, Z) \to \mathrm{Map}_{\mathcal{D}}(X, Z)$ that is associative.
- For every $X \in D$, a morphism $1 \mapsto \mathrm{Map}_{\mathcal{D}}(X, X)$ that satisfies the commutative diagrams of the identity morphism.

⌟

Def. (4.2.2.2) [Category of Enriched Categories]. We can naturally define morphisms and natural transformations of categories enriched over a monoidal category $\mathcal{C}$. The resulting category is denoted by $\mathcal{C}\mathrm{at}_{\mathcal{C}}$. ⌟

Prop. (4.2.2.3) [Completeness and Cocompleteness]. Let $\mathcal{C}$ be a complete and cocomplete symmetric monoidal closed category, then $\mathcal{C}\mathrm{at}_{\mathcal{C}}$ is also complete and cocomplete. ⌟

Proof: Cf.[H. Wolff. V-cat and V-graph].**?** □

Prop. (4.2.2.4) [Transfer of Enriched Structure]. Given a right-lax monoidal functor between monoidal categories $F : \mathcal{C} \to \mathcal{C}'$ and a category $\mathcal{D}$ enriched over $\mathcal{C}$, we may obtain a category $F(\mathcal{D})$ enriched over $\mathcal{C}'$ by asserting $\mathrm{Map}_{F(\mathcal{D})}(X, Y) = F(\mathrm{Map}(X, Y))$. It is an enriched category just by the definition of right-lax monoidal functors. ⌟

Prop. (4.2.2.5) [Underlying Category]. For a category enriched $\mathcal{D}$ over $\mathcal{C}$, by(4.1.5.14), we can transfer the structure via $\mathcal{C} \to \mathcal{S}\mathrm{et} : X \mapsto \mathrm{Hom}(1, X)$, and the resulting category is called the underlying category of $\mathcal{D}$. ⌟

Prop. (4.2.2.6).

- A category enriched in $\mathcal{S}\mathrm{et}$ is just a usual category.
- A right-closed monoidal category is enriched over itself if we define $\mathrm{Map}(X, Y) = Y^X$.(Check). ⌟

Def. (4.2.2.7) [Tensored Category]. Let $\mathcal{C}$ be a right-closed monoidal category and $\mathcal{D}$ a category enriched over $\mathcal{C}$, then $\mathcal{D}$ is called **tensored over** $\mathcal{C}$ if for any $C \in \mathcal{C}$ and $X \in \mathcal{D}$, there is an isomorphism of functors

$$\eta : \mathrm{Map}_{\mathcal{D}}(X, -)^C \cong \mathrm{Map}_{\mathcal{D}}(X \otimes C, -).$$

for some element $X \otimes C \in \mathcal{D}$.

In particular, this implies $\mathrm{Hom}_{\mathcal{C}}(C, \mathrm{Map}(X, Y)) \cong \mathrm{Hom}_{\mathcal{D}}(X \otimes C, Y)$, thus $X \otimes C$ is determined up to a unique isomorphism, and the map $(X, C) \mapsto X \otimes C$ defines a functor $\mathcal{D} \times \mathcal{C} \to \mathcal{D}$ that there are natural morphisms

$$X \otimes (C \otimes D) \cong (X \otimes C) \otimes D.$$

Dually, if $\mathcal{C}$ is left-closed and there is an object ${}^C X$ that there is an isomorphism of functors

$${}^C\,\mathrm{Map}(-, X) \cong \mathrm{Map}(-, {}^C X)$$

then $\mathcal{D}$ is called **cotensored** over $\mathcal{C}$. ⌟

Proof: □

Prop. (4.2.2.8). If $\mathcal{C}$ is a right-closed monoidal category, then it is naturally tensored over itself, as defined in(4.2.2.6). ⌟

Lifting Property and Small Object Argument

Def. (4.2.2.9) [lifting Properties]. Let $\mathcal{C}$ be a category and $p : A \to B, q : X \to Y$ be morphisms, then p is said to have **left lifting property** w.r.t q and q is said to have **right lifting property** w.r.t p if given any diagram $\begin{array}{ccc} A & \longrightarrow & X \\ \downarrow p & \nearrow & \downarrow q \\ B & \longrightarrow & Y \end{array}$, there is a dotted arrow completing the diagram.

For a set A of morphisms of $\mathcal{C}$, let $l(A)$ denote the morphisms that have left lifting property w.r.t A and $r(A)$ the morphisms that have right lifting property w.r.t A. ⌟

Def. (4.2.2.10) [Weakly Saturated Class]. Let $\mathcal{C}$ be a category with all small colimits, then a class of morphisms of $\mathcal{C}$ is called **weakly saturated** if it satisfies:

- Closed under pushout.

- Closed under transfinite composition: Let α be an ordinal and $\{D_\beta\}_{\beta<\alpha}$ be a system of objects in $\mathcal{C}_{C/}$ indexed by α. For $\beta<\alpha$, let $D_{<\beta}$ be the colimit of system $\{D_\gamma\}_{\gamma<\beta}$ in $\mathcal{C}_{C/}$, then if each $D_{<\beta}\to D_\beta$ is in S, then $C\to D_{<\alpha}$ is in S.
- Closed under Retraction: In the category of morphisms of $\mathcal{C}$, if there is a morphism $F:f\to g, G:g\to f$ that $G\circ F=\mathrm{id}$, and $g\in S$, then $f\in S$.

⌟

Cor. (4.2.2.11). The second condition implies all isomorphisms are in S, and S is closed under composition. ⌟

Prop. (4.2.2.12) [Lifting and Retraction]. For a diagram $\begin{array}{ccc} X & = & X \\ \downarrow{\scriptstyle i} & \overset{s}{\nearrow} & \downarrow{\scriptstyle p} \\ Z & \xrightarrow{f} & Y \end{array}$ represents p as a retraction of u, as the diagram $\begin{array}{ccccc} X & \xrightarrow{i} & Z & \xrightarrow{s} & X \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle p} \\ Y & = & Y & = & Y \end{array}$ shows.

Dually a diagram $\begin{array}{ccc} X & \xrightarrow{i} & Y \\ \downarrow{\scriptstyle q} & \overset{s}{\nearrow} & \downarrow{\scriptstyle f} \\ Z & = & Z \end{array}$ represents q as a retraction of i. ⌟

Prop. (4.2.2.13) [Small Object Argument]. Let $\mathcal{C}$ be a presentable category and $A_0=\{\varphi_i:C_i\to D_i\}$ be a small collection of morphisms in $\mathcal{C}$, then there is a morphism $T:\mathcal{C}^{[1]}\to\mathcal{C}^{[2]}$ taking morphisms $f:X\to Z$ in $\mathcal{C}$ to the diagram

$$\begin{array}{ccccc} & & Y & & \\ & \overset{f'}{\nearrow} & & \overset{f''}{\searrow} & \\ X & & \xrightarrow{\quad f \quad} & & Z \end{array}$$

That f' belongs to the weakly saturated class generated by A_0 and $f''\in r(A_0)$.

Moreover, if κ is a regular cardinal that each C_i,D_i is κ-compact, then T commutes with κ-filtered colimits. ⌟

Proof: Cf.[HTT, P788]. □

Lemma (4.2.2.14). $l(A)$ is weakly saturated for any set of morphisms A(Clear). ⌟

Cor. (4.2.2.15) [Generated Weakly Saturated Class]. For any presentable category $\mathcal{C}$ and A a set of morphisms in $\mathcal{C}$, $l(r(A))$ is the smallest weakly saturated class of morphisms containing A. ⌟

Proof: One direction of inclusion is by(4.2.2.14), for the other, if $f:X\to Z\in l(r(A))$, then there is a factorization $X\xrightarrow{f'}Y\xrightarrow{f''}Z$, where $f'\in\overline{A}$ and $f''\in r(A)$, thus $f\in l(f'')$, thus f is retraction of f':

$$\begin{array}{ccc} X & \xrightarrow{f'} & Y \\ \downarrow{\scriptstyle f} & \overset{g}{\nearrow} & \downarrow{\scriptstyle f''} \\ Z & \longrightarrow & Z \end{array} \Rightarrow \begin{array}{ccccc} X & \longrightarrow & X & \longrightarrow & X \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} \\ Z & \xrightarrow{g} & Y & \xrightarrow{f''} & Z \end{array}$$

Thus $f\in\overline{A}$. □

Trees

Cf.[HTT, Appendix]

3 Fibered Categories

Categories of Categories

Def. (4.2.3.1) [2-Category of Categories over Categories]. There is a 2-category of categories over $\mathcal{C}$, where the 1-morphisms are morphisms of categories over $\mathcal{C}$ and the 2-morphisms are base-preserving natural transformations.

Two categories over $\mathcal{C}$ are called **equivalent** if they are equivalent in this 2-category. ⌟

Prop. (4.2.3.2) [2-Fibered Products in the Categories of Categories]. 2-fibered products exists in the categories of categories. ⌟

Proof: Let $F : \mathcal{A} \to \mathcal{C}, G : \mathcal{B} \to \mathcal{C}$ be functors, then we can define a category $\mathcal{A} \times_{\mathcal{C}} \mathcal{B}$ as follows:

- Objects are the triples (A, B, f) where $A \in \mathcal{A}, B \in \mathcal{B}$ and $f : F(A) \to G(B)$ is an isomorphism in $\mathcal{C}$.
- Morphisms from (A, B, f) to (A', B', f') are pairs (a, b) where $a : A \to A', b : B \to B'$ s.t. the diagram

$$\begin{array}{ccc} F(A) & \xrightarrow{f} & G(B) \\ \downarrow{\scriptstyle F(a)} & & \downarrow{\scriptstyle G(b)} \\ F(A') & \xrightarrow{f'} & G(B') \end{array}$$

  is commutative.

$\mathcal{A} \times_{\mathcal{C}} \mathcal{B}$ is a category both over $\mathcal{A}$ and over $\mathcal{B}$, and it fits into a 2-fiber products diagram

$$\begin{array}{ccc} \mathcal{A} \times_{\mathcal{C}} \mathcal{B} & \longrightarrow & \mathcal{B} \\ \downarrow & & \downarrow \\ \mathcal{A} & \longrightarrow & \mathcal{C} \end{array}$$

where the invertible 2-morphism is given by $\psi_{(A,B,f)} = f : F(A) \to G(B)$.

The verification that this defines a final object in the 2-category of 2-commutative diagrams is in[Sta]02X9. □

Cor. (4.2.3.3). The 2-fibered product $\mathcal{A} \times_{\mathcal{C}} \mathcal{B}$ is a groupoid iff $\mathcal{A}, \mathcal{B}$ are all groupoids. ⌟

Prop. (4.2.3.4). Let $\mathcal{A} \to \mathcal{C}, \mathcal{B} \to \mathcal{C}, \mathcal{C} \to \mathcal{D}$ be functors between categories, then there is a 2-fiber product diagram

$$\begin{array}{ccc} \mathcal{A} \times_{\mathcal{C}} \mathcal{B} & \longrightarrow & \mathcal{A} \times_{\mathcal{D}} \mathcal{B} \\ \downarrow & & \downarrow \\ \mathcal{C} & \xrightarrow{\Delta_{\mathcal{C}/\mathcal{D}}} & \mathcal{C} \times_{\mathcal{D}} \mathcal{C} \end{array}$$

⌟

Proof: □

Prop. (4.2.3.5) [2-Fibered Products of Categories]. The $(2,1)$-category of categories over $\mathcal{C}$ has 2-fiber products(4.1.4.6). More explicitly, suppose $F:\mathcal{X}\to\mathcal{S},\mathcal{Y}\to\mathcal{S}$ be morphisms of categories over $\mathcal{C}$, $\mathcal{X}\times_{\mathcal{S}}\mathcal{Y}$ is given as follows:

- Objects of $\mathcal{X}\times_{\mathcal{C}}\mathcal{Y}$ are quadruples (U,x,y,f), where $U\in\mathcal{C},x\in\mathcal{X}_U,y\in\mathcal{Y}_U$, and $f:F(x)\to G(y)$ is an isomorphism in $\mathcal{S}_U$.
- A morphism $(U,x,y,f)\to(U',x',y',f')$ is given by a pair (a,b), where $a:x\to x'$ is a morphism in $\mathcal{X}$ and $y\to y'$ is a morphism in $\mathcal{Y}$ that
  - a,b induce the same morphism $U\to U'$.
  - the diagram
  $$\begin{array}{ccc} F(x) & \xrightarrow{f} & G(y) \\ \downarrow{\scriptstyle F(a)} & & \downarrow{\scriptstyle G(b)} \\ F(x') & \xrightarrow{f'} & G(y') \end{array}$$
  is an isomorphism.

$\mathcal{X}\times_{\mathcal{S}}\mathcal{Y}$ is endowed with morphisms to $\mathcal{X}$ and $\mathcal{Y}$ over $\mathcal{C}$ that the invertible 2-morphism giving the 2-commutativity is $\psi_{(U,x,y,f)}:F(x)\to G(y)$.

The verification of the universal properties are similar to that of(4.2.3.2). ⌟

Cor. (4.2.3.6). There is an equivalence of fibre categories:
$$(\mathcal{X}\times_{\mathcal{S}}\mathcal{Y})_U\cong\mathcal{X}_U\times_{\mathcal{S}_U}\mathcal{Y}_U.$$
⌟

Fibered Categories

Def. (4.2.3.7) [(Co)Cartesian Arrows]. Let $p:\mathcal{F}\to\mathcal{C}$ be a morphism, then a **Cartesian arrow** is an arrow $\varphi:C'\to C$ in $\mathcal{F}$ that for any object $C''\in\mathcal{F}$ the map
$$\mathrm{Hom}(C'',C')\to\mathrm{Hom}(C'',C)\times_{\mathrm{Hom}(p(C''),p(C))}\mathrm{Hom}(p(C''),p(C'))$$
is a bijection. A **coCartesian arrow** is an arrow that corresponds to a Cartesian diagram in $\mathcal{F}^{op}\to\mathcal{C}^{\mathrm{op}}$. ⌟

Prop. (4.2.3.8).

- If f is Cartesian, then $f\circ g$ is Cartesian iff g is Cartesian.
- An arrow in $\mathcal{F}$ whose image is an isomorphism is Cartesian iff it is itself an isomorphism.

⌟

Proof: Easy. □

Def. (4.2.3.9) [Quasi-Fibrantion]. A functor $F:\mathcal{C}\to\mathcal{D}$ is called a **quasi-fibration** if for any $X\in\mathcal{C}$ and an isomorphism $f:F(X)\cong Y$, there is an isomorphism $\overline{f}:X\to\overline{Y}$ mapping to f. ⌟

Def. (4.2.3.10) [2-Category of Fibered Categories]. A **fibered category** over $\mathcal{C}$ is a category over $\mathcal{C}$ $p:\mathcal{F}\to\mathcal{C}$ that for any $\eta\in\mathcal{F}$ and an arrow $f:U\to p(\eta)$, there is a Cartesian arrow $\xi\to\eta$ in $\mathcal{F}$ lifting f. A **cofibered category** over $\mathcal{C}$ is a category $p:\mathcal{F}\to\mathcal{C}$ that the dual category $p^{op}:\mathcal{F}^{op}\to\mathcal{C}^{\mathrm{op}}$ is a fibered category.

A morphism of fibered categories over $\mathcal{C}$ is a morphism of categories over $\mathcal{C}$ that maps Cartesian morphisms to Cartesian morphisms. A 2-morphism of fibered categories is the same as a 2-morphism of categories over categories. ⌟

Def. (4.2.3.11) [Split Fibered Categories]. A **split fibered category** is a fibered category $\mathcal{F} \to \mathcal{C}$ that comes from a functor $\mathcal{C}^{op} \to \mathcal{C}at$. ⌟

Def. (4.2.3.12) [Cleavage]. A **cleavage** of a fibered category $\pi : \mathcal{F} \to \mathcal{C}$ is a choice of Cartesian arrow f^* lifting f for any $f \in \mathcal{A}rr(\mathcal{C})$. ⌟

Lemma (4.2.3.13). Let $F : \mathcal{F} \to \mathcal{G}$ be a morphism of fibered categories over $\mathcal{C}$ that $\mathcal{F}(U) \to \mathcal{G}(U)$ are fully faithful for any $U \in \mathcal{C}$, then F is fully faithful. ⌟

Proof: To show F is fully faithful, it suffices to show for objects X, Y lying over U, V, F induces a bijection of morphisms from x to y lying over a fixed $f : U \to V$. Choose a Cartesian morphism $f^*y \to y$ in $\mathcal{S}_1$ lying over f, then this induces a bijection between morphisms from x to y lying over f and $\mathrm{Hom}_{\mathcal{S}_{1,U}}(x, f^*y)$. Similarly, because F preserves Cartesian morphisms, we get a bijection between morphisms $F(x) \to F(y)$ lying over f and $\mathrm{Hom}_{\mathcal{S}_{2,U}}(F(x), F(f^*y))$. Then the desired bijection follows from the hypothesis. □

Prop. (4.2.3.14) [Equivalence of Fibered Categories]. Let $F : \mathcal{F} \to \mathcal{G}$ be a morphism of fibered categories. Then F is an equivalence iff the restriction $F_U : \mathcal{F}(U) \to \mathcal{G}(U)$ is an equivalence of categories for any object U of $\mathcal{C}$. ⌟

Proof: One direction is trivial, for the other, the proof is similar to the fact essentially surjective+fully faithful implies equivalence.

Because $F(U)$ are equivalences, for any object ξ of $\mathcal{G}$ over U, pick an object $G\xi$ in $\mathcal{F}(U)$ together with an isomorphism $\alpha_\xi : \xi \cong F(G\xi)$. And for any morphism $\xi \to \eta$, by(4.2.3.13), there is a unique arrow $G\varphi : G\xi \to G\eta$ that $F(G\varphi) = \alpha_\eta \circ \varphi \circ \alpha_\xi^{-1}$.

Thus clearly there is a 2-isomorphism $\mathrm{id}_\mathcal{G} \cong F \circ G$. It remains to construct an 2-isomorphism $\mathrm{id}_\mathcal{F} \cong G \circ F$: For any object ξ' over U, since $F(U)$ is fully faithful, there is a unique isomorphism $\beta_{\xi'} : \xi' \cong G \circ F(\xi)$ in $\mathcal{F}(U)$ that $F\beta_{\xi'} = \alpha_{F\xi'}$. Then this is easily checked to be an 2-isomorphism $\beta : \mathrm{id}_\mathcal{F} \cong F \circ G$. □

Prop. (4.2.3.15) [2-Fiber Products of Fibered Categories]. 2-fiber products exists in the category of fibered categories, and it coincides with that defined in(4.2.3.5). ⌟

Proof: it suffices to show for fibered categories $\mathcal{X}, \mathcal{Y}$ over $\mathcal{C}$, $\mathcal{X} \times_\mathcal{C} \mathcal{Y}$ is also fibered over $\mathcal{C}$. Let (x, y, φ) be an object of $\mathcal{X} \times_\mathcal{C} \mathcal{Y}$ mapping to $U \in \mathcal{C}$ and $f : V \to U$ is a morphism in $\mathcal{C}$, choose Cartesian morphisms $a : f^*x \to x$, $b : f^*y \to y$ lying over f, then $F(a)$ and $G(b)$ are Cartesian. Since $\varphi : F(x) \to G(y)$ is an isomorphism, by the property of Cartesian morphisms, there exists a unique isomorphism $f^*\varphi : F(f^*x) \to G(f^*y) \in \mathcal{S}_V$ that $G(b) \circ f^*\varphi = \varphi \circ F(a)$. In other words, $(F(a), F(b)) : (V, f^*x, f^*y, f^*\varphi) \to (U, x, y, \varphi)$ is a morphism in $\mathcal{X} \times_\mathcal{S} \mathcal{Y}$.

The verification that this morphism is Cartesian is omitted**?**. □

Lemma (4.2.3.16). Let $\mathcal{S} \to \mathcal{C}$ be a fibered category that factors through $\mathcal{C}/U$ where $U \in \mathcal{C}$, then $\mathcal{S} \to \mathcal{C}/U$ is also a fibered category. ⌟

Proof: Cf.[[Sta]02XR]. □

Def. (4.2.3.17) [G-Equivariant Object]. Let $G : \mathcal{C}^{op} \to (Grp)$ be a group functor and $p_{\mathcal{F}} : \mathcal{F} \to \mathcal{C}$ a fibered category, and X an object of $\mathcal{C}$ with an action of G. A **G-equivariant object** of $\mathcal{F}(X)$ is an object ρ of $\mathcal{F}(X)$ that there is an action of $G \circ p_{\mathcal{F}}$ on ρ and for any object U and $\xi \in \mathcal{F}(U)$, the function $p_{\mathcal{F}} : \mathrm{Hom}_{\mathcal{F}}(\xi, \rho) \to \mathrm{Hom}_{\mathcal{C}}(U, X)$ is $G(U)$-equivariant.

The category $\mathcal{F}^G(X)$ of G-equivariant objects of $\mathcal{F}(X)$ consisting of $G \circ p_{\mathcal{F}}$-equivariant morphism of G-equivariant objects. ⌟

Prop. (4.2.3.18). Let π_2 is the projection $G \otimes X \to X$, ρ be an object of $\mathcal{F}(X)$, then a G-equivariant structure on ρ is the same as a Cartesian arrow $\beta : \pi_2^* \rho \to \rho$ that $p_{\mathcal{F}} \beta = \alpha$, and satisfies the desired commutative diagram corresponding to $(gh)x = g(h(x))$. And a morphism of G-equivariant objects just corresponds to a morphism of pairs (ρ, β). ⌟

Proof: Cf.[Vistoli, P68]. □

Def. (4.2.3.19) [Presheaf of Arrows]. Let $\mathcal{F}$ be a fibered category over $\mathcal{C}$, and $\xi, \eta \in \mathcal{F}(S)$, then we can define a quasi-functor $\mathcal{H}om_S(\xi, \eta) \to (\mathcal{C}/S)$, where

$$\mathcal{H}om_S(\xi, \eta)(U/S) = \{(\xi_1 \to \xi, \eta_1 \to \eta, \varphi)\}$$

where $\xi_1 \to \xi, \eta_1 \to \eta$ are Cartesian arrows over $U \to S$, and $\varphi : \xi_1 \to \eta_1 \in \mathcal{F}(U)$. The arrows in $\mathrm{Hom}_S(\xi, \eta)$ are uniquely defined by the property of Cartesian arrows. Then it is a quasi-functor, by(4.2.3.30).

Then it is equivalence to a presheaf $\underline{\mathrm{Hom}}_S(\xi, \eta)$, by(4.2.3.31). Equivalently, this presheaf can be defined by designating a choice of Cartesian arrows. ⌟

Prop. (4.2.3.20)[Splitting a Fibered Category]. Let $\mathcal{F} \to \mathcal{C}$ be a fibered category, then there exists a canonically defined split fibered category $\widetilde{\mathcal{F}} \to \mathcal{C}$ with a canonical equivalence of fibered categories $\widetilde{\mathcal{F}} \to \mathcal{F}$ over $\mathcal{C}$. ⌟

Proof: There is a functor $\mathcal{C}^{op} \to \mathcal{C}at : U \mapsto \mathrm{Hom}(h_U, \mathcal{F})$, with corresponds to a split fibered category $\widetilde{\mathcal{F}}$. There is an obvious morphism $\widetilde{\mathcal{F}} \to \mathcal{F}$, sending an object $\varphi : h_U \to \mathcal{F}$ to $\varphi(\mathrm{id}_U) \in \mathcal{F}(U)$. And for any $f : U \to V \in \mathcal{C}$ and a $\varphi : h_U \to \mathcal{F}$, we send $f^* \varphi \to \varphi \in \widetilde{\mathcal{F}}$ to $\varphi(f : V/U \to U/U) \in \mathcal{F}$, Then we get a canonical map of fibered categories $\widetilde{\mathcal{F}} \to \mathcal{F}$ over $\mathcal{C}$. It is an equivalence of categories by(4.2.3.14) and(4.2.3.33). □

Categories Fibered in Groupoids, Sets and Equivalence Relations

Def. (4.2.3.21) [Category Fibered in Groupoids]. A **category (co)fibered in groupoids/sets/equivalence relations** over $\mathcal{C}$ is a category $\mathcal{F}$ (co)fibered over $\mathcal{C}$ that $\mathcal{F}(U)$ is a groupoid/setoids/equivalence relations(4.1.1.14) for any $U \in \mathcal{C}$. Also we call a category fibered in equivalence relations over $\mathcal{C}$ a **quasi-functor**. ⌟

Prop. (4.2.3.22) [Characterization of Category Fibered in Groupoids]. Let $\mathcal{F}$ be a category over $\mathcal{C}$, then $\mathcal{F}$ is fibered over groupoids over $\mathcal{C}$ iff

- Every morphism in $\mathcal{F}$ is Cartesian.
- Given any $\eta \in \mathcal{F}, U \in \mathcal{C}$ and a morphism $f : U \to p_{\mathcal{F}}(\eta)$, there is an arrow $\varphi : \xi \to \eta \in \mathcal{F}$ mapping to f.

And dually for cofibered categories. ⌟

Proof: If these two holds, then $\mathcal{F}$ is clearly fibered over $\mathcal{C}$, and for any arrow $f : \xi \to \eta$ in $\mathcal{F}(U)$, there is a morphism $g : \eta \to \xi$ that is right inverse to f, then clearly it is the inverse.

Conversely, if $\mathcal{F}$ is fibered over $\mathcal{C}$, it suffices to check1: for any arrow f, the image in $\mathcal{C}$ can be lifted to a Cartesian diagram in $\mathcal{F}$, and differs f by an isomorphism, thus f is also Cartesian by(4.2.3.8). □

Cor. (4.2.3.23). if $\mathcal{A}$ is a category fibered in groupoids over $\mathcal{B}$ and $\mathcal{B}$ is a category fibered in groupoids over $\mathcal{C}$, then $\mathcal{A}$ is a category fibered in groupoids over $\mathcal{C}$. ⌟

Prop. (4.2.3.24) [Associated Category Fibered in Groupoids]. Let $\mathcal{F} \to \mathcal{C}$ be a fibered category, then the **associated category fibered in groupoids** $\mathcal{F}_{cart}$ is the category obtained by deleting all the non-Cartesian arrows. Then $\mathcal{F}_{cart}$ is a category fibered in groupoids over $\mathcal{C}$. ⌟

Proof: Firstly $\mathcal{F}_{cart}$ is a category by(4.2.3.8), and it is a category fibered in groupoids by(4.2.3.22). □

Def. (4.2.3.25) [RIgid Fibered Categories]. A **rigid fibered category** is a fibered category whose associated category fibered groupoids is fibered in setoids. Equivalently, there are no isomorphisms above any id_U. ⌟

Prop. (4.2.3.26) [2-Fibered Products of Categories Fibered in Groupoids]. The 2-fibered products of categories fibered in groupoids over $\mathcal{C}$ is a category fibered in groupoids over $\mathcal{C}$. ⌟

Proof: The 2-fibered products exist by(4.2.3.15), and using (4.2.3.6), it is fibered in groupoids because the 2-fibered products of groupoids is a groupoid by(4.2.3.3). □

Prop. (4.2.3.27) [Characterization of Categories Fibered in Setoids]. Let $\mathcal{F}$ be a category over $\mathcal{C}$, then $\mathcal{F}$ is fibered in setoids over $\mathcal{C}$ iff for any object η of $\mathcal{F}$ and an arrow $f : U \to p_{\mathcal{F}}\eta \in \mathcal{C}$, there is a unique arrow $\xi \to \eta$ mapping to f. ⌟

Proof: Let $\mathcal{F}$ be a category fibered in sets, then pick a Cartesian arrow $\widetilde{f}$ over f, then any other lifting factors through this lifting by the property of Cartesian, then it is identity, because $\mathcal{F}(U)$ is a setoid.

Conversely, if the hypothesis holds, then clearly $\mathcal{F}(U)$ is a setoid, and the fibered category condition holds, because of the uniqueness. □

Cor. (4.2.3.28) [Presheaves and Categories Fibered in Setoids]. Let $\mathcal{C}$ be a category, then categories fibered in setoids over $\mathcal{C}$ are exactly those equivalent to a presheaf over $\mathcal{C}$. ⌟

Cor. (4.2.3.29). In particular, for any object $X \in \mathcal{C}$, the presheaf h_X determines a category fibered in sets, which is just the comma category $\mathcal{C}/X \to \mathcal{C}$. ⌟

Prop. (4.2.3.30) [Characterization of Quasi-Functors]. A category $\mathcal{F}$ over $\mathcal{C}$ is a quasi-functor iff:

- Given any object $\eta \in \mathcal{F}$ and an arrow $f : U \to p_{\mathcal{F}}\eta$, there is a lifting $\xi \to \eta$ mapping to f. And given any two such extensions, there is a morphism $\xi' \to \xi$ commuting them.
- Given any two objects $\xi, \eta \in \mathcal{F}$ and an arrow $f : p_{\mathcal{F}}\xi \to p_{\mathcal{F}}\eta$, there is at most one arrow $\widetilde{f} : \xi \to \eta$ lifting f.

⌟

Proof: □

Prop. (4.2.3.31). A fibered category over $\mathcal{C}$ is a quasi-functor iff it is equivalent to a presheaf. ⌟

Proof: If it is equivalent to a functor, then $\mathcal{F}(U)$ is equivalent to a setoid, thus it is an equivalent relation, by(4.1.1.15). Conversely, if $\mathcal{F}$ is a quasi-functor, then it is fibered in groupoids, thus by(4.2.3.22) every morphism is Cartesian, and if we denote $\Phi(U)$ the equivalence classes of $\mathcal{F}(U)$, then a morphism $U \to V$ will induce a morphism $\Phi(V) \to \Phi(V)$ by the property of Cartesian arrows. Then clearly this defines a presheaf that is equivalent to $\mathcal{F}$. □

Representability

Def. (4.2.3.32) [Representable Fibered Category]. A fibered category is called **representable** if it is equivalent to the fibered category $\mathcal{C}/X$ defined in(4.2.3.29) for some $X \in \mathcal{C}$. ⌟

Prop. (4.2.3.33) [2-Categorical Yoneda Lemma]. Let $\mathcal{F}$ be a fibered category over $\mathcal{C}$ and $X \in \mathcal{C}$, there is an equivalence of categories:

$$\mathrm{Hom}_{\mathcal{C}}((\mathcal{C}/X), \mathcal{F}) \cong \mathcal{F}(X) : \varphi \mapsto \varphi(\mathrm{id}_X)$$

⌟

Proof: To show this functor is essentially surjective, choose a choice of pullbacks of $\mathcal{F}$, for any $\xi \in \mathcal{F}(X)$, we define a $F : \mathcal{C}/X \to \mathcal{F}$ that maps a $\varphi : U \to X$ to $\varphi^*\xi$, and to any morphism in $\mathcal{C}/X$ an arrow in $\mathcal{F}$ induced by Cartesian property.

To show it is fully faithful, notice a natural transformation of $\varphi, \psi \in \mathrm{Hom}_{\mathcal{C}}((\mathcal{C}/X), \mathcal{F})$ is determined by their value on id_X, and any map $\varphi(\mathrm{id}_X) \to \psi(\mathrm{id}_X)$ induces a natural transformation, by Cartesian properties. □

Cor. (4.2.3.34) [Characterization of Representability]. Translating the 2-Yoneda lemma and(4.2.3.14), we see that a fibered category $\mathcal{F}$ is representable by $X \in \mathcal{C}$ iff $\mathcal{F}$ is fibered in groupoids, and there is an object $\xi \in \mathcal{F}(X)$ that for any object $\rho \in \mathcal{F}$, there is a unique arrow $\rho \to \xi$. ⌟

Cor. (4.2.3.35). If $\mathcal{X}, \mathcal{Y}$ are fibered categories over $\mathcal{C}$ representable by U, V resp., then there is an isomorphism of sets

$$\mathrm{Hom}_{\mathcal{C}}(\mathcal{X}, \mathcal{Y})/2 - \text{isomorphisms} \cong \mathrm{Hom}_{\mathcal{C}}(U, V)$$

⌟

Proof: By Yoneda lemma there is an equivalence $\mathrm{Hom}_{\mathcal{C}}(\mathcal{X}, \mathcal{Y}) \cong \mathrm{Hom}_{\mathcal{C}}(U, V)$, and then $\mathrm{Hom}_{\mathcal{C}}(\mathcal{X}, \mathcal{Y})$ is an equivalence relation by(4.1.1.15), so the isomorphism is clear. □

Def. (4.2.3.36) [Representable 1-Morphisms]. Let $\mathcal{C}$ be a category and $F : \mathcal{X} \to \mathcal{Y}$ be a morphism of categories fibered over $\mathcal{C}$, then F is called **representable** if for any $U \in \mathcal{C}$ and a morphism $\mathcal{C}/U \to \mathcal{Y}$, the fibered category $(\mathcal{C}/U) \times_{\mathcal{Y}} \mathcal{X} \to \mathcal{C}/U$ is representable(4.2.3.32)(Notice it is a fibered category by(4.2.3.15) and(4.2.3.16)). ⌟

Prop. (4.2.3.37) [Diagonal and Representability]. Let $\mathcal{S}$ be a category fibered in groupoids over $\mathcal{C}$. Assume $\mathcal{C}$ has fibered product, then the following are equivalent:

- $\Delta_S : \mathcal{S} \to \mathcal{S} \times_{\mathcal{C}} \mathcal{S}$ is representable.
- For every $U \in \mathcal{C}$, any $G : \mathcal{C}/U \to \mathcal{S}$ is representable.

⌟

Proof: Cf.[Sta]02YA.

The key to this proposition is the fibered product diagram(4.2.3.15)(4.1.1.48)

$$\begin{array}{ccc} X \times_{\mathcal{F}} Y & \longrightarrow & \mathcal{F} \\ \downarrow & & \downarrow \Delta \\ X \times_S Y & \xrightarrow{f \times g} & \mathcal{F} \times_S \mathcal{F} \end{array}$$

which still holds in the 2-commutative sense.

So if $\Delta_{\mathcal{F}}$ is schematic, then $X \times_{\mathcal{F}} Y$ is a scheme, so $X \to \mathcal{F}$ is schematic, for any scheme X. Conversely, consider the fibered products

$$\begin{array}{ccccc} \mathcal{F} \times_{\mathcal{F} \times_S \mathcal{F}} X & \longrightarrow & X \times_{\mathcal{F}} X & \longrightarrow & \mathcal{F} \\ \downarrow & & \downarrow & & \downarrow \Delta \\ X & \xrightarrow{\Delta} & X \times_S X & \xrightarrow{f \times g} & \mathcal{F} \times_S \mathcal{F} \end{array}$$

induced by $h = f \times g : X \mapsto \mathcal{F} \times_S \mathcal{F}$. So in order to prove $\Delta_{\mathcal{F}}$ is schematic, it suffices to prove $\mathcal{F} \times_{\mathcal{F} \times_S \mathcal{F}} X$ is a scheme, and for this, it suffices to prove $X \times_{\mathcal{F}} X$ is a scheme. But $X \times_{\mathcal{F}} X \to X$ is a pullback of $X \to \mathcal{F}$, so it is a scheme. $\square$

4.3 Categorical Logic

Main references are [Categorical Logic Notes, Jacob Lurie], [Coend Calculus, Fosco Loregian], [Harder-Narasimhan Filtrations, Huayi Chen], [Harder-Narasimhan Theory, Jonathan Pottharst], [Coend Calculus].

1 Monads and Categories

Def. (4.3.1.1) [Monad]. Let $\mathcal{C}$ be a category, a **monad** on $\mathcal{C}$ is an endofunctor $\mathcal{C} \to \mathcal{C}$ together with two natural morphisms:

- (multiplication)$\mu : T \circ T \to T$.
- (unit)$\mathrm{id}_{\mathcal{C}} \to T$.

that satisfies associativity and unit diagrams. ⌟

Def. (4.3.1.2) [Algebras over Monads]. An **algebra over a monad** T is an object X together with a morphism $\alpha : TX \to X$ that satisfies the diagrams for an algebra. ⌟

2 Group Formation

The goal of this subsection is to give a formation that encompass both the group theory and algebraic group theory.

Def. (4.3.2.1) [Group Formations]. A **group formation** is a category $\mathcal{C} \in \mathcal{C}\mathrm{at}$ with a class of arrows $\mathcal{S} \in \mathcal{C}$ consisting of monomorphisms, satisfying the following axioms:

- G is complete and cocomplete.
- G has a zero object e.
- $\mathcal{S}$ is stable under pullbacks.
- If $N \to H \to G \in \mathcal{S}$ and $H \to G$ is a monomorphism, then $N \to H \in \mathcal{S}$.
- Let $N \to G \in \mathcal{S}$, then N is called a **normal subobject** of G, and $N = \ker(G \to \mathrm{Coker}(N \to G))$.
- For $G \in \mathcal{C}$, coproducts exist in $\mathcal{C}/G$, and if $N \to G, H \to G \in \mathcal{S}$, then the coproduct is also in $\mathcal{S}$, denoted by $NH \to G$.
- Let $N \to G \in \mathcal{S}$ and $H \to G$ a monomorphism, then
  - there is a natural isomorphism: $H/N \cap H \cong HN/N$.
  - If $N \to G \in \mathcal{S}$, then there is a natural isomorphism $G/NH \cong (G/N)/(H/H \cap N)$.

⌟

Prop. (4.3.2.2). ⌟

3 Filtrations of a Category

Def. (4.3.3.1) [Filtrations in a Category]. Let $\mathcal{C}$ be a category with an initial object, a **filtration** of an object X in $\mathcal{C}$ is a family $\mathcal{F} = (X_t)_{t \in \mathbb{R}}$ of subobjects of X indexed by $\mathbb{R}$ that satisfies:

- (decreasing property) if $s \leq t$, then $X_s \to X$ factors through X_t.
- (separation property) for sufficiently small t, X_t is the initial object.

- (exhaustiveness) for sufficiently large s, $X_s = X$.
- (right locally constant property) for any $t \in \mathbb{R}$, there exists $\delta > 0$ that for any $s \in [t, t+\delta)$, the morphism $X_t \to X_s$ are isomorphisms.
- (finite jump)the jump set of $\mathcal{F}$ is finite.

Naturally, we define morphisms of filtrations. ⌟

Def. (4.3.3.2) [Pullback and Pushforward Filtrations]. Suppose fibered products exist in $\mathcal{C}$, for any morphism $f : X \to Y$ and a filtration $\mathcal{G} = (Y_t) \to Y$, then the family $f^*\mathcal{G} = (Y_t \otimes_Y X) \to X$ is a filtration on X, called the **pullback filtration**.

If $f : X \to Y$ and $\mathcal{F} : (X_t) \to X$ is a filtration on X, then if there is a filtration $f_*\mathcal{F}$ on Y and a morphism of filtrations $\mathcal{F} \to f_*\mathcal{F}$ compatible with f, then $f_*\mathcal{F}$ is called the **pushforward filtrations**. ⌟

4 Harder-Narasimhan Formalism

Main references are[Jon20].

Def. (4.3.4.1) [Harder-Narasimhan Formalism]. A **Harder-Narasimhan formalism** consists of

- An exact category $\mathcal{C}$(4.8.2.1).
- A function $\deg : \mathrm{Ob}(\mathcal{C}) \to \mathbb{Z}$ that is additive w.r.t. short exact sequences.
- An exact faithful **generic fiber functor** to an Abelian category $F : \mathcal{C} \to \mathcal{A}$ that induces for each object $F : \mathcal{E} \in \mathcal{C}$ a bijection

  $$\{\text{strict objects of } \mathcal{E}\} \cong \{\text{subobjects of } F(\mathcal{E})\}$$

  where a **strict subobject** is an object that can be prolonged to an exact sequence.
- An additive function rank: $\mathcal{A} \to \mathbb{N}$ on $\mathcal{A}$ that $\mathrm{rank}(\mathcal{L}) = 0 \iff \mathcal{L} = 0$, and its composition with F is also called rank.
- If $u : \mathcal{E} \to \mathcal{E}'$ is a morphism in $\mathcal{C}$ that $F(u)$ is an isomorphism, then $\deg(\mathcal{E}) \le \deg(\mathcal{E}')$ with equality iff u is an isomorphism.

⌟

Cor. (4.3.4.2).

- We are free to choose the "kernel" for u that $F(u)$ is surjection.
- The subobjects of subobjects are subobjects, by axiom3.

⌟

Def. (4.3.4.3) [Saturation]. Let X' be a subobject of X, then we let $\widetilde{X'}$ denote the strict subobject of X corresponding to the subobject $F(X')$ of $F(X)$, called the **saturation** of X'. The saturation satisfies:

-
-
-

⌟

Proof: Cf.[Jon20]P3. □

Prop. (4.3.4.4). Every morphism $f : X \to Y$ has a kernel and a image in $\mathcal{C}$, and $0 \to \ker f \to X \to \operatorname{Im} f \to 0$ is an exact sequence. ⌟

Proof: Cf.[Jon20]P3. □

Prop. (4.3.4.5) [HN-Formalism on the Category of Filtered Vector Spaces]. If L/K is a field extension, there is a category $\mathcal{V}\mathrm{ect}\,\mathrm{Fil}_{L/K}$ consisting of $(V, \mathrm{Fil}^\bullet)$ where $V \in \mathcal{V}\mathrm{ect}_K$ and $\mathrm{Fil}^\bullet$ is a finite filtration on $V \otimes_K L$. It is an exact category by declaring exact sequences be those induce exact sequences on the gradeds.

The generic fiber functor is $\mathcal{V}\mathrm{ect}\,\mathrm{Fil}_{L/K} \to \mathcal{V}\mathrm{ect}_K : (V, \mathrm{Fil}^\bullet) \mapsto V$, and rank is as usual, the **Hodge-Tate degree** is defined to be

$$t_{\text{H-T}}((V, \mathrm{Fil}^\bullet)) = \sum i \dim_L \mathrm{gr}^i(V \otimes_K L).$$

This is a HN-filtration. ⌟

Proof: The axioms can be directly checked, noticing that a subfiltration W_n of a filtration V_n is a strict object iff $W_k = W_n \cap V_k$. □

Def. (4.3.4.6) [Slope]. In a HN-formalism, the **slope** is defined to be $\mathrm{slope}(E) = \frac{\deg(E)}{\mathrm{rank}(E)}$.

$\mathcal{E}$ is called **semistable of slope** λ iff $\mathrm{slope}(\mathcal{E}) = \lambda$, and $\mathrm{slope}(\mathcal{E}') \le \lambda$ for any nonzero strict subobject $\mathcal{E}' \subset \mathcal{E}$. ⌟

Prop. (4.3.4.7). If $0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0$ be a short exact sequence in $\mathcal{C}$, then:

- If two of them have the same slope, then so does the third.
- If two of them have different slope, then we know the ordering of these slopes.

⌟

Proof: Just notice that the degree and rank are all additive functions. □

Prop. (4.3.4.8). If $\mathcal{E}$ is semistable of slope λ, then for any morphism $u : \mathcal{E} \to \mathcal{E}''$ that $F(u)$ is surjective, $\mu(\mathcal{E}'') \ge \lambda$. ⌟

Proof: Take the kernel of $F(u)$ in $\mathcal{A}$, which corresponds to a strict object $\mathcal{E}'$ of $\mathcal{E}$, and $0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0$ is exact, so we can use(4.3.4.19). □

Cor. (4.3.4.9). If $\mathcal{E}, \mathcal{F}$ are semistable of slopes $\lambda > \mu$, then $\mathrm{Hom}_{\mathcal{C}}(\mathcal{E}, \mathcal{F}) = 0$. ⌟

Proof: Notice F is faithful. □

Prop. (4.3.4.10) [Semistable Objects]. If $f : \mathcal{E} \to \mathcal{F}$ be a map of vector bundles of the same slope λ, then $\ker(f)$ and $\mathrm{Coker}(f)$ are all semistable vector bundles of slope λ, and if $0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0$ is exact and $\mathcal{E}', \mathcal{E}''$ are semistable of slope λ, then so does $\mathcal{E}$. ⌟

Proof: Use $F(f)$ to find the "coimage" A and the "image" B of f, then there is a map from $F(A)$ to $F(B)$ which is an isomorphism, but they have the same degree and rank, thus $A \cong B$ by the last axiom. And the image must has slope λ. Then $\ker(f), \mathrm{Coker}(f)$ all can be defined, and they have the same slope λ by(4.3.4.19).

$\ker(f)$ is semistable because strict subobjects of $\ker(f)$ are also strict subobjects of $\mathcal{E}$(4.3.4.2). And for $\mathrm{Coker}(f)$, if it is not semistable, choose $\overline{\mathcal{F}'} \subset \mathrm{Coker}(f)$ that has slope$> \lambda$, let $\mathcal{F}'$ be the inverse image, then $0 \to \mathrm{Im}(f) \to \mathcal{F}' \to \overline{\mathcal{F}'} \to 0$, then by(4.3.4.19) $\mathrm{slope}(\mathcal{F}') > \lambda$, contradicting the semi-stability of $\mathcal{F}$.

For the extension, $\mathrm{slope}(\mathcal{E}) = \lambda$ by(4.3.4.19), and for a strict subobject $\mathcal{F}$ of $\mathcal{E}$, then we can find F', F'' be strict objects of $\mathcal{E}'$, $\mathcal{E}''$ respectively that there is an exact sequence $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$?, which shows $\mathrm{slope}(\mathcal{F}) \le \lambda$, so $\mathcal{E}$ is semistable. □

Harder-Narasimhan Filtration

Lemma (4.3.4.11) [Final Subobjects of Maximal Slope]. Let X be an object of $\mathcal{C}$ and X', X'' its subobjects of maximal slope, then $X' + X''$ and $X' \cap X''$ are also of maximal slope. ⌟

Proof: Cf.[Jon20]P8. □

Def. (4.3.4.12). Given an object X of $\mathcal{C}$, consider the following condition on a nonzero subobject X' of X:

For all subobjects X'' of X properly containing X', $\mu(X'') < \mu(X')$. ⌟

Def. (4.3.4.13) [SCSS]. Let X' be a subobject of X, then the following conditions are equivalent:

- X' satisfies condition(4.3.4.12) and is semistable.
- X' satisfies condition(4.3.4.12) and is of maximal slope.
- X' is the final object of X of maximal slope.

If X' satisfies these equivalent conditions and $X' \neq X$, then X is called a **strongly contradicting semi-stability** or SCSS of X. ⌟

Proof: Cf.[Jon20]P8. □

Prop. (4.3.4.14). Every object X of $\mathcal{C}$ admits a SCSS. ⌟

Def. (4.3.4.15) [Harder-Narasimhan Filtration]. Let $\mathcal{E} \in \mathcal{C}$, a chain of strict objects $0 \subset \mathcal{E}_0 \subsetneq \mathcal{E}_1 \subsetneq \ldots \subsetneq \mathcal{E}_m = \mathcal{E}$ is called a **Harder-Narasimhan filtration** iff each quotient $\mathcal{E}_i/\mathcal{E}_{i-1}$ is semistable of slope λ_i and $\lambda_1 > \lambda_2 > \ldots > \lambda_m$. ⌟

Prop. (4.3.4.16) [Faltings]. Every object $\mathcal{E} \in \mathcal{C}$ has a unique functorial Harder-Narasimhan filtration. ⌟

Proof: For uniqueness: if there are two filtrations, it suffices to show that $\mathcal{E}'_1 = \mathcal{E}_1$, because notice by(4.3.4.2) $\mathcal{E}_i$ is a strict subobjects of $\mathcal{E}_j$ for any $i < j$, so we finish by induction on the length of the filtration and considering $\mathcal{E}/\mathcal{E}_1$.

For this, firstly $\lambda_1 = \lambda'_1$, suppose the contrary and $\lambda_1 > \lambda'_1$, then $\lambda_1 > \lambda'_i$ for each i, so $\mathrm{Hom}(\mathcal{E}_1, \mathcal{E}'_i/\mathcal{E}'_{i-1}) = 0$ for each i by(4.3.4.32), so by induction $\mathrm{Hom}(\mathcal{E}_1, \mathcal{E}) = 0$, contradiction.

Next by the same reason as in the proof above, $\mathcal{E}_1 \hookrightarrow \mathcal{E}$ has image in $\mathcal{E}'_1$, and the reverse is true for $\mathcal{E}'_1$, so $\mathcal{E}_1 \cong \mathcal{E}'_1$ in $\mathcal{E}$.

For existence: Use induction on $\mathrm{rank}(\mathcal{E})$. If $\mathcal{E}$ is semistable, then we finish. Otherwise, there is a strict subobject $\mathcal{F}$ and $0 \to \mathcal{F} \to \mathcal{E} \to \mathcal{G} \to 0$ that $\mathrm{slope}(\mathcal{F}) > \mathrm{slope}(\mathcal{E})$, so $\mathrm{rank}(\mathcal{F}), \mathrm{rank}(\mathcal{G}) < \mathrm{rank}(\mathcal{E})$. Now by induction $\mathcal{F}$ and $\mathcal{G}$ has HN-filtration, thus by argument as above, we see that $\mathcal{E}$ cannot have strict subobject with slope bigger than slopes appearing in the HN-filtration of $\mathcal{F}, \mathcal{G}$. So if we choose a strict subobject of $\mathcal{E}_1$ of maximal rank among the strict subobjects of maximal slope, we claim the subobjects of $\mathcal{E}/\mathcal{E}_1$ all have slopes smaller than $\mathrm{slope}(\mathcal{E}_1)$: if some $\mathrm{slope}(\mathcal{G}) \geq \mathrm{slope}(\mathcal{E}_1)$, consider its inverse image $\mathcal{G}'$, then $0 \to \mathcal{E}_1 \to \mathcal{G}' \to \mathcal{G} \to 0$, thus $\mathrm{slope}(\mathcal{G}') \geq \mathrm{slope}(\mathcal{E}_1)$ and has bigger rank, contradiction. So we can use induction on $\mathcal{E}/\mathcal{E}_1$. □

HN-Polygons

Harder-Narasimhan Categories

This subsection is unnecessary. Main references are [Harder-Narasimhan Categories]

Def. (4.3.4.17) [Harder-Narasimhan Categories]. A **Harder-Narasimhan category** consists of a geometric exact category $(\mathcal{C}, \mathcal{E}, A)$(4.8.2.4) consists of

1. A function $\deg : Ob(\mathcal{C}_A) \to \mathbb{R}$ that is additive w.r.t short exact sequences in $\mathcal{E}_A$.
2. A function rank: $Ob(\mathcal{C}) \to \mathbb{N}$ on $\mathcal{A}$ that is additive w.r.t short exact sequences in $\mathcal{E}$, $\operatorname{rank}(X) = 0 \iff X = 0$.

The **slope** of a nonzero object X is defined to be $\mu(X) = \deg(X)/\operatorname{rank} X$. And $\mathcal{X}$ is called **semistable of slope** λ iff $\mu(X) = \lambda$, and $\mu(X') \le \lambda$ for any nonzero geometric subobject $X' \subset X$.

And the category satisfies the following axiom:

- **NH**: For any nonzero geometric object X, there exists a geometric subobject $X_{des} \subset X$ that

$$\mu(X_{des}) = \sup\{\mu(Y) | Y \text{is a non-zero geometric subobject of } X\}$$

and moreover, any nonzero geometric subobject Z of X that $\mu(Z) = \mu(X_{des})$ is a geometric subobject of X_{des}.

Notice that X_{des} is semistable and unique up to isomorphisms, called the **destablization** of X. ⌟

Cor. (4.3.4.18). A geometric object of rank 1 is semistable. ⌟

Proof: For any nonzero geometric subobject $X' \subset X$, $\operatorname{rank} X' = \operatorname{rank} X = 1$, so $\operatorname{rank} X/X' = 0$ hence $X/X' = 0$ and $X' \cong X$. Then clearly $\mu(X') = \mu(X)$ and X is semistable. □

Cor. (4.3.4.19). If $0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0$ be a short exact sequence in $\mathcal{E}_A$, then:

- If two of them have the same slope, then so does the third.
- If two of them have different slope, then we know the ordering of these slopes.

⌟

Proof: Just notice that the degree and rank are all additive functions. □

Prop. (4.3.4.20) [Abelian Categories as Harder-Narasimhan Categories]. Let $(\mathcal{C}, \mathcal{E}, A)$ be a geometric exact category with functions deg and rank, and $\mathcal{C}$ is an Abelian category, $\mathcal{E}$ is the set of short exact sequences, then $(\mathcal{C}, \mathcal{E}, A, \deg, \operatorname{rank})$ is a Harder-Narasimhan category. ⌟

Proof: We need to check HN: induct on $\operatorname{rank} X$: The condition is clear when X is semistable, in particular when $\operatorname{rank} X = 1$(4.3.4.18), and when X is not semistable, let Y be a geometric subobject of X that $\mu(X') > \mu(X)$ and $\operatorname{rank} X'$ is maximal, then by induction hypothesis, there is a destablization Y_{des}, and we want to show X'_{des} is just X_{des}: Let Y be a nonzero geometric subobject of X. If Y is a geometric subobject of X', then $\mu(Y) \le \mu(X'_{des})$. If Y is not a geometric subobject of X', then $Y + X'$ is greater than X', and $\operatorname{rank}(Y + X') > \operatorname{rank} X'$, so by maximality, $\mu(Y + X') \le \mu(X) < \mu(X')$. Moreover, there is an exact sequence

$$0 \to Y \cap X' \to Y \oplus X' \to Y + X' \to 0$$

so

$$\begin{aligned}\deg Y &= \deg(Y \cap X') + \deg(Y + X') - \deg(X')\\ &< \mu(X'_{des}) \operatorname{rank}(Y \cap X') + \mu(X')(\operatorname{rank}(Y + X') - \operatorname{rank}(X'))\\ &\le \mu(X'_{des})(\operatorname{rank}(Y \cap X') + \operatorname{rank}(Y + X') - \operatorname{rank}(X'))\\ &= \mu(X'_{des}) \operatorname{rank}(Y).\end{aligned}$$

In particular, if $\mu(Y) = \mu(X'_{des})$, then Y must be a geometric subobject of X' hence a geometric subobject of X'_{des}. so HN holds for X. □

Def. (4.3.4.21) [Harder-Narasimhan Filtration]. Let $\mathcal{X}$ be a nonzero geometric object, a chain of admissible monomorphisms $0 = X_0 \to X_1 \to \ldots \to X_m = X$ is called a **Harder-Narasimhan filtration** of X iff each quotient $\mathcal{E}_i/\mathcal{E}_{i-1}$ are all semistable of slope λ_i and $\lambda_1 > \lambda_2 > \ldots > \lambda_m$, called the slopes associated to X. ⌟

Prop. (4.3.4.22) [Harder-Narasimhan Filtrations Exist]. Let $(\mathcal{C}, \mathcal{E}, A, \deg, \mathrm{rank})$ be a Harder-Narasimhan category, then the Harder-Narasimhan filtration exists for any nonzero geometric object X. ⌟

Proof: We induct on the rank of X: if X is semistable, this is clear, so we are done in the case $\mathrm{rank}\, X = 1$ by(4.3.4.18). We choose $X_1 = X_{des}$, then X_{des} is semistable and $X' = X/X_{des} \neq 0$. Now $\mathrm{rank}\, X' < \mathrm{rank}\, X$, we can apply induction hypothesis to obtain a HN-filtration $0 = X'_1 \xrightarrow{f'_1} X'_2 \to \ldots \to X'_{n-1} \xrightarrow{f'_{n-1}} X'_n = X'$. Now let $X_i = X \times_{X'} X'_i$(exists by Ex6(4.8.2.1)), then $X_1 = X_{des}$. Since $X \to X'$ is an admissible epimorphism, $X_i \to X'_i$ are also admissible epimorphisms, and there are Cartesian diagrams

$$\begin{array}{ccc} X_i & \xrightarrow{f_i} & X_{i+1} \\ \downarrow{\scriptstyle \pi_i} & & \downarrow{\scriptstyle \pi_{i+1}} \\ X'_i & \xrightarrow{f'_i} & X'_{i+1} \end{array}$$

and f_i are monomorphisms, so f_i is the kernel of $X_{i+1} \to X'_{i+1}/X'_i$, which is an admissible epimorphism, so f_i is admissible. There are natural isomorphisms $\varphi_i : X_{i+1}/X_i \to X'_{i+1}/X'_i$(? Cf.[Harder-Narasimhan Filtrations]), and axiom A6(4.8.2.4) shows φ is compatible with the geometric structure, so X_{i+1}/X_i are all semistable, and notice

$$\mu(X_2/X_1) = \frac{\mathrm{rank}(X_2)\mu(X_2) - \mathrm{rank}(X_1)\mu(X_1)}{\mathrm{rank}(X_2) - \mathrm{rank}(X_1)} < \mu(X_1)$$

so $0 \to X_1 \to X_2 \to \ldots \to X_m = X$ is a HN-filtration for X. □

Prop. (4.3.4.23) [HN-Formalism for Filtrations in an Abelian Category]. Let $\mathcal{C}$ be an Abelian category and $\mathcal{E}$ the set of all short exact sequences in $\mathcal{C}$, $A(X)$ is the set of isomorphism classes of filtrations on X, then $(\mathcal{C}, \mathcal{E}, A)$ is a geometric exact category, by(4.8.2.8), given any additive rank function on $\mathcal{C}$, and define a degree function for any filtration $\mathcal{F} = (X_\lambda)$ as

$$\deg(\mathcal{F}) = \int_{\mathbb{R}} \lambda(d\,\mathrm{rank}\, X_\lambda),$$

then deg is additive w.r.t short exact sequences of filtrations, and $(\mathcal{C}, \mathcal{E}, A, \deg, \mathrm{rank})$ is a Harder-Narasimhan filtration.

Then a filtration is semistable iff it has only one jump. Then the HN-filtration of a filtration is just the jump set ordered decreasingly. ⌟

Prop. (4.3.4.24) [HN Formalism for Vector Spaces with Two Norms]. The vector spaces with two norms is a Harder-Narasimhan category, Cf.[Harder-Narasimhan Filtrations, P9]. ⌟

Prop. (4.3.4.25) [HN-Formalism for Torsion-Free Sheaves]. The category of torsion-free sheaves on a geometrically normal projective variety of dimension $d \geq 1$ over a field K is a Harder-Narasimhan category. Cf.[Harder-Narasimhan Filtrations, P10]. ⌟

Prop. (4.3.4.26) [HH-Formalism for Hermitian Adelic Bundle]. Let K be a number field, then the category of Hermitian adelic bundle over K is a Harder-Narasimhan category. Cf.[Harder-Narasimhan Filtrations, P10]. ⌟

Prop. (4.3.4.27) [HN Formalism for Filtered Vector Spaces Field]. If L/K is a field extension, there is a category $VectFil_{L/K}$ consisting of (V, Fil) where V is a K-vector space and Fil is a (finite) filtration of vectors spaces over L on $V \otimes_K L$(4.3.3.1). It is a geometric exact category by(4.8.2.8) and a Harder-Narasimhan category by(4.3.4.20).

The rank is as usual, and the degree is defined to be

$$\deg((V, Fil)) = \int_{\mathbb{R}} \lambda(d \operatorname{rank} V_\lambda)\text{(4.3.4.23)}$$

⌟

Slope Inequalities and Functoriality

Def. (4.3.4.28) [Additional Conditions]. In this subsubsection, we assume the Harder-Narasimhan filtration satisfies the following axiom that is ⌟

Def. (4.3.4.29) [Slope Inequality Axioms]. To show the functoriality of the Harder-Narasimhan filtration, we need the following axiom:

- (SI): If X_1, X_2 are two semistable geometric objects that $\mu(X_1) > \mu(X_2)$, then there are no non-zero morphism from X_1 to X_2 compatible with the geometric structures(4.8.2.5).

⌟

Prop. (4.3.4.30). If SI holds, then ⌟

Prop. (4.3.4.31). If $\mathcal{E}$ is semistable of slope λ, then for any morphism $u : \mathcal{E} \to \mathcal{E}''$ that $F(u)$ is an isomorphism, slope$(\mathcal{E}'') \geq \lambda$. ⌟

Proof: Take the kernel of $F(u)$ in $\mathcal{A}$, which corresponds to a strict object $\mathcal{E}'$ of $\mathcal{E}$, and $0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0$ is exact, so we can use(4.3.4.19). □

Cor. (4.3.4.32). If $\mathcal{E}, \mathcal{F}$ are semistable of slopes $\lambda > \mu$, then $\mathrm{Hom}_{\mathcal{C}}(\mathcal{E}, \mathcal{F}) = 0$. ⌟

Prop. (4.3.4.33) [Semistable Vector Bundles Form a Weak Serre Subcategory]. If $f : \mathcal{E} \to \mathcal{F}$ be a map of vector bundles of the same slope λ, then $\ker(f)$ and $\mathrm{Coker}(f)$ are all semistable vector bundles of slope λ, and if $0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0$ is exact and $\mathcal{E}', \mathcal{E}''$ are semistable of slope λ, then so does $\mathcal{E}$. ⌟

Proof: Use $F(f)$ to find the "coimage" A and the "image" B of f, then there is a map from $F(A)$ to $F(B)$ which is an isomorphism, but they have the same degree and rank, thus $A \cong B$ by the last axiom. And the image must has slope λ. Then $\ker(f), \mathrm{Coker}(f)$ all can be defined, and they have the same slope λ by(4.3.4.19).

$\ker(f)$ is semistable because strict subobjects of $\ker(f)$ are also strict subobjects of $\mathcal{E}$(4.3.4.2). And for $\mathrm{Coker}(f)$, if it is not semistable, choose $\overline{\mathcal{F}'} \subset \mathrm{Coker}(f)$ that has slope$> \lambda$, let $\mathcal{F}'$ be the inverse image, then $0 \to \mathrm{Im}(f) \to \mathcal{F}' \to \overline{\mathcal{F}'} \to 0$, then by(4.3.4.19) slope$(\mathcal{F}') > \lambda$, contradicting the semi-stability of $\mathcal{F}$.

For the extension, slope$(\mathcal{E}) = \lambda$ by(4.3.4.19), and for a strict subobject $\mathcal{F}$ of $\mathcal{E}$, then we can find F', F'' be strict objects of $\mathcal{E}'$, $\mathcal{E}''$ respectively that there is an exact sequence $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$?, which shows slope$(\mathcal{F}) \leq \lambda$, so $\mathcal{E}$ is semistable. □

4.4 Topology I

Main references are [Mun00], [Mor19], [Jec03].

1 Basics

Def. (4.4.1.1) [Topological Spaces]. ⌟

Def. (4.4.1.2) [Continuous Functions]. For $X, Y \in \mathcal{T}\mathrm{op}$, a map $f : X \to Y$ is called a **continuous map** if for any open subset $U \subset Y$, $f^{-1}(U) \subset X$ is also open. ⌟

Def. (4.4.1.3) [Limits]. For $X \in \mathcal{T}\mathrm{op}$, and $(x_n)_{n\in\mathbb{Z}} \subset X$, $y \in X$ is called a **limit of sequence** if for any open subset $y \in U \subset X$, there exists some $N_U \in \mathbb{Z}_+$ s.t. for any $N > N_U$, $X_N \in U$.

Let $S \subset X$ be a subspace, then $x \in X$ is called a **limit point** of $S \subset X$ if for any open subset $x \in U \subset X$, $(U \cap S) \setminus \{x\} \neq \varnothing$.

$x \in X$ is called an **isolated point** of X if x is not a limit point of $X \subset X$. Equivalently, $\{x\} \subset X$ is open. A closed subspace of X without isolated points is called a **perfect subspace**. ⌟

Def. (4.4.1.4) [Semicontinuous Functions]. A function from $X \to [-\infty, \infty]$ is called **upper semicontinuous** iff $f^{-1}([-\infty, a))$ are all open. It is called **lower semicontinuous** iff $f^{-1}((a, \infty])$ are all open. ⌟

Def. (4.4.1.5) [Separable Topological Spaces]. A topological space is called **separable** if it has a countable dense subset. ⌟

Def. (4.4.1.6) [Product Topology]. Arbitrary product exists in the category of topological spaces. It is constructed as follows: for a family of topology spaces X_i indexed over an index set I, the product $\prod_I X_i$ is the set-theoretic product endowed with the topology generated by the basis $\pi_i^{-1}(U_i)$ for U_i open in X_i. ⌟

Prop. (4.4.1.7) [Limits and Colimits]. Arbitrary limits and colimits exist in the category of topological spaces. The limits is given as a subspace of the product topology, and the colimits $X = \operatorname{colim} X_i$ is given a topology that $U \subset X$ is open iff $U \cap X_i$ is open for each i. ⌟

Prop. (4.4.1.8) [Pullback Space]. Let $E \to X$ and $f : X' \to X$ be maps of spaces, then there is a pullback map $f^*E = E \times_X X' \to X'$, called the **pullback space**. ⌟

Def. (4.4.1.9) [Quotient Topology]. Let $f : X \to Y$ be a surjective map of spaces, and X has a topology, then we can define a **quotient topology** on Y that $U \subset Y$ is open iff $f^{-1}(U)$ is open in X.. It has the universal property that any continuous map $X \to Z$ that factors through f set-theoretically factors through f as a continuous map.

Such a map is called a **quotient map**. ⌟

Prop. (4.4.1.10). A surjective open map pr is a quotient map. ⌟

Proof: It is clearly that a subset U is open iff $\mathrm{pr}^{-1}(U)$ is open. □

Def. (4.4.1.11) [Glueing Space]. Let $A \subset X$ and $f : A \to Y$, then we have the glueing space $Y \coprod_f X$. ⌟

Def. (4.4.1.12) [Mapping Cylinder]. Let $f : X \to Y$ be a map, then we define the **mapping cylinder** $M(f) = Y \coprod_f X \times I$, where $X \times \{0\} \subset X \times I$ mapsto Y by f. ⌟

Def. (4.4.1.13) [Cone]. For $X \in \mathfrak{Top}$, define the **cone over** X to be the space $C(X) = (X \times \mathbb{I})/(X \times \{1\})$. Notice that $C(\varnothing) = \text{pt}$. ⌟

Def. (4.4.1.14) [Mapping Cone]. Let $f : X \to Y$ be a map, then we define the **mapping cone** $C(f) = M(f)/X \times \{1\}$. ⌟

Lemma (4.4.1.15). If $f : X \to Y$ is a surjective continuous map that $f(E) \neq Y$ for any proper closed subspace of X, then for any $U \subset X$ open, $f(U) \subset \overline{Y \backslash f(X \backslash U)}$. ⌟

Proof: Take $y \in f(U)$ and a nbhd V of y in Y, we show that V intersect $Y \backslash f(X \backslash U)$: $W = U \cap f^{-1}(V)$ is nonempty, thus $f(X \backslash W) \neq Y$, take $y' \in Y \backslash f(X \backslash W)$, then it is clear $y' \in Y \backslash f(X \backslash U)$, and $y' \in V$. □

Def. (4.4.1.16) [Locally Closed Subset]. A subset Z of X is called **locally closed** if for any $z \in Z$, there is a nbhd U of z in X that $U \cap Z$ is closed in Z. Equivalently, a locally closed subset is the intersection of an open subset with a closed subset. ⌟

Proof: An intersection of an open subset and a closed subset is clearly locally closed. Conversely, if Z is locally closed, we choose for each $z \in Z$ a nbhd U_z that $U_z \cap Z$ is closed in U_z, then we can show $Z = \overline{Z} \cap \bigcup_z U_z$. This is because if $x \in \overline{Z} \cap \bigcup_z U_z$, then $x \in U_z$ for some z, and also $x \in \overline{Z}$, thus x is in Z. □

Filter Langrange

Def. (4.4.1.17) [Convergence and Filter]. For a filter $\mathcal{F}$ on a topological space, $\mathcal{F}$ **converges** to a point y iff any open set containing y is in $\mathcal{F}$.

If X is a set and Y is a topological space and $X \to Y$ is a function, then $y \in Y$ is a **$\mathcal{F}$-limit of f** if $f_*\mathcal{F}$ converges to Y. ⌟

Prop. (4.4.1.18) [Ultrafilter Convergence Theorem]. Let X, Y be a topological space, then:

1. Y is compact iff any ultrafilter on Y has a limit point.
2. Y is Hausdorff iff any ultrafilter on Y has at most one limit point.
3. a function $f : X \to Y$ is continuous iff for any filter on X converging to x, the filter $f_*(\mathcal{F})$ converges to y.

⌟

Proof:

1. If Y is compact but every point is not a limit point, then for any x, there is an open set U_x that $U_x \notin \mathcal{F}$, but then f.m. of them covers Y, which is in $\mathcal{F}$, so one of them must be in $\mathcal{F}$ by(2.2.10.7), contradiction.
   Conversely, if $\cup_I U_i = X$ but no finite union of them cover X, then $X - U_i$ satisfies the finite intersection property, so there is an ultrafilter containing all $X - U_i$ by(2.2.10.4) and(2.2.10.5). Then clearly any point x is not a limit point of $\mathcal{F}$.
2. If Y is Hausdorff and x, y are both limit point of a filter $\mathcal{F}$, then there are two non-intersecting nbhd of them in $\mathcal{F}$, so its intersection $\varnothing \in \mathcal{F}$, contradiction.
   Conversely, if x, y are two point that their nbhds both intersect, then their nbhds together satisfies the finite intersection property, so there is an ultrafilter containing all of them, by(2.2.10.4) and(2.2.10.5), thus converging to both x and y.
3. This is an easy consequence considering the filter of all the nbhd containing x.

□

Connected Components

Def. (4.4.1.19) [Connectedness]. A space X is called **connected** if it satisfies: for any open subset U, V of X that $U \cup V = X$ and $U \cap V = \varnothing$, either $U = \varnothing$ or $V = \varnothing$.

X is called **locally connected** if there is a basis of X consisting of connected open subsets of X. ⌟

Def. (4.4.1.20) [Path-Connectedness]. A space X is called **path-connected** if any two points of X can be connected by an arc.

X is called **locally path-connected** if there is a basis of X consisting of path-connected open subsets of X. ⌟

Prop. (4.4.1.21). If X is an ordered set with the least upper bound property and satisfies: for any $x < y \in X$, there exists $z \in X$ s.t. $x < z < y$. Then X is connected, so are intervals and rays in X. ⌟

Proof: Let Y be an interval or ray in X. Suppose for contradiction $Y = A \coprod B$, where A, B are open and non-empty in Y. Choose $a \in A, b \in B$, then $[a, b] \subset Y$. Let $A_0 = A \cap [a, b]$ and $B_0 = B \cap [a, b]$, and $c = \sup A_0 \in [a, b]$.

Then $c \notin B_0$: If $c \in B_0$, then $c \neq a$, and because B_0 is open, there exists some $a \leq d < c$ s.t. $(d, c] \subset B_0$. So d is a smaller upper bound for A_0, contradiction.

And also $c \notin A_0$: If $c \in A_0$, then $c \neq b$, and because A_0 is open, there exists some $c < e \leq b$ s.t. $[c, e) \subset A_0$. Then by hypothesis, there exists $z \in (c, e) \subset A_0$, contradicting the fact c is an upper bound for A_0.

Then we derived a contradiction that $c \notin Y$, which proves Y is connected. □

Def. (4.4.1.22) [Connected Components]. In a topological space X, if $x \in X$, the **connected component** of x is the maximal connected subspace of X containing x. The **path-connected component** of x is the maximal path-connected subspace of X containing x ⌟

Prop. (4.4.1.23).

- Any connected component of X is closed.
- If X is locally connected, then any connected component of X is clopen.
- If X is locally path-connected, then any path-connected component of X is open, and any connected component is also open.

⌟

Prop. (4.4.1.24) [Clopen Subsets and Connected Components]. Let X be a normal topological space and $x \in X$, then the connected component of X containing x is the intersection of clopen subsets containing x, denoted by A. ⌟

Proof: Assume A splits into two components B, D. Since A is closed, B and D are both closed, because X is normal there are disjoint open neighborhoods U and V around B and D, respectively. The open sets U and V cover the intersection of all clopen neighborhoods of A, so cause X is compact, there must exist a finite number of clopen sets around A, say $A_1, \ldots, A_n$ such that $U \cup V$ covers $K = \bigcap_1^n A_i$.

Note that K is clopen. We can assume that $x \in U$. It is not difficult to see that $K \cap U$ is clopen and does not contain all of A, contradicting the definition of A. □

Cor. (4.4.1.25). For a compact Hausdorff topological space X and a point $x \in X$, the connected component of X containing x is the intersection of all compact open neighborhoods of x, because X is normal(4.4.7.6). ⌟

Def. (4.4.1.26) [Totally Disconnected Space]. A space is called **totally disconnected** iff any connected subset of X contains only one point. ⌟

Prop. (4.4.1.27). A subspace of a totally disconnected space is totally disconnected, because totally disconnected is equivalent to the only connected subsets are pt sets. ⌟

Def. (4.4.1.28) [Contor Sets, Brouwer]. A **Contor set** is a nonempty, perfect, compact, metrizable and zero dimensional topological space. Equivalently, it is a topological space homeomorphic to the classical Contor ternary set. ⌟

Proof: □

Extremally Disconnected Space

Def. (4.4.1.29) [Extremally Disconnected Space]. A topological space S is called **extremally disconnected** if the closure of any open subset of X is open. ⌟

Prop. (4.4.1.30). Let X be an extremally disconnected space, If U, V are disjoint open subsets of X, then $\overline{U}, \overline{V}$ ⌟

Proof: Because $V \cap \overline{U} = \varnothing$, thus similarly $\overline{V} \cap \overline{U} = \varnothing$. □

Lemma (4.4.1.31). Let $f : X \to Y$ be a continuous surjective map of compact Hausdorff spaces that Y is extremally disconnected and $f(Z) \neq Y$ for any proper closed subspace of X, then f is a homeomorphism. ⌟

Proof: By(4.4.2.11) it suffices to show that f is injective. Suppose $f(x) = f(x') = y$, then choose disjoint nbhd U, U' of x, x', and $T = f(X \backslash U), T' = f(X \backslash U')$ closed in Y, then $Y = T \cup T'$ and y is contained in the closure of $Y \backslash T$ and $Y \backslash T'$ by(4.4.1.15), but this contradicts(4.4.1.30). □

Prop. (4.4.1.32) [Projective Spaces]. Compact Hausdorff extremally disconnected spaces are exactly the projective objects in the category of compact Hausdorff spaces. ⌟

Proof: Assume X is projective, let $U \subset X$ be open, and the complement by Z, then consider the surjection $\overline{U} \coprod Z \to X$, and let σ be the projection, then $\sigma(U) \subset \overline{U}$, thus $\sigma^{-1}(\overline{U}) = \overline{U}$, and it is open.

Conversely, if X is extremally disconnected, then by(4.4.2.13), there is a compact subset $E \subset Y$ that $f(E) = X$ and $f(E') \neq X$ for all closed subspace $E' \subset E$. Then(4.4.1.31) says $f|_E$ is a homeomorphism, and the inverse of it gives a desired section. □

Prop. (4.4.1.33) [Gleason]. In an extremally disconnected space X, a convergent sequence is eventually constant. In particular, $\mathbb{Z}_p$ is a profinite group that is not extremally disconnected. ⌟

Proof: Cf.[Projective Topological Spaces] □

2 Compactness

Def. (4.4.2.1) [Quasi-Compact Space]. A topological space is called **compact** or **quasi-compact** iff any open covering of it has a finite sub-covering. A subspace of a topological space is called **precompact** if its closure is compact. ⌟

Def. (4.4.2.2) [Quasi-Compact Morphism]. A map of topological spaces is called a **quasi-compact morphism** if the inverse image of any quasi-compact open subset is quasi-compact open. ⌟

Prop. (4.4.2.3) [Alexander Subbase Theorem]. A topological space is compact iff the closed subsets has the finite intersection property(2.2.10.3). In fact, it suffices to show that the family of complements of a subbasis of open sets has the finite intersection property. ⌟

Proof: Cf.[Sta]08ZP. □

Prop. (4.4.2.4). Let X be a totally ordered set with the least upper bound property, then each closed interval of X is compact in the order topology. In particular, this applies to a complete totally ordered set X(2.2.3.22). ⌟

Proof: Let $a < b$ and $\mathcal{U}$ a covering of $[a, b]$. We first show that for any $x \in [a, b)$, there exists some $x < y \le b$ that $[x, y]$ can be covered by at most two elements of $\mathcal{U}$: If x has an immediate successor, then take y to be it. If x has no immediate successor, choose an element U of $\mathcal{U}$ containing x, then U contains some $[x, c)$. Choose $y \in [x, c)$, then $[x, y]$ is covered by a single element of $\mathcal{U}$.

Now let C be the set of points $y \in (a, b]$ that $[a, y]$ can be covered by f.m. elements of $\mathcal{U}$. We showed before this set is non-empty. Let c be the least upper bound of C, then $a < c \le b$.

Next, we show $c \in C$: take an element U of $\mathcal{U}$ containing c, then U contains some $(d, c]$. There must be some element of C lying in the interval $(d, c]$, otherwise d is an upper bound of C. Then $[a, y]$ is covered by f.m. elements of $\mathcal{U}$, so $c \in C$.

Finally, we show $c = b$, but this is because otherwise we can find $c < y \le b$ that $[c, y]$ is covered by 2 elements, thus $y \in C$, so $y \le c$, contradiction. □

Prop. (4.4.2.5) [Tychonoff]. An arbitrary direct product of compact topological spaces is compact. ⌟

Proof: We prove the finite intersection property. If A is a family of subsets that any finite intersection of closure of them is nonempty, then consider a maximal family $\mathfrak{D}$ of subsets containing A that any finite intersection of closures of them is nonempty, it exists by Zorn's lemma. Consider the projection of $\mathfrak{D}$ onto a coordinate, then by Hypothesis, it has an intersection x_α. Now we want to show $x = (x_\alpha)$ belongs to each $D \in \mathfrak{D}$.

If U_β is any subbasis element containing x, then U_β intersect each $\mathfrak{D}$ because $x_\beta \in \pi_\beta(D)$, so it is in $\mathfrak{D}$, by maximality of $\mathfrak{D}$. So the finite intersections are also in $\mathfrak{D}$, so all local basis of x are in $\mathfrak{D}$. This means that local basis intersect each element of $\mathfrak{D}$, that is, all closure of elements in $\mathfrak{D}$ contains x. □

Def. (4.4.2.6) [Sequentially Compact]. A subset A in a space X is called **sequentially compact** iff any sequence of points in A has a convergent subsequence in X. It is called **self sequentially compact** if it is sequentially compact in itself. ⌟

Prop. (4.4.2.7). $f : X \to Y$, X is compact and Y is Hausdorff, then for a descending chain Y_i of closed subsets of X,

$$f(\bigcap_n Y_n) = \bigcap_n f(Y_n).$$

⌟

Proof: The left side is compact, so if $x \notin f(\bigcap_n Y_n)$, there is a closed subsets $x \in T$ that $T \cap f(\bigcap_n Y_n)$=0, so $f^{-1}(T)\bigcap_n Y_n = 0$, so $f^{-1}(T) \cap Y_n = 0$ for some n, hence $x \notin f(Y_n)$. □

Prop. (4.4.2.8) [Fixed Point Theorem]. If X is a compact metric space M, T is a continuous map $X \to X$ that $d(x,y) < d(Tx,Ty)$, then T has a unique fixed point in X. ⌟

Proof: The uniqueness is obvious, for the existence, first notice T is obviously continuous, so consider $d(x,Tx)$, this is a continuous function on M, so it contains a minimum value, if it not 0, then $d(Tx,T^2x) < d(x,Tx)$, which is a contradiction. □

Def. (4.4.2.9) [Proper Map]. A **proper map** is a continuous map s.t. the inverse image of compact subsets are compact. ⌟

Prop. (4.4.2.10). If X is compact and Y is Hausdorff, then a continuous map $f : X \to Y$ is proper. ⌟

Cor. (4.4.2.11). A continuous bijective map from a compact space to a Hausdorff space is a homeomorphism. ⌟

Prop. (4.4.2.12) [Proper Continuous Maps Closed]. Let $f : X \to Y$ be a proper continuous map with Y locally compact Hausdorff, then f is a closed map. ⌟

Proof: Let $K \subset X$ closed, and $y \in \overline{f(K)}$. Choose precompact open nbhd U of y, then $f^{-1}(\overline{U})$ is compact in X, so $f(K \cap f^{-1}(\overline{U})) = f(K) \cap \overline{U}$ is compact and thus closed in Y. Then $y \in f(K)$, and $f(K)$ is closed. □

Lemma (4.4.2.13). Let $f : X \to Y$ be a continuous map of compact Hausdorff spaces, then there exists a smallest closed subset E of X that $f(E) = Y$. ⌟

Proof: Use Zorn's lemma, noticing that the intersection of a chain of possible E_is also maps to Y, by the intersection property(4.4.2.3). □

Stone-Čech Compactification

Def. (4.4.2.14) [Stone-Čech Compactification]. The **Stone-Čech Compactification** β is defined to be a functor from the category of sets to the category of compact Hausdorff space that is left adjoint to the forgetful functor.

The construction of $\beta(X)$ is as follows: βX =the set of all ultrafilters on X, and the topology is generate by $U_A = \{\mathcal{F} | A \in \mathcal{F}\}$ as a basis of clopen subsets. For a map $f : X \to Y$, the map $\beta X \to \beta Y$ is given by f_*. ⌟

Proof: First βX is a compact Hausdorff space: it is compact because if there are sets A_i that any ultrafilter contains at least one of them, then f.m. of them must cover X, otherwise $X - A_i$ satisfies the finite intersection property thus is contained in some ultrafilter, by(2.2.10.4) and(2.2.10.5), contradiction, Then by(2.2.10.7) shows that any ultrafilter contains one of them. It is Hausdorff because for any two different ultrafilter, there must be an A that $A \in \mathcal{F}_1$ and $X - A \in \mathcal{F}_2$. f_* is continuous because $f^{-1}(U_A) = U_{f^{-1}(A)}$.

Now for any map $f : X \to Y$ where Y is a topological space, map an ultrafilter $\mathcal{F}$ to the unique limit point of $f_*\mathcal{F}$ in Y(existence and uniqueness by(4.4.1.18)). This map is continuous from βX to Y because for any open set $V \subset Y$, $U_{f^{-1}(V)}$ is mapped into V. And for any $\beta X \to Y$ continuous, consider $X \to Y$ which maps x to the image of the principle ultrafilter $\mathcal{F}_x$ in Y.

This two map are mutually converses to each other, first for a $f : X \to Y$, $X \to \beta X \to Y$ is f itself, because the pushout of the principle ultrafilter clearly converges to $f(x)$. And for a $\beta X \to Y$, if $\mathcal{F}$ doesn't map to $\lim f_*\mathcal{F}$ but mapped to some t, then by definition, there is a nbhd U of t that $f^{-1}(U) \notin \mathcal{F}$, but by continuity, there is a $\mathcal{F} \in U_B$ mapped into U. But then $B \in f^{-1}(U)$, otherwise if $x \in B - f^{-1}(U)$, then $\mathcal{F}_x$ is mapped to U, contradiction, so $f^{-1}(U)$ containing B is also in $\mathcal{F}$, contradiction. □

Lemma (4.4.2.15). In fact, the spaces in the image of the Stone-Čech compactification are all profinite spaces. ⌟

Proof: As shown before, for any two different ultrafilter, there must be an A that $A \in \mathcal{F}_1$ and $X - A \in \mathcal{F}_2$, U_A is open and closed. □

Prop. (4.4.2.16) [Stone Representation Theorem]. The Stone-Čech compactification β gives an equivalent of categories from the category of Boolean algebras to the category of profinite spaces. ⌟

Proof: βB is a profinite space by lemma(4.4.2.15), and B can be recovered from βB as the Boolean algebra of all clopen subsets of βB, because βB is compact. This is a inverse isomorphism because**?**. □

Prop. (4.4.2.17). The Stone-Čech compactification of a set βS_0 is extremally disconnected. ⌟

Proof: We check condition(4.4.1.32): For any surjection $S' \to \beta S_0$, we may take a lift $S_0 \to S$ arbitrarily, then by definition there is a morphism $\beta S_0 \to S'$ extending this morphism. It is a section by the universal property. □

Locally Compact Space

Def. (4.4.2.18) [Locally Compact Space]. A Hausdorff space is called **locally compact** if for any point x, there is a compact subset containing a nbhd of x. ⌟

Prop. (4.4.2.19). If X is Hausdorff, then X is locally compact iff for any $x \in X$ and $x \in U$ open, there exists a precompact nbhd V that $x \in V \subset \overline{V} \subset U$. ⌟

Proof: One direction is trivial. For the other, for any $x \in X$ and a nbhd U of x, let U_0 be a precompact nbhd of X, then $\overline{U}_0 \backslash U$ is closed thus compact and disjoint from x. Because X is Hausdorff, we can find a nbhd V' of x that $\overline{V'}$ is disjoint from $\overline{U}_0 \backslash U$. Now let $V = V' \cap U_0$, then $\overline{V} \subset \overline{U}_0$ is closed thus compact, and $\overline{V} \subset \overline{V'} \cap \overline{U}_0 \subset U$. □

Cor. (4.4.2.20). Open subsets and closed subsets of a locally compact Hausdorff space X is locally compact Hausdorff. ⌟

Proof: If $A \subset X$ is closed and $x \in A$, then there exists a precompact nbhd U of $x \in X$, then $A \cap \overline{U}$ is closed in $\overline{U}$ thus compact, and contains the nbhd $U \cap A$ of $x \in A$, so A is locally compact.

If $A \subset X$ is open, $x \in A$, let $x \in U \subset A$, and U open in X, then we can apply(4.4.2.19) to find a precompact nbhd V that $x \in V \subset \overline{V} \subset U$, so A is locally compact. □

Prop. (4.4.2.21) [One-Point Compactification]. Let X be a space, then X is locally compact Hausdorff iff there exists a compact Hausdorff space Y containing X s.t. $Y \backslash X$ is a single point. Moreover, in this case, Y is unique up to homeomorphisms, called the **one-point compactification** of X. ⌟

Proof: Cf.[Mun00]P183. □

Cor. (4.4.2.22). A space X is homeomorphic to an open subset of a compact open subspace iff it is locally compact Hausdorff, by(4.4.2.21) and(4.4.2.20). ⌟

Prop. (4.4.2.23). A locally compact second countable Hausdorff space X has a countable basis consisting of precompact open subsets. In particular, X is σ-compact. ⌟

Proof: Choose a countable basis $\{U_n\}$ of X. For any $x \in X$ and any nbhd U of x, there exists a precompact $U_x \subset U$ containing x by(4.4.2.19). Then for some $n(x)$, $U_{n(x)} \subset U_x$ containing x, so $U_{n(x)}$ is precompact. Thus the set of U_n that is precompact forms a countable basis of X. □

Prop. (4.4.2.24). If $f : X \to Y$ is a quotient map and Z is locally compact, then $X \times Z \to Y \times Z$ is also a quotient map. ⌟

Proof: Consider W as $Y \times Z$ in the quotient map topology, then $X \times Z \to W$ is continuous, which means $X \to \mathrm{Map}(Z, W)$ is continuous. But then $Y \to \mathrm{Map}(Z, W)$ is continuous because Y is a quotient map. Applying(4.4.3.7), we see $Y \times Z \to W$ is continuous. $W \to Y \times Z$ is continuous by quotient map hypothesis, so $Y \times Z \cong W$. □

Compactly Generated Spaces

Def. (4.4.2.25) [Compactly Generated Spaces]. A **compactly generated space** is a space that is the colimit of its compact Hausdorff subspaces. The category of compactly generated spaces is denoted by $\mathcal{CG}$. ⌟

Prop. (4.4.2.26). For $X \in \mathcal{CG}$ and $Y \in \mathcal{T}\mathrm{op}$, a set-theoretical map $f : X \to Y$ is continuous iff for any $K \in \mathcal{T}\mathrm{op}$ compact Hausdorff and a map $i : K \to X$, the composite map $K \to Y$ is continuous. ⌟

Prop. (4.4.2.27) [Compact Generating Functor]. There is a **compact generating functor** $(-)_c : \mathcal{T}\mathrm{op} \to \mathcal{CG}$ right adjoint to the inclusion functor. ⌟

Proof: k is constructed by $X \mapsto \varinjlim_{K \subset X, K \text{ compact}} K$. Notice $X_c = X$ set-theoretically. It is easy to verify that if $Y \in \mathcal{CG}$ and $Y \to X$ is continuous, then the set-theoretical map $Y \to X_c$ is also continuous. So $(-)_c$ is right adjoint to the inclusion functor. □

Cor. (4.4.2.28). $\mathcal{CG}$ is both complete and cocomplete, and the colimits coincide with colimits in $\mathcal{T}\mathrm{op}$. ⌟

Cor. (4.4.2.29). $\mathcal{CG}$ is Cartesian closed(4.1.5.7). ⌟

Cor. (4.4.2.30). The right adjoint to the Cartesian product is the compactification of the mapping space functor(4.4.3.1), by(4.4.3.6) and(4.4.2.27). ⌟

Prop. (4.4.2.31). Locally compact Hausdorff topological spaces are compactly generated. ⌟

Proof: For $X \in \mathcal{T}\mathrm{op}$, if $Z \subset X$ satisfies $Z \cap K$ is closed for any compact Hausdorff subset $K \subset X$, for any $x \in X$, there exists a precompact nbhd U of $x \in X$, so $Z \cap \overline{U}$ is closed, and $Z \cap U$ is closed in U. Thus Z is closed in X. □

Prop. (4.4.2.32). Quotients and closed subspaces of a compactly generated space are compactly generated. Colimits of compactly generated spaces are compactly generated. ⌟

Proof: These follow from(4.4.2.25). □

Prop. (4.4.2.33). If $X \in \mathcal{CG}$ and Y is locally compact Hausdorff, then $X \times Y \in \mathcal{CG}$. ⌟

Proof: Notice by(4.4.3.7), a map $X \times Y \to Z$ is continuous iff $C \times Y \to Z$ is continuous for any compact Hausdorff subset $C \subset X$. The assertion is equivalent to $X \times Y \to (X \times Y)_c$ is continuous, which is then equivalent to $C \times Y \to (X \times Y)_c$ continuous for any compact subset $C \subset X$. But Y is compactly generated, and C is locally compact, thus it suffices to show $C \times C' \to (X \times Y)_c$ is continuous for any compact subset $C' \subset Y$. Then this is true because $C \times C'$ is compact. □

3 Mapping Spaces

Compact-Open Topology on Mapping Spaces

Def. (4.4.3.1) [Compact-Open Topology]. The **compact-open topology** on a function space $\mathrm{Map}(X, Y)$ is a topology generated by the sets $(K, U) = \{f : f(K) \subset U\}$, where K is compact in X and U is open in Y. ⌟

Prop. (4.4.3.2). For $X' \to X, Y \to Y' \in \mathcal{T}op$, the induced map $\mathrm{Map}(X, Y) \to \mathrm{Map}(X', Y')$ is continuous. In particular, if $X \cong X'$ and $Y \cong Y'$, then $\mathrm{Map}(X, Y) \cong \mathrm{Map}(X', Y')$. ⌟

Prop. (4.4.3.3). If Y is compact and X a metric space, this the compact open topology on $\mathrm{Map}(Y, X)$ coincides with the uniform topology on functions. ⌟

Proof: If $f \in (K, U)$, then $f(K) \subset U$, then there is a $\varepsilon > 0$ that $B(K, \varepsilon) \subset U$, thus $B(f, \varepsilon) \subset (K, U)$.

For any $f \in \mathrm{Map}(Y, X)$, $f(Y)$ is compact thus there are f.m. open balls $B(f(y_i), \frac{\varepsilon}{3})$ that covers $f(Y)$. Now if $K_i = \overline{f^{-1}(B(f(y_i), \frac{\varepsilon}{3}))}$, then $\cup K_i = Y$, and $f \in \cap_i (K_i, B(f(y_i), \frac{\varepsilon}{2}))$. Also $\cap_i (K_i, B(f(y_i), \frac{\varepsilon}{2})) \subset B(f, \varepsilon)$, because for any $g \in \cap_i (K_i, B(f(y_i), \frac{\varepsilon}{2}))$ and $y \in K_i$, $|f(y) - g(y)| \leq |f(y) - f(y_i)| + |f(y_i) - g(y)| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$. □

Def. (4.4.3.4) [Relative Maps]. Let $A \subset X$ and $B \subset Y$, we denote by $\mathrm{Map}((X, A), (Y, B))$ the subspace of $\mathrm{Map}(X, Y)$ consisting of continuous functions $f : X \to Y$ that map A into B. ⌟

Prop. (4.4.3.5) [Composition is Continuous]. If Y is locally compact Hausdorff, then the composition map

$$\mathrm{Map}(Y, Z) \times \mathrm{Map}(X, Y) \to \mathrm{Map}(X, Z)$$

is continuous. ⌟

Proof: For any compact $K \subset X$, open $U \subset Y$ and $g \circ f \in (K, U)$, $f(K) \subset g^{-1}(U) \subset Y$. Because Y is locally compact, there is an precompact open subset V that $f(K) \subset V \subset \overline{V} \subset g^{-1}(U)$, then $(\overline{V}, U) \times (K, V)$ maps into (K, U). □

Lemma (4.4.3.6) [Subbasis]. Let X be Hausdorff, W_α be a subbasis of Y, then (K, W_α) where $K \subset X$ compact is a subbasis of $\mathrm{Map}(X, Y)$. ⌟

Proof: If $f \in (K, U) \subset \mathrm{Map}(X, Y)$, let $U = \bigcup_\beta U_\beta$, where $U_\beta = \bigcap_{j=1}^{k(\beta)} W_{\beta, j}$. Now $K \subset \bigcup_\beta f^{-1}(U_\beta)$, because K is compact Hausdorff thus the partition of unity(4.4.7.9) gives us f.m. compact subsets $K_1, \ldots, K_n$ of K that $K_i \subset f^{-1}(U_{\beta_i})$ for some β. Then

$$f \in \bigcap_{i=1}^{n} \bigcap_{j=1}^{k(\beta_i)} (K_i, W_{\beta_i, j}) = \bigcap_{i=1}^{n} (K_i, U_{\beta_i}) \subset (K, \bigcup_{i=1}^{n} U_{\beta_i}) \subset (K, U).$$

□

Prop. (4.4.3.7) [Adjointness of Mapping Space]. Let Y be a locally compact Hausdorff space, then

$$\mathrm{Map}(X\times Y,Z)\cong \mathrm{Map}(X,\mathrm{Map}(Y,Z))$$

as sets. And if moreover X is Hausdorff, then it is a homeomorphism. ⌟

Proof: Let $\varphi\in \mathrm{Map}(X\times Y,Z)$, for any $x\in X$, take $\varphi(x):Y\to Z:\varphi(x)(y)=\varphi(x,y)$, then $\varphi(x)$ is continuous, and $\widetilde{\varphi}:X\mapsto \mathrm{Map}(Y,Z):x\mapsto\varphi(x)$ is continuous: for any compact $K\subset Y$ and open $U\subset Z$, $\widetilde{\varphi}^{-1}((K,U))=\{x\in X|\varphi(x\times K)\subset U\}$, which is open.

Conversely, for any $\psi:X\to \mathrm{Map}(Y,Z)$, let $\widetilde{\psi}:X\times Y\to Z$ be given by $\widetilde{\psi}(x,y)=\psi(x)(y)$. Then $\widetilde{\psi}$ is continuous: For any open $U\subset Z$, if $(x,y)\in\widetilde{\psi}^{-1}(U)$, then $\psi(x)y\subset U$. Because $\psi(x)$ is continuous, there is a nbhd W of $y\in Y$ that $\varphi(x)(W)\subset U$. Then because Y is locally compact Hausdorff, there is a precompact nbhd V of $y\in Y$ that $y\in V\subset\overline{V}\subset W$. Then $\psi^{-1}((\overline{V},U))$ is a nbhd of $x\in X$, and $(x,y)\in(\psi^{-1}((\overline{V},U)),V)\subset\widetilde{\psi}^{-1}(U)$, thus $\widetilde{\psi}^{-1}(U)$ is open, and $\widetilde{\psi}$ is continuous.

Now let $F:\varphi\mapsto\widetilde{\varphi}$ and $G:\psi\mapsto\widetilde{\psi}$, then we show F,G are both continuous: By(4.4.3.6), $(K,(L,U))$ is a subbasis of $\mathrm{Map}(X,\mathrm{Map}(Y,Z))$. F is continuous because $F((K\times L,U))=(K,(L,U))$. G is continuous because $X\times Y$ is Hausdorff and for any J compact in $X\times Y$, $J\times J\xrightarrow{(\mathrm{pr}_1,\mathrm{pr}_2)}X\times Y$ is continuous, so for any $U\subset Z$ open, there exists $J_1\subset X,J_2\subset Y$ compact s.t. $G((J_1,(J_2,U)))\subset(J,U)$. □

Cor. (4.4.3.8). If Y is locally compact and Hausdorff, $A\subset X,B\subset Y,C\subset Z$, then

$$\mathrm{Map}((X\times Y,X\times B\cup A\times Y),(Z,C))\cong\mathrm{Map}((X,A),\mathrm{Map}((Y,B),(Z,C)))$$

as sets, and if moreover X is Hausdorff, then it is a homeomorphism. ⌟

Def. (4.4.3.9) [Admissible Topology]. For $X,Y\in\mathcal{T}\mathrm{op}$, an **admissible topology** on $\mathrm{Map}(X,Y)$ is a topology that makes the evaluation map $e:\mathrm{Map}(X,Y)\times X\to Y$ continuous. ⌟

Prop. (4.4.3.10). The compact-open topology on $\mathrm{Map}(X,Y)$ is coarser than admissible topology on it(4.4.3.9). And if X is locally compact Hausdorff, then it is admissible. ⌟

Proof: It suffices to show any (K,U) is open in $\mathrm{Map}(X,Y)$. Let $f\in(K,U)$, then for any $x\in K$, $e(f,x)\in U$, thus there is a nbhd U_x of f and a nbhd W_x of x that $e(U_x\times W_x)\subset U$. Now because K is compact, we can choose a nbhd V of f that $e(V\times K)\subset U$. Thus $f\in V\subset(K,U)$, and (K,U) is open in $\mathrm{Map}(X,Y)$. If Y is locally compact Hausdorff, then $\mathrm{Map}(Y,Z)\times Y\to Z$ continuous by applying(4.4.3.5) with $X=\mathrm{pt}$. □

Mapping Spaces in $\mathcal{CG}$

Def. (4.4.3.11) [Mapping Spaces]. For $X,Y\in\mathcal{CG}$, the mapping space $\mathrm{Map}_c(X,Y)$ is the compact generation(4.4.2.27) of the space of continuous functions from X to Y with the topology generated by the sets $(K,U)=\{f:f(i(K))\subset U\}$, where K is a compact Hausdorff space, $i:K\to X$ and U is open in Y. ⌟

Prop. (4.4.3.12). For $X'\to X,Y\to Y'\in\mathcal{CG}$, the induced map $\mathrm{Map}_c(X,Y)\to\mathrm{Map}_c(X',Y')$ is continuous. In particular, if $X\cong X'$ and $Y\cong Y'$, then $\mathrm{Map}_c(X,Y)\cong\mathrm{Map}_c(X',Y')$. ⌟

Lemma (4.4.3.13) [Evaluations are Continuous]. For $X,Y\in\mathcal{CG}$, the composition map

$$\mathrm{Map}_c(Y,X)\times_c Y\to X$$

is continuous. ⌟

Proof: It suffices to prove that for any compact Hausdorff space K, F mapping into $\mathrm{Map}(Y,X), Y$, $K \times F \to X$ is continuous: For $(f_0, y) \in \mathrm{Map}_c(Y,X) \times_c Y$ and $f_0(y) \in U$, as f_0 is continuous, there exists a nbhd N of $y \in Y$ s.t. $f_0(\overline{N \cap F}) \subset U$, and then $(f_0, y) \in (K \cap (\overline{N \cap F}, U), N \cap F)$ is mapped into U. □

Prop. (4.4.3.14) [Adjointness of Mapping Space]. For $X, Y, Z \in \mathcal{CG}$, there is a natural homeomorphism

$$\mathrm{Map}_c(X \times_c Y, Z) \cong \mathrm{Map}_c(X, \mathrm{Map}_c(Y, Z))$$

⌟

Proof: Let $\varphi \in \mathrm{Map}_c(X \times_c Y, Z)$, for any $x \in X$, take $\varphi(x) : Y \to Z : \varphi(x)(y) = \varphi(x,y)$, then $\varphi(x)$ is continuous, and $\widetilde{\varphi} : X \mapsto \mathrm{Map}(Y,Z) : x \mapsto \varphi(x)$ is continuous: if $\varphi(x) \in (K,U)$, $\widetilde{\varphi}^{-1}((K,U)) = \{x \in X | \varphi(x \times i(K)) \subset U\}$, which is open.

To prove this construction is continuous, notice we have already seen that if $f : X \times_c Y \to Z$ is continuous then $f : Y \to \mathrm{Map}_c(Y, Z)$ is continuous. Apply this to

$$\mathrm{Map}_c(Y \times_c X, Z) \times_c Y \times_c X \to Z$$

we see that

$$X \times_c \mathrm{Map}_c(Y \times_c X, Z) \to \mathrm{Map}_c(Y, Z)$$

is continuous, and

$$\mathrm{Map}_c(Y \times_c X, Z) \to \mathrm{Map}_c(X, \mathrm{Map}_c(Y, Z))$$

is continuous. Similarly, as

$$\mathrm{Map}_c(X, \mathrm{Map}_c(X, Z)) \times_c Y \times_c X \to Z$$

is continuous, we get

$$\mathrm{Map}_c(X, \mathrm{Map}_c(Y, Z)) \to \mathrm{Map}_c(X \times_c Y, Z)$$

is continuous, and it is clearly the inverse to the construction above. □

Cor. (4.4.3.15). For $X, Y, Z \in \mathcal{CG}$, $A \subset X, B \subset Y, C \subset Z$, then there is a natural homeomorphism

$$\mathrm{Map}((X \times Y, X \times B \cup A \times Y), (Z, C)) \cong \mathrm{Map}((X, A), \mathrm{Map}((Y, B), (Z, C)))$$

⌟

Cor. (4.4.3.16). products in $\mathcal{CG}$ commute with colimits. ⌟

Cor. (4.4.3.17) [Compositions are Continuous]. For $X, Y, Z \in \mathcal{CG}$, the composition map

$$\mathrm{Map}_c(Y, Z) \times_c \mathrm{Map}_c(X, Y) \to \mathrm{Map}_c(X, Z)$$

is continuous. ⌟

Proof: It suffices to show that

$$\mathrm{Map}_c(Y, Z) \times_c \mathrm{Map}_c(X, Y) \times_c X \to Z$$

is continuous, and this follows from(4.4.3.13). □

Construction of Spaces

Def. (4.4.3.18) [Path Spaces]. For $f : A \to B \in \mathcal{T}\mathrm{op}$, let E_f be the subspace of $A \times \mathrm{Map}(I, B)$ consisting of pairs (a, γ) that $\gamma(0) = a$.

The fibers of $E_f \to B$ are called **homotopy fibers** of f. ⌟

Def. (4.4.3.19) [n-Loop Space]. The n-**loop space** of X is defined to be $\Omega^n(X, x_0) = M(I^n, \partial I^n; X, x_0)$. Then by(4.4.3.8) we have

$$\Omega(\Omega^n(X, x_0), \widetilde{x}_0) \cong \Omega^{n+1}(X, x_0).$$

⌟

Prop. (4.4.3.20) [Loop spaces are Homotopy Fibers]. Let $f : x_0 \to B$ be a point, then E_f is the **path space** PB of all paths starting from x_0, and the homotopy fiber over x_0 is just the loop space $\Omega(X, x_0)$. PB is contractible, with the contraction given by $H : PB \times I \to PB : \gamma_t(x) = \gamma(tx)$. ⌟

4 Profinite Space

Def. (4.4.4.1) [Profinite Space]. A space is called a **profinite space** if it is a cofiltered limit of discrete topological spaces. The category of profinite spaces is denoted by $\mathcal{P}\mathrm{rof}$.

A profinite space is the same thing as a totally disconnected, compact Hausdorff topological space. Thus a closed subspace of a profinite space is profinite. ⌟

Proof: The profinite spaces are clearly totally disconnected, compact Hausdorff(by Tychonoff).

Conversely, if it is totally disconnected and compact Hausdorff, let $\mathcal{I}$ be the set of clopen decompositions $X = \coprod_I U_i$ of X, then for each $I \subset \mathcal{I}$, there is a map $X \to I$, and there is a partial order on the decompositions of X. We show that the map $X \to \lim_{I \subset \mathcal{I}} I$ is a homeomorphism. It is injective by(4.4.1.26)(4.4.1.24)(4.4.7.6). It is surjective by compactness of X, and it is clearly open, thus homeomorphism by(4.4.2.11). □

Cor. (4.4.4.2). A cofiltered limit of profinite spaces is profinite. ⌟

Prop. (4.4.4.3). Any open covering of a profinite space has a clopen disjoint subcover. ⌟

Proof: By(4.4.4.1), we may assume that $X = \lim_{i \in I} X_i$, where X_i is finite. Let f_i be the projection, as the limit is filtered, a fundamental family of nbhds of a point (x_i) $f_i^(x_i)$, Then for each covering, we may assume it is finite $X = \cup_{i \in I} f_i^{-1}(x_i)$, choose a $j > i$ for each i, as I is cofiltered, then $X = \coprod_{x \in X_j} f_j^{-1}(x)$ satisfies the desired property. □

Prop. (4.4.4.4). If X is quasi-compact and any connected component of X is the intersection of clopen sets containing it (e.g. X is normal(4.4.1.24)), then $\pi_0(X)$ is a profinite space. ⌟

Proof: $\pi_0(X)$ is an image of X, so it is quasi-compact, also it is clearly totally disconnected. To show it is Hausdorff, let C, D be disjoint connected components of X, then $C = \cap U_\alpha$, where U_α are clopen. Since $C \cap D = \varnothing$, $U_\alpha \cap D = \varnothing$ for some α. and then the image of U_α separates C and D in $\pi_0(X)$. □

Locally Profinite Space

Def. (4.4.4.5) [Locally Profinite Space]. A **locally profinite space** is a totally disconnected, locally compact Hausdorff topological space. The category of locally profinite space is denoted by `LocProfSpa`. ⌟

Prop. (4.4.4.6). A locally closed subsets of a locally profinite space is locally profinite. And compact subsets are profinite. ⌟

Proof: Closed subsets are clearly locally profinite, for the open subsets, it is also locally compact. □

Cor. (4.4.4.7). Any open covering of a compact subsets of a locally profinite space has an clopen disjoint subcover, by(4.4.4.3). ⌟

Prop. (4.4.4.8). The set of all compact open subsets form a basis of the topology of G. ⌟

Prop. (4.4.4.9). If $X \in$ `LocProfSpa` and K is a compact subspace of X. Let $K \subset \cup U_\alpha$ be an open covering, then there exist f.m. disjoint open compact subsets $V_i \subset X$ that each $V_i \cap K \subset U_\alpha$ for some α, and $K \subset \cup V_i$. ⌟

Proof: Because K is profinite(4.4.4.6), (4.4.4.3) shows there is a finite disjoint compact open subcover W_i of U_α, then $W_i = V_i \cap K$ for V_i compact, and using compactness of W_i, we can assume V_i is compact. Finally to make V_i disjoint, we can let $V_i = V_i \backslash (\cup_{k=1}^{i-1} V_k)$. □

Structure Sheaves and Distributions

Cf.[Representations of the Group GL(n,F) over Local Fields Bernstein/Zelevinsky] and [Bernstein, Representation of p-adic Groups, Bernstein].

Def. (4.4.4.10) [Structure Sheaves and Distributions]. For $X \in$ `LocProfSpa`, the structure sheaf C_X^∞ on X is defined to be the locally constant sheaf $\underline{\mathbb{Z}}$ on X.

The space $C_c^\infty(X)$ of **test functions**(or **smooth functions** on X is the set of locally constant continuous functions with compact supports.

For any group $W \in \mathcal{A}$b, the space of **distribution on** X with values in W is defined to be $\mathrm{Dist}(X, W) \overset{\triangle}{=} \mathrm{Hom}(C_c^\infty(X), W)$. And denote $\mathrm{Dist}(X) = \mathrm{Dist}(X, \mathbb{C})$.

More generally, if $\mathcal{F}$ is a C_X^∞-sheaf, then the space of **distributions on** $\mathcal{F}$ on X valued in W is defined to be $\mathrm{Dist}(X, \mathcal{F}; W) \overset{\triangle}{=} \mathrm{Hom}(\Gamma_c(X, \mathcal{F}), W)$. ⌟

Prop. (4.4.4.11) [Distributions]. If $X \in$ `LocProfSpa`, $\mathcal{F}$ is a C_X^∞-sheaf, $W \in \mathcal{A}$b, then for any open subset $U \subset X$ and $Z = X \backslash U$, there is an exact sequence:

$$0 \to \Gamma_c(U, \mathcal{F}; W) \to \Gamma_c(X, \mathcal{F}; W) \to \Gamma_c(Z, \mathcal{F}; W) \to 0.$$

thus also an exact sequence:

$$0 \to \mathrm{Dist}(Z, \mathcal{F}; W) \to \mathrm{Dist}(X, \mathcal{F}; W) \to \mathrm{Dist}(U, \mathcal{F}; W) \to 0.$$

In particular, there is an exact sequence

$$0 \to \mathrm{Dist}(Z) \to \mathrm{Dist}(X) \to \mathrm{Dist}(U) \to 0,$$

⌟

Proof: The left exactness is clear. To show the right surjectivity, let $f \in \Gamma_c(Z, \mathcal{F})$, then for each $x \in \mathrm{Supp}(f)$, there is a compact open nbhd U_x that f restricts to an element of $\Gamma(U_x, \mathcal{F})$. Then these U_x cover $\mathrm{Supp}(f)$, then by(4.4.4.7), there is a disjoint finite cover $\{U_i\}$ of $\mathrm{Supp}(f)$ that f are induced by $f_i \in \Gamma(U_i, \mathcal{F})$. Now we can replace U_i by $U_i \backslash \cup_{j<i} U_j$ to let U_i be disjoint, then f extends to an element of $\cup U_i$. □

Prop. (4.4.4.12). If X, Y are both locally profinite, then

$$C_c^\infty(X \times Y) = C_c^\infty(X) \otimes C_c^\infty(Y)$$

⌟

Proof: Because the subspaces of the form $U \times V$ for U, V open form a subbasis of $X \times Y$, so any compact open subset of $X \times Y$ is a disjoint union of sets of the form $U \times V$. □

Def. (4.4.4.13) [Cosmooth $C_c^\infty(X)$-Modules]. A **cosmooth $C_c^\infty(X)$-module** is a $C_c^\infty(X)$-module M that for any $m \in M$, there exists some compact open $U \subset X$ that $m = \chi_U m$. ⌟

Prop. (4.4.4.14) [Cosmooth $C_c^\infty(X)$-Module and $C^\infty(X)$-Sheaves]. Let $\mathcal{F}$ be a C_X^∞-sheaf on X, then the space $\Gamma_c(X, \mathcal{F})$ is a cosmooth $C_c^\infty(X)$-module(4.4.4.13), and this defines an equivalence of categories between the category of non-degenerate $C_c^\infty(X)$-modules and $C^\infty(X)$-sheaves.

Notice that in this case, a $C_c^\infty(X)$-module M being non-degenerate is equivalent to: for any $m \in M$, there is a compact open subset U that $\chi_U m = m$. ⌟

Proof: For any non-degenerate $C_c^\infty(X)$-module M, define a sheaf $\mathcal{F}_M$ of the compatible stalks in $\prod_{x\in X} M/M(x)$, where

$$M(x) = \{m \in M | \chi_U m = 0 \text{ for some } x \in U\}.$$

Then we show these two functors are inverse to each other: One direction is clear, as the sheaf $\mathcal{F}$ is just the sheaf of compatible stalks in $\prod_{x\in X} \mathcal{F}_x$, and it is easy to see $\mathcal{F}_x \cong M/M(x)$. For the other direction, any element in $\Gamma_c(X, \mathcal{F}_M)$ is induced from $f_i \in \Gamma(U_i, \mathcal{F}_M)$, where U_i are pairwise disjoint compact open subsets, by(4.4.4.7), and it is easy to see $\Gamma(U_i, \mathcal{F}_M) = \chi_U M$. Thus $\Gamma_c(X, \mathcal{F}_M) = C_c^\infty(X)M$, and the non-degeneracy of M shows $\Gamma_c(X, \mathcal{F}_M) \cong M$. □

Remark (4.4.4.15). Notice that $M(x)$ can be equivalently defined to be the space spanned by the elements

$$\{gm | g \in C_c^\infty(X), g(x) = 0, m \in M\}.$$

⌟

5 Real Numbers

References are [Mun00].

Topology

Prop. (4.4.5.1) [$\mathbb{R}$ is Connected]. $\mathbb{R}$ is connected, and so are intervals and rays in $\mathbb{R}$. ⌟

Proof: This follows from(4.4.1.21), as the hypothesis is satisfied by(2.2.9.1) and the fact for any $a < b \in \mathbb{R}, a < \frac{a+b}{2} < b$. □

Prop. (4.4.5.2). $\mathbb{R}^n$ satisfies the Heine-Borel property(4.4.8.3), i.e. bounded closed sets are compact. ⌟

Proof: It suffices to consider the square metric. If A is bounded, then A is in $[-N, N]^n$ for some number N. $[-N, N]^n$ is compact by(4.4.2.4) and(4.4.2.5). □

Borel Set

Def. (4.4.5.3). Let U be a ultrafilter on a set I and $\{a_I\}$ be a bounded sequence of real numbers. Then a number a is called the U**-limit** of $\{a_I\}$ is for every $\varepsilon > 0, \{i \in I||a_i - a| < \varepsilon\} \in U$.

There is at most one limit, because $\{i \in I||a_i - a| < \varepsilon\}, \{i \in I||a_i - b| < \varepsilon\}$ will be disjoint hence cannot both be in U. ⌟

Prop. (4.4.5.4) [Generalized Limit]. Let U be an ultrafilter on $\mathbb{N}$, then for any bounded sequence of real numbers $\{a_n\}$, $\lim_U a_n$ exists. i.e. There is a functional from l^∞ to $\mathbb{R}$.

And if $\{a_n\}$ has a limit pt a in the usual sense, then $\lim_U a_n = a$ for any non-principal ultrafilter U, because any $\{i \in I||a_i - a| < \varepsilon\}$ is cofinite hence in U(2.2.10.9). ⌟

Proof: Let $A_x = \{n|a_n < x\}$. Then A_x is monotone, then we can choose $c = \sup\{x|A_x \notin U\}$(2.2.3.22). And it is easily verified that $c = \lim_U a_n$. □

Cor. (4.4.5.5) [Density Measure]. There exists a measure m on $\mathbb{N}$ that $m(A) = d(A)$ for each set $A \subset \mathbb{N}$ that has a density $d(A)$. ⌟

Proof: Let U be a non-principal ultrafilter on $\mathbb{N}$(2.2.10.9), let $m(A) = \lim_U \frac{A(n)}{n}$. It is clearly additive and monotone. And it equals the density by(4.4.5.4) □

6 Separation Axioms

Prop. (4.4.6.1). Any Quasi-compact T_0 space X contains a closed point. ⌟

Proof: Consider the family of non-empty closed subsets of X, there is a minimal element by quasi-compactness. Choose a minimal element T, and let $x \in T$, then $\overline{\{x\}} = T$. Then x is closed, otherwise there is some $x' \neq x \in \overline{\{x\}}$, and $\overline{\{x'\}} \neq \overline{\{x\}}$ because X is T_0. □

Hausdorff

Prop. (4.4.6.2). If X is a Hausdorff space and $S_1 \supset S_2 \supset \ldots$ is a nested chain of compact connected subsets of X, then $S = \cap S_i$ is also compact and connected. ⌟

Proof: S is clearly compact. Suppose it is disconnected, then $S = A_1 \cup A_2$ is a disjoint union of compact open subsets. Then we can find two open disjointsubset U_1, U_2 of X s.t. $A_i = U_i \cap S$. Then by the compactness of S_1 and(4.4.2.3), it can be shown that $S_n \in U_1 \cup U_2$ for n large, so S_n is disconnected, contradiction. □

Hausdorffization

Cf.[the Hausdorff Quotient].

Regular

Completely Regular

Normal (T4)

Prop. (4.4.6.3) [Urysohn lemma]. Let X be normal, A and B two closed subset of X, then there exists a continuous map from X to $[0, 1]$ that maps A to 0 and B to 1. ⌟

Proof: Use the countability of rational numbers to construct a family of U_q s.t.

$$p < q \Rightarrow \bar{U}_p \subset U_q$$

Then choose $f(x) = \inf\{p \in \mathbb{Q} | x \in U_p\}$, then this f meets the requirement. □

Cor. (4.4.6.4) [Tietze extension]. If X is normal and Y is a closed subspace, then any continuous function f on Y can be extended to a continuous function on X. ⌟

Proof: □

7 Paracompactness

Def. (4.4.7.1) [Paracompactness]. A space X is called **paracompact** if any open covering $\mathcal{U}$ has a locally finite open refinement covering. ⌟

Prop. (4.4.7.2) [Characterization of Paracompactness]. If X is regular, then TFAE:

1. Each open cover of X has an open locally finite refinement.
2. Each open cover of X has a locally finite refinement.
3. Each open cover of X has a closed locally finite refinement.
4. Each open cover of X is even. i.e. for any cover, there is an open nbhd V of diagonal of $X \times X$ such that $\forall x$, $V[x] = \{y | (x, y) \in V\}$ refines the cover.
5. Each open cover of X has an open σ-discrete refinement.
6. Each open cover of X has an open σ-locally finite refinement.

If this is satisfied, then X is called **paracompact**. ⌟

Proof: $6 \to 2$:Just minus every open set the part of open sets that appeared in families that ordered before it. $2 + 4 \to 1$:Use the lemma below, we can transform the cover $\mathcal{A}$ into $V[\mathcal{A}] \cap U_A$ which is an open locally finite cover
Cf.[General Topology Kelley] and [Mun00]P254. □

Lemma (4.4.7.3). If X satiesfies 4, let U be a nbhd of diagonal of $X \times X$, then their exists a symmetric nbhd of diagonal s.t. $V \circ V \subset U$, where $U \circ V = \{(x, z) | (x, y) \in U, (y, z) \in V, \exists y\}$. ⌟

Proof: $\forall x$ in X, there is a nbhd s.t. $W[x] \times W[x] \subset U$, this is an open cover, so there is a nbhd R of diagonal s.t. $R[x]$ refines it. Hense $R[x] \times R[x] \subset U$. Let $V = R \cap R^{-1}$, $V \circ V$ is the union of sets $V[x] \times V[x]$, so $V \circ V \subset U$. □

Lemma (4.4.7.4). In the preceding proposition, if X satisfies 4, Let $\mathcal{A}$ be a locally finite(resp. discrete i.e. intersect only one) family of subsets of X, then use the last lemma, there is a nbhd V of diagonal of $X \times X$ such that $V[A] = \{y | (x, y) \in V, \exists x \in A\}$ is locally finite(resp. discrete). ⌟

Proof: Choose for every pt a nbhd satisfy the property, then it is an open cover. Choose a diagonal nbhd U for the property 4, then choose coordinate symmetric nbhd V of diagonal s.t. $V \circ V \subset U$. If $V[x]$ intersect $V[A]$, then $V \circ V[x]$ intersect A. Done. □

Prop. (4.4.7.5). A locally compact second countable Hausdorff space X is paracompact. ⌟

Proof: Let $\mathcal{U}$ be a covering of X, because X is second countable and locally compact, by(4.4.2.23), we may assume $\mathcal{U}$ is a countable covering and consisting of precompact subsets. Moreover, we can change U_n to $U_n' = \cup_{i=1}^n U_i$, because if $\{B_\alpha\}$ is a locally finite refinement of $\{\cup_{i=1}^n U_i\}$, then $\{B_\alpha \cap U_\alpha\}$ is a locally finite refinement of $\{U_i\}$. So $U_n \subset U_{n+1}$, and because $\overline{U}_n$ is compact, we may assume $\overline{U}_n \subset U_{n+1}$.

Now let $K_n = \overline{U}_{n+1} \backslash U_n$(where $U_0 = \varnothing$), then K_n are all compact, and $W_n = U_{n+1} \backslash \overline{U}_{n-2}$ is an open subset containing K_n. So there are f.m. open subsets of W_n that cover K_n. There open subsets is then a refinement covering of $\mathcal{U}$, and they are locally finite, because any $x \in X$ is contained in U_n for some n. □

Prop. (4.4.7.6) [Paracompact Spaces are Normal]. A Hausdorff paracompact space X is normal. In particular, a compact Hausdorff space is normal. ⌟

Proof: Firstly X is regular: Let $x \in X$ and B a closed subset disjoint from x, then because X is Hausdorff, there is a covering of B by open subsets V_α that $x \notin \overline{V}_\alpha$. Now consider the open covering $\{X \backslash B, V_\alpha\}$ of X, then there is a locally finite refinement $\{B_\beta\}$. Those B_α that intersect B is then a locally finite covering of B. Let U be the union of these open subsets, then $B \subset U$ and $x \notin \overline{U}$, because of the locally finiteness.

To prove X is normal, we do the same but x replaced by a closed subset disjoint from B and use regularity. □

Prop. (4.4.7.7) [Paracompactness for Manifolds]. For a connected Hausdorff locally Euclidian space, the condition of paracompact, second countable and a compact exhaustion is equivalent. ⌟

Proof: Cf.[Paracompactness and second countable]. □

Lemma (4.4.7.8) [Shrinking Lemma]. Let X be a paracompact Hausdorff space and $\{U_\alpha\}_{\alpha\in I}$ an open covering of X, then there is an open covering $\{V_\alpha\}$ of X that $\overline{V}_\alpha \subset U_\alpha$ for any α. ⌟

Proof: Let $\mathcal{A}$ be the family of open subsets A of X that $\overline{A} \subset U_\alpha$ for some α, then because X is normal(4.4.7.6), $\mathcal{A}$ is a covering of X. Then we find a locally finite open covering $\mathcal{B}$ of $\mathcal{A}$, and let the covering map be $B_\beta \subset U_{f(\beta)}$, then we can get a covering $\mathcal{V}$ of X indexed by I that $V_\alpha = \cup_{f(\beta)=\alpha} B_\beta$. This is also locally finite, and $\overline{V}_\alpha \in U_\alpha$ by the locally finiteness of $\mathcal{B}$. □

Prop. (4.4.7.9) [Partition of unity]. In a paracompact Hausdorff space, given any open cover $\{U_\alpha\}$, there exists a partition of unity $\{\rho_\alpha\}$ that $\mathrm{supp}\rho_\alpha \subset U_\alpha$, and $\{\mathrm{Supp}(\rho_\alpha)\}$ is locally finite. Moreover, if X is locally compact, we can assume ⌟

Proof: Using shrinking lemma(4.4.7.8) twice, we can find locally finite open coverings $\{W_\alpha\}, \{V_\alpha\}$ that $\overline{W}_\alpha \subset V_\alpha$, $\overline{V}_\alpha \subset U_\alpha$. Because X is normal, we can find functions ψ_α on X that $\psi(W_\alpha) = 1, \psi_\alpha(X \backslash V_\alpha) = 0$. Then $\mathrm{Supp}(\psi) \subset \overline{V}_\alpha \subset U_\alpha$, so $\{\mathrm{Supp}(\psi_\alpha)\}$ is locally finite. So we can define $\Phi(x) = \sum_\alpha \psi_\alpha(x)$. $\Phi(x) > 0$ for any x because $\{W_\alpha\}$ is a covering of X. Finally, we define $\rho_\alpha = \psi_\alpha/\Phi$, then this is a partition of unity dominated by $\{U_\alpha\}$. □

8 Metric Space

Def. (4.4.8.1) [Metric Balls]. Let X be a metric space and $x \in X, \delta \in \mathbb{R}_+$, define the metric balls

$$U(x,\delta) = \{y \in X : d(x,y) < \delta\}, \quad \mathbb{D}(x,\delta) = \{y \in X : d(x,y) \le \delta\}.$$

⌟

Prop. (4.4.8.2) [Metric Spaces are Paracompact]. Any metric space is paracompact. ⌟

Proof: Cf.[Mun00]P257. □

Def. (4.4.8.3) [Heine-Borel Property]. A metric space X is said to satisfy the **Heine-Borel property** if every closed and bounded subset of X is compact. ⌟

Complete Metric Space

Def. (4.4.8.4). A set E in a metric space is called **totally bounded** iff for every $\varepsilon > 0$, there exists a finite set F that $E \subset B(F, \varepsilon)$. This definition is compatible with that in the case of a topological vector space when it is metrizable. ⌟

Prop. (4.4.8.5). The closure of a totally bounded set in a metric space is totally bounded. ⌟

Proof: For each $\varepsilon > 0$, choose a finite set F that $E \subset B(F, \varepsilon/2)$, then $\overline{E} \subset B(F, \varepsilon)$. □

Prop. (4.4.8.6). A totally bounded metric space X is separable. ⌟

Proof: $\cup N_n$ is dense and countable in X, where N_n is a finite $1/n$-net of X. □

Prop. (4.4.8.7) [Hausdorff]. Let X be a metric space, then:

1. A sequentially compact(4.4.2.6) subset M is totally bounded and the converse is true if X is complete.
2. A subset M is compact iff it is self-sequentially compact iff it is closed and sequentially compact.
3. A subset M is precompact iff it is sequentially compact(4.4.2.6).

⌟

Proof: 1: If M is not totally bounded, then for some $\varepsilon > 0$, we can choose consecutively a sequence of points x_i that $d(x_i, x_j) \geq \varepsilon$, this cannot has a convergent subsequence in X.

Conversely, if M is totally bounded, choose a $1/k$-net for each k, then for any sequence in M, there is a y_i that some infinite subsequence $\{x_n^{(1)}\} \subset B(y_1, 1)$, and consecutively find infinite subsequences $\{x_n^{(m)}\} \subset B(y_k, 1/k)$, then finally choose the diagonal, then it is a Cauchy sequence.

2: If it is compact, given a sequence, if no point is a convergent point, then each point has a nbhd that contains at most one point of the sequence. Then by compactness, there are at most f.m. points, contradiction. A compact set must has the convergent point in itself because it is closed as M is Hausdorff.

Conversely, if it is self-sequentially compact, then it is totally bounded by 1. so if M is not compact, then for each n it has $1/n$-net N_n, then there is at least one x_n that $B(x_n, 1/n)$ cannot by covered by f.m. of the covering, The sequence $\{x_n\}$ has a subsequence $\{x_{n_k}\}$ that is convergent to x. But $x \in M$ is in some open cover, so $B(x_{n_k}, 1/n_k)$ is contained in some open cover, contradiction.

That closed and sequentially compact is equivalent to self sequentially compact is obvious.

3: If it is precompact, then it is sequentially compact by 2, conversely, if x_i is a sequence in $\overline{M}$, then choose $|y_n - x_n| \leq 1/n$, so some sequence y_{n_k} is convergent to $y_0 \in \overline{M}$, so x_{n_k} also converges to y_0. So $\overline{M}$ is self-sequentially compact, so it is compact by 2. □

Cor. (4.4.8.8) [Arzela-Ascoli]. For $X \in$ CHaus, $F \subset C(X)$ is a sequentially compact(precompact, by(4.4.8.7)) subset iff it is uniformly bounded and equicontinuous. ⌟

Proof: As $C(M)$ is complete metric space, sequentially compact is equivalent to totally bounded. If it is totally bounded, then it is clearly uniformly bounded, and for every $\varepsilon > 0$, find a $\varepsilon/3$-net for F, which means f.m. functions in F that any other function is $\varepsilon/3$-close to one of them. So they are equicontinuous.

Conversely, if it is uniformly bounded and equicontinuous, for every $\varepsilon > 0$, find a finite covering of M that for any two points x, y in one cover of them, $|f(x) - f(y)| < \varepsilon/3$ for all $f \in F$. Then choose for each covering a point x_i, consider $f : F \to \mathbb{C}^n : \varphi \mapsto (\varphi(x_1), \ldots, \varphi(x_n))$, then the image is bounded, hence precompact by(4.4.5.2), so it is totally bounded by(4.4.8.7). So we can choose a $\varepsilon/3$-net φ_k for x_i simultaneously, and it is by $\varepsilon/3$ argument that these φ_k is a ε-net for F. ☐

Prop. (4.4.8.9) [Fixed point theorem]. If X is a complete metric space and $f : X \to X$ satisfies $d(f(x), f(y)) \leq \lambda d(x, y)$ for some $0 \leq \lambda < 1$, then f has a unique fixed point in X. If X is moreover compact, then and f that $d(f(x), f(y)) < d(x, y)$ will have a unique fixed point. ⌟

Proof: $x + f(x) + f^2(x) + \cdots$ is the fixed point. And uniqueness is easy. For compact case, notice the image $\mathrm{Im}\, f^n$ is a descending chain, it must stable to some T. If $x, y \in Y$ attains the diameter of Y, and let $x = f(X), y = f(Y)$, where $X, Y \in T$, then $d(x, y) < d(X, Y) \leq d(x, y)$, contradiction. ☐

Prop. (4.4.8.10) [Dilation Closed]. If X, Y are metric spaces that X is complete metric space, then if $f : X \to Y$ is continuous function that is a dilation, i.e. $d(f(x_1), f(x_2)) \geq d(x_1, x_2)$, then $f(X)$ is closed.

So a continuous dilation map on a complete metric space is a closed map. ⌟

Proof: If $y \in \overline{f(X)}$, then because Y is metric, there are x_n that $y = \lim f(x_n)$. Thus $\{f(x_n)\}$ is Cauchy in Y, and $\{x_n\}$ is Cauchy too. So there is a $x = \lim x_n$, and clearly $f(x) = y$. ☐

Compact Metric Space

Lemma (4.4.8.11) [Lebesgue Number Lemma]. For any open covering U_i of a compact metric space X, there exists a $\delta > 0$ that any subset X of diameter smaller than δ is contained in some U_i. ⌟

Proof: If X is in the covering U_i, then there is nothing to prove, otherwise, it suffices to assume the covering is a finite covering, let $C_i = X - U_i$, and let $f(x) = \frac{1}{n}\sum d(x, C_i)$. Notice $f(x) > 0$, because $x \notin C_i$ for some C_i. Now it is also continuous, so it has a minimal value$> \delta > 0$.

Now if B has diameter smaller than δ, then if $x_0 \in B$, $\delta < f(x_0) < d(x, C_{i_0})$, where $d(x, C_{i_0})$ is the maximal among $d(x, C_k)$, and $B \in B(x, \delta)$, thus $B \in U_{i_0}$. ☐

Prop. (4.4.8.12) [Uniform Continuity Theorem]. If $f : X \to Y$ is a continuous map between two metric spaces that X is compact, then f is uniformly continuous. ⌟

Proof: Take an open covering of Y with balls $B(y_i, \varepsilon/2)$ of diameter $\varepsilon/2$, and consider their inverse image, then choose the lebesgue number δ for this covering(4.4.8.11), we see that for any $d(x, y) < \delta$, $d(f(x), f(y)) < \varepsilon$. ☐

Prop. (4.4.8.13). If f is an isometry of a compact metric space X, then it is a bijection thus an homeomorphism. ⌟

Proof: It is clearly injective. If it is not surjective, then choose a $x \notin \mathrm{Im}(f)$, because $\mathrm{Im}(f)$ is compact hence closed in X, $d(x, \mathrm{Im}(f)) = \varepsilon > 0$. Now consider the minimal N that we can cover X with open subsets of diameter smaller than ε, this N exists because X is compact. Now if U_i covers X, then the one that contains x cannot intersect with $\mathrm{Im}(f)$. But $f^{-1}(U_i)$ is an open cover of X with smaller numbers of open subsets, contradiction. ☐

9 Baire Spaces

Def. (4.4.9.1) [Baire Spaces]. A subset of a topological space X is called of **first category** if it is contained in some countable union of closed subsets of X having no interior point. It is called of **second category** if it is not of first category.

A **Baire space** is a topological space that any nonempty open subsets of X is of second category. ⌟

Prop. (4.4.9.2) [Baire Category Theorem]. Every complete metric space & locally compact Hausdorff space is a Baire space. ⌟

Proof: Choose consecutively (precompact)open subsets that doesn't intersect $\overline{E_n}$ to find a limit point. □

10 Uniform Spaces

Def. (4.4.10.1) [Uniform Spaces]. ⌟

Def. (4.4.10.2) [Cauchy Filter in the Topological Group Case]. A **Cauchy filter** is a topological Abelian group is a filter $\mathcal{F}$ that for any nbhd U of 0, there exists $E \in \mathcal{F}$ that $x - y \in U$ if $x, y \in E$. ⌟

Def. (4.4.10.3) [Complete Uniform Spaces]. A topological Abelian group is called **complete uniform space** iff it is Hausdorff, and any Cauchy filter has a limit. ⌟

11 Manifolds

Def. (4.4.11.1) [Manifolds]. A (topological) **manifold** of dimension n is a topological space that is Hausdorff, second-countable and locally Euclidean. By(4.4.7.7), the last condition is equivalent to say it is paracompact.

The category of topological manifolds is denoted by $\mathcal{M}$ani. ⌟

Thm. (4.4.11.2) [Annulus Theorem, Rado-Moise-Quinn-Kirby]. For any map $h : \mathbb{R}^n \to \mathbb{R}^n$ that maps $\mathbb{D}^n$ into its interior, there is a homeomorphism $\mathbb{D}^n \backslash h(\mathbb{D}^n) \cong \mathbb{S}^{n-1} \times \mathbb{I}$ that identifies $\partial\mathbb{D}^n$ and $h(\partial\mathbb{D}^n)$ with $\mathbb{S}^{n-1} \times \{0\}, \mathbb{S}^{n-1} \times \{1\}$ resp. ⌟

Proof:

□

Def. (4.4.11.3) [Jordan Curves]. A **Jordan curve** in a topological space X is an injective closed curve $\gamma : [a, b] \to X$. ⌟

Thm. (4.4.11.4) [Jordan Curve Theorem, Jordan1887]. Let γ be a Jordan curve in $\mathbb{R}^2$, then $\mathbb{R}^2 \backslash \gamma$ has exactly two components, one is bounded, denoted by $\operatorname{int}\gamma$, while the other is unbounded. ⌟

Proof: □

Triangularizations

Def. (4.4.11.5) [Triangularizations]. A **triangularizable space** is a space that is homeomorphic to the geometrization of a simplicial set X(4.6.3.8) such that

- X is generated by its n-simplices for some $n \in \mathbb{Z}$.
- For any $A, B \in X_n$, $A \cap B = \varnothing$ or $A \cap B \in X_{n-1}$.
- For any $Z \in X_{n-1}$, there are at most two $A \in X_n$ s.t. $Z \subset A$.

Any such homeomorphism is called a **triangularization** of this space. ⌟

Thm. (4.4.11.6) [Triangularization of Surfaces, Rado1920]. All compact connected surface is triangularizable. ⌟

Proof: ? □

Def. (4.4.11.7) [Pachner Moves]. Let M be a triangulated n-dimensional manifold, and let $C \subset M$ be a sub-triangulated manifold of dimension n with an isomorphism $\varphi : C \to C' \subset \partial\Delta_{n+1}$. Then the **Pachner move** on N associated to C is the triangulated manifold

$$N' = (N \setminus C) \cup_\varphi (\partial\Delta_{n+1} \setminus C').$$

⌟

Example (4.4.11.8). For surfaces, there are two Pachner moves(and their inverses):

- $(ABC) \cup (ACD) \mapsto (ABD) \cup (BCD)$.
- $(ABC) \mapsto (ABD) \cup (BCD) \cup (CAD)$.

⌟

Thm. (4.4.11.9) [Pachner1991]. Given any closed surface Σ, any two triangulations of Σ is related by a finite sequence of isotopies and Pachner moves(4.4.11.7). ⌟

Proof: □

Surfaces

Def. (4.4.11.10) [Topological Surfaces]. A **topological surface** (with boundaries) is a topological manifold of dimension 2 (with boundaries). ⌟

Def. (4.4.11.11) [Planer Glueing Diagram]. A **planer glueing diagram** is a polygon with some glueing of its edges with orientations clockwise such that no three edges are glued together. We can label the edges by symbols and their inverses. different symbols are considered not glued together. For example, $aba^{-1}b^{-1}, abab$.

A **compact planer glueing diagram** is a planer glueing diagram that every symbol appear exactly twice in the the edges of the polygon. ⌟

Prop. (4.4.11.12). The space correspond to a planer glueing diagram is a compact topological surface with boundaries.

The space correspond to a compact planer glueing diagram is a compact topological surface. ⌟

Proof: It is compact as a quotient of a compact space. It can verified that it is locally Euclidean at each space. And it is clearly Hausdorff. □

Lemma (4.4.11.13). $\mathbb{T}^2\#\mathbb{RP}^2 \cong \mathbb{RP}^2\#\mathbb{RP}^2\#\mathbb{RP}^2$. ⌟

Proof: By(4.4.11.11), it suffices to show that $aabcb^{-1}c^{-1}$ is homeomorphic to $eeffgg$. For this, use cut-and-paste.? □

Thm. (4.4.11.14)[Classification of Surfaces]. Any compact topological surface is homeomorphic to exactly one of the following: $\mathbb{S}^2, \#^n\mathbb{T}^2$ or $\#^n\mathbb{RP}^2$, $n \in \mathbb{Z}_+$. The corresponding planer diagram is aa^{-1}, $a_1b_1a_1^{-1}b_1^{-1}\dots a_nb_na_n^{-1}b_n^{-1}$, $e_1e_1e_2e_2\dots e_ne_n$. ⌟

Proof: By triangularization theorem(4.4.11.6), it is easy to see that any compact surface is the space corresponding to a compact planer diagram. Then it suffices to show any compact planer diagram is isomorphic to either aa^{-1}, $a_1b_1a_1^{-1}b_1^{-1}\dots a_nb_na_n^{-1}b_n^{-1}$, $e_1e_1e_2e_2\dots e_ne_n$.

Firstly we can reduce to the case where all vertices are glued together: Take a vertex P, then we can spot all the vertices that are glued to P. If these are not all the vertices, we can find an edge $e = PQ$, and let RPQ be a triangle, then we can cut this triangle out to paste along the edge pairing e. Then we can reduce the number of vertices glued to P. Eventually, we can eliminate P.

Secondly we can collet all edges with the same orientation(i.e. $\dots a\dots a\dots$) to be adjacent: (i.e. $\dots aa\dots$). To do this, suppose $a = P_1Q_1 = P_2Q_2$, we simply cut along the line P_1P_2 and glue a together.

Now if all edges glued together are of the same orientations, then it is clearly isomorphic to $\#^n\mathbb{RP}^2$. Otherwise there are edged a, a^{-1} glued together with the opposite orientation. Then there must be another pair b, b^{-1} s.t. these four pairs are ordered by a, b, a^{-1}, b^{-1}. This is because otherwise there will be two vertices. Then by some cut-and-paste, we can move these edges together as $\dots aba^{-1}b^{-1}\dots$. By induction, we can make all edges with the opposite orientations together and in pairs.

Thus our diagram is a connected sum of $\mathbb{T}^2$ and $\mathbb{RP}^2$. Then we can reduce the diagram to one of the three kinds by(4.4.11.13).

Finally, it suffices to show these three kinds are different: Their Euler characteristics are

$$\chi(\mathbb{S}^2) = 2, \quad \chi(\#^n\mathbb{T}^2) = 2 - 2n, \quad \chi(\#^n\mathbb{RP}^2) = 2 - n.$$

So the only case their Euler characters equal are $\chi(\#^n\mathbb{T}^2) = \chi(\#^{2n}\mathbb{RP}^2)$. But in this case, they are still not homeomorphic, as $H_2(\#^n\mathbb{T}^2) = \mathbb{Z}$ and $H_2(\#^{2n}\mathbb{RP}^2) = 0$. □

12 Common Spaces

Def. (4.4.12.1) [Torus]. The (n-dimensional) **torus** $\mathbb{T}^n$ is defined to be $\mathbb{T}^n = (\mathbb{S}^1)^n$. ⌟

Def. (4.4.12.2) [$\mathbb{RP}^n$]. The **real projective space** $\mathbb{RP}^n$ is the $\mathbb{R}$-points of $\mathbb{RP}_\mathbb{R}$ with the canonical topology. ⌟

Def. (4.4.12.3) [Möbius Band]. The **Möbius band** is the space defined to be the planer glueing diagram $abac$. ⌟

Def. (4.4.12.4) [Klein Bottle]. The **Klein bottle** $\mathbb{K}^2$ is the space defined by the planer glueing diagram $aba^{-1}b$. ⌟

4.5 Model Categories

Main references are [Model Category and Simplicial Methods, Goerss], [Model Categories, Kantor], [Homotopy Theories and Model Categories, Dwyer/Spalinski], [Lur09], [Hovey, Model Categories].

Def. (4.5.0.1). If $\mathcal{C} \in \mathcal{C}at$ and S is a class of morphisms in $\mathcal{C}$, we denote $l(S)$ the set of morphisms that has left lifting property w.r.t. all morphisms in $\mathcal{C}$, and $r(S)$ the set of morphisms that have right lifting property w.r.t. all morphisms in $\mathcal{C}$. Then $l(S)$ is stable under pushout and $r(S)$ is stable under pull backs. ⌟

Def. (4.5.0.2)[Model Structure]. A **model structure** on a category $\mathcal{C}$ is three classes of morphisms: **fibrations**, **cofibrations** and **weak equivalences** that satisfy the following axioms: (Denote a A **trivial (co)fibration** is a (co)fibration that is also a weak equivalence.)

M1 C has finite limits and colimits.

M2 (two out of three)If two of f, g, fg is weak equivalence, then so is the third.

M3 (retracts) Fibrations, cofibrations and weak equivalences are closed under retract.

M4 (lifting property)We have a lifting property with a cofibration i and fibration p when either of them is a weak equivalence.

M5 (factorization)Any map f can be factored as pi where i is trivial cofibration and p is a fibration, and also as pi where i is a cofibration and p is a trivial fibration.

Remark (4.5.0.3). Notice the axioms are symmetric in fibrations and cofibrations, thus the opposite category $\mathcal{C}^{op}$ has a natural model structure. So whenever we write a theorem, we should always remember its dual counterpart. ⌟

⌟

Lemma (4.5.0.4) [Closedness]. A model category satisfies the retraction axiom iff:

- fibration= r(trivial cofibrations),
- cofibration= l(trivial fibrations),
- weak equivalence= uv, where $v \in l$(fibrations) and $u \in r$(cofibrations).

⌟

Proof: If these are satisfied, retraction axiom is easy: A retract satisfies the same lifting properties. Hence retraction of a (co)fibration is a (co)fibration. For retracts weak equivalences, Cf.[Quillen, Homotopical Algebra, Chap5.2].

Conversely, using(4.2.2.12), we first factorize a $p = f \circ i$, where i is a trivial cofibration, then because $p \in r(i)$, pis a retraction of f hence a fibration. And similarly for cofibrations and weak equivalences. □

Cor. (4.5.0.5). In a model category,
trivial fibrations= r(cofibrations),
trivial cofibrations= l(fibrations). ⌟

Proof: The proof is the same as that of(4.5.0.4). □

Cor. (4.5.0.6). In a model category, the class of (trivial)fibrations is stable under base change and the class of (trivial)cofibrations is stable under cobase change. ⌟

Prop. (4.5.0.7). Let p be a fibration in C_{cf}, then $p \in r(\mathrm{Cof})$ iff $\gamma(p)$ is an isomorphism, Cf.[Quillen 5.2]. So if conditions of(4.5.0.4) are satisfied (i.e. C is a closed model category), $\gamma(f)$ is an isomorphism iff f is a weak equivalence by the characterization of weak-equivalence of(4.5.0.4). ⌟

Proof: □

Def. (4.5.0.8) [Left Proper Model Categories]. A model category is called **left proper** if weak equivalences are stable under cobase change by cofibrations. Dually it is called **right proper** if weak equivalences are stable under base change by fibrations. ⌟

Prop. (4.5.0.9) [Cofibration is Left Proper]. For a pushout diagram

$$\begin{array}{ccc} A & \xrightarrow{i} & B \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j'} \\ A' & \xrightarrow{i'} & B' \end{array}$$

in a model category $\mathcal{C}$, if i is cofibration and A, A' are cofibrant, and j is weak equivalence, then j' is also weak equivalence. ⌟

Proof: It suffices to show j' is an isomorphism in $\mathrm{Ho}(\mathcal{C})$(4.5.1.15). For this, by Yoneda lemma, it suffices to show $\mathrm{Hom}_{\mathrm{Ho}(\mathcal{C})}(B', Z) \cong \mathrm{Hom}_{\mathrm{Ho}(\mathcal{C})}(B, Z)$ for any fibrant object Z.

For surjectivity, by(4.5.1.18), it suffices to show $\pi(B', Z) \cong \pi(B, Z)$. Given a map $f : B \to Z$, because j is weak equivalence, there is a map $g : A' \to Z$ that $g \circ j \sim f \circ i$. Then by(4.5.1.10), there is a $f' \sim f$ that $f' \circ i = g \circ j$, which determines a morphism $B' \to Z$.

For injectivity, If P is a path object that $H : B \to P$ induces a homotopy between maps $s \circ j', s' \circ j'$, then we need to extend this homotopy to $\widetilde{H} : B' \to P$, and the method is the argument is the same as above. □

Cor. (4.5.0.10). If $\mathcal{M}$ is a model category s.t. each object is cofibrant, then $\mathcal{M}$ is left proper. ⌟

1 Homotopies

Def. (4.5.1.1)[Cylinder Objects]. A **cylinder object** for an object X is an object $X \wedge I$ which gives a factorization of the natural map $X \coprod X \to X$ as $X \coprod X \xrightarrow{i} X \wedge I \xrightarrow{j} X$, where $j \in W$. It is called a **good cylinder object** if i is a cofibration, and **very good cylinder object** if j is trivial fibration. By factorization axiom, every object has a very good cylinder object.

There are two natural morphisms $X \mapsto X \wedge I$, denoted by ∂_0 and ∂_1.

Dually we can define **path object** Y^I for Y, and every object has a very good path object. ⌟

Prop. (4.5.1.2). If A is cofibrant and $A \wedge I$ is a cylinder object for A, then $\partial_i : A \to A \times I$ are trivial cofibrations. ⌟

Proof: Because it's pushout of $\varnothing \to A$ and $\sigma \circ \partial_i = \mathrm{id}_A$. □

Cor. (4.5.1.3). if $f \sim^l g$, then f is a weak equivalence iff g is a weak equivalence. ⌟

Proof: This is because $f = H \circ \partial_0, g = H \circ \partial_1$, and we can use(4.5.1.2). □

Def. (4.5.1.4) [Homotopies]. Two morphisms $f, g : X \to Y$ are called **(good/very good) left homotopic**, denoted by $f \sim^l g$ iff there is a (good/very good) cylinder object $X \coprod X \to X \wedge I$ with $X \wedge I \to Y$ that induce $(f, g) : X \coprod X \to Y$. Dually for right homotopies. And we denote by $\pi^l(A, B)/\pi^r(A, B)$ the equivalence classes of $\mathrm{Hom}(A, B)$ under the equivalence relation generated by left/right homotopies.

If $f, g \in \mathrm{Hom}(X, Y)$ and $\varphi \in \mathrm{Hom}(Y, Z)$ that $\varphi \circ f = \varphi \circ g$, then f, g is called **left homotopic over** Z if there is a homotopy H of $f \sim^l g$ that φH is the trivial homotopy. Dually for **right homotopic under** X. ⌟

Lemma (4.5.1.5) [Very Good Homotopies]. For $f, g \in \mathrm{Hom}(X, Y)$, if $f \sim^l g$, then f, g are good left homotopic. And if Y if fibrant, then f, g are moreover very good left homotopic. ⌟

Proof: The first assertion is each, just choose a factorization of the cylinder object $X \coprod X \xrightarrow{i} X \wedge I' \xrightarrow{j} X \wedge I$ that i is cofibrant. If Y is fibrant, then we further factorize $X \wedge I' \xrightarrow{i} X \wedge I'' \xrightarrow{j} X$, where i is cofibrant and j is trivial fibration, then by two out of three, i is also trivial cofibration, and it suffices to extend the homotopy $X \wedge I' \to Y$ to $X \wedge I'' \to Y$, and this is because Y is fibrant. □

Prop. (4.5.1.6) [Homotopy is Equivalence Relation]. If A is cofibrant, then the left homotopy is an equivalence relation on $\mathrm{Hom}(A, B)$. ⌟

Proof: Reflexivity and symmetry is trivial, the only problem is transitivity, so we construct a glueing $A \wedge I''$ as the pushout of $\partial_1 : A \to A \wedge I$ and $\partial_0' : A \to A \wedge I'$. $A \wedge I'' \to A$ is a weak equivalence by the universal property and(4.5.0.4), so this is a cylinder object. The rest is easy. □

Prop. (4.5.1.7) [Properties of Left Homotopies]. If A is cofibrant and $f, g \in \mathrm{Hom}(A, B)$, then

1. If f, g are right homotopic, then $s \to B^I$ can be chosen to be trivial Cof.
2. If f, g are right homotopic, then so does $uf \sim ug$ or $fv \sim gv$. Thus if A is cofibrant, there is a composition map: $\pi^r(A, B) \times \pi^r(B, C) \to \pi^r(A, C)$.
3. For any trivial fibration $X \to Y$, $\pi^l(A, X) \to \pi^l(A, Y)$ is a bijection.

And dual arguments hold for fibrant objects. ⌟

Proof:

1. factorize $B \to B^I$ to $B \to B^{I'} \to B^I$ where $B \to B^{I'} \in TCof$ and $B^{I'} \to B^I \in W$, so $B^{I'}$ is also a cylinder object and the homotopy $A \to B^I$ can be lifted to $A \to B^{I'}$.
2. there is a diagram
$$\begin{CD} B @>{su}>> C^I \\ @V{s}VV @VV{(d_0,d_1)}V \\ B^I @>{(d_0u, d_1u)}>> C \times C \end{CD}$$
which has a lifting φ, then composed with $A \to B^I$ will give the desired homotopy.
3. the map is well-defined, it is surjective because of lifting property, and it is injective because $A \coprod A \to A \times I \in \mathrm{Cof}$ so the homotopy can be lifted to X.
Cf.[Homotopy Theories and Model Categories, P20, 21].

□

Lemma (4.5.1.8) [Left and Right Homotopies]. If X is cofibrant, then for $f, g \in \mathrm{Hom}(X, Y)$, if $f \sim_l g$, then $f \sim_r g$. And the dual conclusion holds for Y fibrant.

In particular, for morphisms between bifibrant objects, left and right homotopic are equivalent. ⌟

Proof: Consider a cylinder object $j : X \wedge I \to X$ for X and a path object for Y. Soppse f, g are left homotopic via a map $H : X \wedge I \to Y$, then we consider the diagram

$$\begin{array}{ccc} X & \xrightarrow{f} Y \longrightarrow & Y^I \\ \Big\downarrow{\scriptstyle \partial_1} & \nearrow & \Big\downarrow \\ X \wedge I & \xrightarrow{(f\circ j)\times H} & Y \times Y \end{array} .$$

Then it can be solved by some $\widetilde{H}$ because ∂_1 is trivial cofibration(4.5.1.2), and then it can be checked $H \circ \partial_1$ gives the desired right homotopy. □

Prop. (4.5.1.9) [Whitehead's Theorem]. Let $X, Y \in \mathcal{C}$ be bifibrant, then a map $f : X \to Y$ is an equivalence iff there is a $g : X \to Y$ that fg and gf are homotopic to id. ⌟

Proof: Cf.[Homotopy Theories and Model Categories, P23]. □

Prop. (4.5.1.10) [Lifting Criterion]. Let $\mathcal{C}$ be a model category and $i : A \to B$ be a cofibration between cofibrant objects, and X is fibrant, $g : B \to X, f : A \to X$ satisfies $g \circ i \sim f$, then there is a $g' \sim g$ that $g' \circ i = f$. ⌟

Proof: Choose a good cylinder object $C(A)$ for A and factorize

$$C(A) \coprod_{A \coprod A} (B \coprod B) \to C(B) \to B$$

where the first map is cofibration and the second is trivial fibration, then $C(B)$ is a good cylinder object for B.

The homotopy is given by a map $C(A) \coprod_A B \to X$, and we check $(A) \coprod_A B \to C(B)$ is a trivial cofibration(check $C(A) \coprod_A B \to B$ is weak equivalence using(4.5.0.6) and check $C(A) \coprod_A B \to C(A) \coprod_{A \coprod A}(B \coprod B)$ is a cofibration as a cobase change of $A \to B$ and $C(A) \coprod_{A \coprod A}(B \coprod B) \to C(B)$ is a cofibration by definition), so the homotopy extends to a homotopy $C(B) \to X$, which is a homotopy between g and some g' and $g' \circ i = f$. □

Def. (4.5.1.11). Let C_c, C_f, C_{cf} denote the full subcategory of cofibrant, fibrant and cofibrant-fibrant objects. And we define πC_c as the category module right homotopy equivalence between morphisms, dually for πC_f.

Notice(4.5.1.7) assures $\pi C_c, \pi C_f$ are truly categories.

Notice for C_{cf}, left homotopy is equivalent to right homotopy by(4.5.1.8), so πC_{cf} is full subcategory for both πC_c and πC_f. ⌟

Lemma (4.5.1.12) [Fibrant and Cofibrant Replacement]. For an object X in a model category $\mathcal{C}$, the axioms show there is a cofibrant object QX and a trivial fibration $QX \to X$. Also there is a fibrant object RX and a trivial cofibration $X \to RX$. We fix choices of Q, R that is identity on bifibrant objects, and consider it a mapping from $\mathcal{C}$ to $\mathcal{C}$.

Then given any morphism $f : X \to Y$, there is a morphism $\widetilde{f} : QX \to QY$ lifting f, and $\widetilde{f}$ depends up to left and right homotopy only on f. And if Y is fibrant, then it depends up to left and right homotopy only on the left homotopy classes of f.

Dually assertions also holds, so we have functors: $Q : \mathcal{C} \to \pi\mathcal{C}_c$ and $R : \mathcal{C} \to \pi\mathcal{C}_f$. ⌟

Proof: The existence of the lifting follows from the fact QX is fibrant and $QY \to Y$ is trivial fibration. The uniqueness of left homotopy follows from(4.5.1.7), and also right homotopy, because QX is cofibrant and use(4.5.1.8). For the last assertion, notice when Y is fibrant,(4.5.1.7) shows the left homotopy class of $QX \to Y$ is determined, and use(4.5.1.7) again, the class of $\widetilde{f}$ is also determined. □

Cor. (4.5.1.13). The restrictions define functors $Q' : \pi\mathcal{C}_c \to \pi\mathcal{C}_{cf}$ and $R' : \pi\mathcal{C}_f \to \pi\mathcal{C}_{cf}$. ⌟

Def. (4.5.1.14) [Homotopy Category]. For any model category $\mathcal{C}$, we construct a **homotopy category** $\mathrm{Ho}(\mathcal{C})$ whose objects are the same as $\mathcal{C}$, but $\mathrm{Hom}_{\mathrm{Ho}(\mathcal{C})}(X,Y) = \mathrm{Hom}_{\pi C_{cf}}(RQX, RQY) = \pi(RQX, RQY)$.

There is a functor $\gamma : \mathcal{C} \to \mathrm{Ho}(\mathcal{C})$ by sending X to RQX, by(4.5.1.12). ⌟

Prop. (4.5.1.15) [Weak Equivalence and Isomorphisms]. A morphism in $\mathcal{C}$ maps to an isomorphism in $\mathrm{Ho}(\mathcal{C})$ iff it is a weak equivalence. The morphisms in $\mathrm{Ho}(\mathcal{C})$ are generated by the image of morphisms in $\mathcal{C}$ and the inverse of images of weak equivalences in $\mathcal{C}$. ⌟

Proof: If $f \in \mathcal{C}$ is a weak equivalence, then $f' = RQ(f)$ is also a weak equivalence, by two out of three lemma. Then Whitehead theorem(4.5.1.9) shows f' is an isomorphism in πC_{cf} hence in $\mathrm{Ho}(\mathcal{C})$. Conversely, if f' has an inverse in $\mathrm{Ho}(\mathcal{C})$, then f' is a weak equivalence by Whitehead(4.5.1.9) again, and so is f.

For the last assertion, just notice $\mathrm{Hom}(RQX, RQY) \to \mathrm{Hom}_{\mathrm{Ho}(\mathcal{C})}(X,Y)$ is a surjection, and $X \to RQX, Y \to RQY$ are weak equivalence hence are isomorphisms in $\mathrm{Ho}(\mathcal{C})$. □

Cor. (4.5.1.16). If $F, G : \mathrm{Ho}(\mathcal{C}) \to \mathcal{D}$ are two functors and $t : F\circ\gamma \to G\circ\gamma$ is a natural transformation, then t also gives a natural transformation $F \to G$. ⌟

Proof: This is because the objects of $\mathrm{Ho}(\mathcal{C})$ are the same as that of $\mathcal{C}$, and the morphisms are generated by $\gamma(f)$ and $\gamma(g)^{-1}$ where g is a weak equivalence. Then the desired transformation commutative diagrams commute. □

Lemma (4.5.1.17). Let $\mathcal{C}$ be a model category and $F : \mathcal{C} \to \mathcal{D}$ be a functor taking weak equivalences to isomorphisms, then if $f \sim^l g$ or $f \sim^r g$, $F(f) = F(g)$. ⌟

Proof: We only prove for left homotopy and the right homotopy is dual: given the cylinder object $A \wedge I$, just need to prove that $F(\partial_0) = F(\partial_1)$. □

Prop. (4.5.1.18). Suppose A is cofibrant and X is fibrant, then the map $\gamma : \mathrm{Hom}(A,X) \to \mathrm{Hom}_{\mathrm{Ho}(C)}(A,X)$ is surjective, and induces a bijection $\pi(A,X) \cong \mathrm{Hom}_{\mathrm{Ho}(C)}(A,X)$. ⌟

Proof: (4.5.1.17) shows γ identifies homotopic maps. Consider the following commutative diagram:

$$\begin{array}{ccc} \pi(RA, QX) & \longrightarrow & \pi(A,X) \\ \downarrow\gamma & & \downarrow\gamma \\ \mathrm{Hom}_{\mathrm{Ho}(\mathcal{C})}(RA, QX) & \longrightarrow & \mathrm{Hom}_{\mathrm{Ho}(\mathcal{C})}(A,X) \end{array}.$$

The second vertical arrow is isomorphism by(4.5.1.15), the first arrow is isomorphism by(4.5.1.7). The left vertical arrow is identity by construction, so the right vertical arrow is also isomorphism. □

Cor. (4.5.1.19). There is a natural isomorphism $\pi\mathcal{C}_{cf} \cong \mathrm{Ho}(\mathcal{C})$. ⌟

Prop. (4.5.1.20) [Homotopy Category as Localizing Category]. Let $\mathcal{C}$ be a model category and W the class of weak equivalences, then the functor $\gamma : \mathcal{C} \to \mathrm{Ho}(\mathcal{C})$ is the localizing category of $\mathcal{C}$ w.r.t W. ⌟

Proof: Cf.[Homotopy Theories and Model Categories, P29].**?** □

2 Quillen Adjunctions and Derived Functors

Def. (4.5.2.1) [Quillen Adjunctions]. An adjunction $(F, G) : \mathcal{C} \rightleftarrows \mathcal{D}$ between model categories is called a **Quillen adjunction** if F preserves cofibrations and G preserves fibrations. By adjointness and(4.5.0.4), in fact F preserves also trivial cofibrations and G preserves trivial fibrations.

Moreover, it is called a **Quillen equivalence** if for any cofibrant object $C \in \mathcal{C}$ and fibrant object $D \in \mathcal{D}$, a map $C \to G(D)$ is a weak equivalence iff the adjoint map $F(C) \to D$ is a weak equivalence. ⌟

Def. (4.5.2.2) [Derived Functors]. Let $\mathcal{C}$ be a model category and $F : \mathcal{C} \to \mathcal{D}$ a functor, then a **left derived functor** of F is a left Kan extension of F along $\gamma : \mathcal{C} \to \mathrm{Ho}(\mathcal{C})$.

Dually we can define **right derived functors**. ⌟

Prop. (4.5.2.3) [Existence of Derived Functors]. In the situation of(4.5.2.2), if F maps weak equivalences between cofibrant objects to isomorphisms in $\mathcal{D}$, then the left derived functor (LF, t) exists, and for each cofibrant object X, the morphism $t_X : LF(X) \to F(X)$ is an isomorphism.

Dually for the right derived functor case. ⌟

Proof: Cf.[Homotopy Theories and Model Categories, P42]. □

Lemma (4.5.2.4). Let $\mathcal{C}$ be a model category and $F : \mathcal{C}_c \to \mathcal{D}$ be a functor that maps trivial cofibrations in C_c to isomorphisms, then F maps right-homotopic morphisms to the same morphism. ⌟

Proof: Let $H : A \to B^I$ be a right homotopy between f and g, where B^I is a very good path object(4.5.1.5), then $B \to B^I$ is a trivial cofibration, and thus mapped by F to an isomorphism. Then we can show $F(\partial_0) = F(\partial_1)$, and then $F(f) = F(g)$. □

Def. (4.5.2.5) [Total Left Derived Functors]. Let $F : \mathcal{C} \to \mathcal{D}$ be a morphism of model categories, then a **total derived functor**

$$LF : \mathrm{Ho}(\mathcal{C}) \to \mathrm{Ho}(\mathcal{D})$$

is defined to be a left derived functor of the morphism $\mathcal{C} \to \mathcal{D} \to \mathrm{Ho}(\mathcal{D})$. ⌟

Lemma (4.5.2.6) [Brown]. Let F be a morphism of model categories that maps trivial cofibration between cofibrant objects to weak equivalences, then it preserves weak equivalences between cofibrant objects. ⌟

Proof: If $f : A \to B$ is a weak equivalence between cofibrant objects, then we can factor the morphism $(f, \mathrm{id}) : A \coprod B \to B$ as $A \coprod B \xrightarrow{q} C \xrightarrow{p} B$ that q is cofibration and p is trivial fibration. It can be shown that $q \circ \partial_i : B \to C$ are trivial fibrations and C is cofibrant, thus $F(q \circ \partial_i)$ are weak equivalences, and hence also $F(p)$ is weak equivalence and so does $F(f)$. □

Prop. (4.5.2.7) [Total Derived Functors and Quillen Equivalence]. If (F, G) is a pair of Quillen functors between two model categories $\mathcal{C}, \mathcal{D}$, then total derived functors

$$LF : \mathrm{Ho}(\mathcal{C}) \rightleftarrows \mathrm{Ho}(\mathcal{D}) : RG$$

exists and form an adjunction pair. And if (F, G) is a Quillen equivalence, then (LF, RG) defines an equivalence of homotopy categories. ⌟

Proof: By(4.5.2.3) and its dual and(4.5.2.6), the total derived functors LF, RG exist.

Next for A cofibrant in $\mathcal{C}$ and X fibrant in $\mathcal{D}$, we can show the adjunction map $\mathrm{Hom}(A, G(X)) \cong \mathrm{Hom}(F(A), X)$ preserves homotopy equivalence relations(4.5.1.8) and induces an isomorphism $\pi(A, G(X)) \cong \pi(F(A), X)$: If $H : A \wedge I \to X$ is a good homotopy between f, g, then $A \wedge I$ is cofibrant, and because F preserves colimits and because of(4.5.2.6), $F(A \wedge I)$ is cylinder object for $F(A)$, thus $f^\flat \sim g^\flat$. A dual argument shows the converse.

Now for any $A \in \mathcal{C}$ and $X \in \mathcal{D}$, there is a bijection

$$\mathrm{Hom}_{\mathrm{Ho}(\mathcal{C})}(A, RG(X)) \cong \pi(QA, G(SX)) \cong \pi(F(QA), SX) \cong \mathrm{Hom}_{\mathrm{Ho}(D)}(LFA, X)$$

where the first isomorphism is due to the fact $QA \to RQA$ is trivial cofibration and $G(SX)$ is fibrant, thus we can use(4.5.1.7), dually for the last isomorphism.

Finally if (F, G) is a Quillen equivalence, then consider the unit map:

$$A \to RG(LF(A)).$$

If A is cofibrant, then this is $A \to G(SF(A))$ which is a weak equivalence because $F(A) \to SF(A)$ does, so it is an isomorphism in $\mathrm{Ho}(\mathcal{C})$. Now any object in $\mathrm{Ho}(C)$ is isomorphic to a cofibrant object, we know the unit map is an isomorphism. Dually the counit map is an isomorphism, thus LF, GF are a pair of equivalences. □

3 Combinatorial Model Structure

Cf.[HTT, A.2.6]

Def. (4.5.3.1) [Cofibrantly-Generated Model Categories]. A **cofibrantly-generated model category** is a model category $\mathcal{C}$ that

- there is a small set I of generating cofibrations that generates the class of cofibrations as the minimal weakly saturated class containing I.
- there is a small set J of generating trivial cofibrations that generates the class of trivial cofibrations as the minimal weakly saturated class containing J.

⌟

Def. (4.5.3.2) [Combinatorial Model Categories, Smith]. A **combinatorial model category** is a cofibrantly generated(4.5.3.1) and locally presentable(4.1.2.5) model category. ⌟

Prop. (4.5.3.3) [Smith]. Let $\mathcal{M}$ be a combinatorial model category and $\mathcal{M}^{[1]}$ the category of arrows, then the full subcategory generated by fibrations, weak equivalences, or trivial fibrations are all full accessible(4.1.2.4) subcategories of $\mathcal{M}^{[1]}$. ⌟

Proof: Cf.[Lur09]P818. □

Prop. (4.5.3.4) [Constructing Combinatorial Model Categories]. Let $\mathcal{M}$ be a locally presentable category and W, C be classes of morphisms in $\mathcal{M}$ s.t.

- C is a weakly saturated class generated by a small subset C_0.
- $C \cap W$ is a weakly saturated class.
- $W \subset A^{[1]}$ is a full accessible subcategory.
- W satisfies the 2-out-of-3 property.

- $r(C) \subset W$.

Then $\mathcal{M}$ admits a combinatorial model category with

- Cofibrations: C.
- Weak equivalences: W.
- Fibrations: $r(C \cap W)$.

⌟

Proof: Cf.[Lur09]P821. □

Lemma (4.5.3.5). Situation as in(4.5.3.4), the class $C \cap W$ is a weakly saturated class generated by a small subset $S \subset C \cap W$. ⌟

Proof: Cf.[Lur09]P819. □

Prop. (4.5.3.6) [Constructing Left Proper Model Categories]. Let $\mathcal{M}$ be a locally presentable category with a class W of morphisms and a small set of morphisms C_0 s.t.

- W is a perfect class?,
- C_0 is stable under cobase change.
- W is stable under cobase change by C_0.
- $r(C_0) \subset W$.

Then there is a left proper combinatorial model category on $\mathcal{M}$ with

- Cofibrations: The weakly saturated closure C of C_0.
- Weak Equivalences: W.
- Fibrations: $r(C \cap W)$.

Moreover, any left proper combinatorial model category arises in this way. ⌟

Proof: Cf.[Lur09]P823. □

4 Generating new Model Categories

Prop. (4.5.4.1) [Overcategories and Undercategories]. If $\mathcal{C}$ is a model category and $A \in \mathcal{C}$, then the undercategory $\mathcal{C}_{A/}$ and the overcategory $\mathcal{C}_{/A}$ have natural model structures. ⌟

Proof: □

Prop. (4.5.4.2) [Transfer Model Structures via Left Adjoint]. Let

$$F : \mathcal{C} \rightleftarrows \mathcal{D} : G$$

be an adjoint pair of categories and

- $\mathcal{C}, \mathcal{D}$ are complete and cocomplete,
- $\mathcal{C}$ is a cofibrantly generated model category,
- $\mathcal{C}, \mathcal{D}$ are presentable categories and G is an accessible functor.
- If we define a morphism f in $\mathcal{B}$ a fibration/weak equivalent iff $G(f)$ is a fibration/weak equivalence, and a cofibration iff it has left lifting property w.r.t. trivial fibrations, then $\mathcal{B}$ has a path object factorization and a fibrant replacement operator.

Then this defines a cofibrantly generated model category on $\mathcal{B}$, and makes (F, G) a Quillen adjunction. ⌟

Proof: It suffices to show that the factorization property holds: In fact, it suffices to show if I, J are generating classes of cofibrations and trivial cofibrations, then $F(I)$, $F(J)$ are generating classes of cofibrations and trivial cofibrations. But this suffices to show $F(J)$ is are weak equivalence. For this, show that any morphism in $\mathcal{B}$ that has left lifting properties w.r.t. all fibrations is a weak equivalence using hypothesis item4.**?** □

Bousfield Localizations

Cf.[P.S. Hirschhorn. Model categories and their localizations].

Def. (4.5.4.3) [Bousfield Localizations]. Let $\mathcal{M}, \mathcal{M}'$ be model categories with the same underlying category, then $\mathcal{M}'$ is called a **Bousfield localization** of $\mathcal{M}$ if

- $\mathrm{Cof}(\mathcal{M}) = \mathrm{Cof}(\mathcal{M}')$.
- $\mathrm{Weak}(\mathcal{M}) \subset \mathrm{Weak}(\mathcal{M}')$.

⌟

5 Enriched and Monoidal Model Categories

Def. (4.5.5.1) [Left Quillen Bifunctor]. Let $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be model categories, then a functor $\mathcal{A} \times \mathcal{B} \to \mathcal{C}$ is called a **left Quillen bifunctor** if

- For any cofibrations $i : A \to A' \in \mathcal{A}, B \to B' \in \mathcal{B}$, the induced map
$$i \wedge j : F(A', B) \coprod_{F(A,B)} F(A, B') \to F(A', B')$$
is a cofibration in $\mathcal{C}$.
- F preserves small colimits separably in each variables.

⌟

Def. (4.5.5.2) [Monoidal Model Category]. A **monoidal model category** is a monoidal category $\mathcal{S}$ equipped with a model structure that:

- The tensor product $\otimes : S \times S \to S$ is a left Quillen bifunctor.
- The unit objects $1 \in \mathcal{S}$ is cofibrant.
- The monoidal structure is closed.

⌟

Def. (4.5.5.3) [Enriched Model Category]. Given a monoidal model category $\mathcal{S}$, an $\mathcal{S}$**-enriched model category** is an $\mathcal{S}$-enriched category $\mathcal{A}$ with a model structure satisfying:

- $\mathcal{A}$ is tensored and cotensored over $\mathcal{S}$**?**.
- the tensor product $\mathcal{A} \times \mathcal{S} \to \mathcal{S}$ is a left Quillen bifunctor(4.5.5.1).

⌟

Prop. (4.5.5.4). The second condition in(4.5.5.3) is equivalent to the following: For a cofibration $i : U \to V$ and a fibration $p : X \to Y$, the induced map
$$\mathrm{Map}(V, X) \xrightarrow{(i^*, p_*)} \mathrm{Map}(U, X) \times_{\mathrm{Map}(U,Y)} \mathrm{Map}(V, Y)$$
is a fibration in $\mathcal{S}$, and trivial fibration if any of i, p is weak equivalence. ⌟

Proof: Use the adjunction relations to write it out?. □

Def. (4.5.5.5) [Fibrant Enriched Categories]. Let $\mathcal{A}$ be a $\mathcal{S}$-enriched category, the we denote $\mathcal{A}^\circ$ the subcategory of bifibrant objects of $\mathcal{A}$, which is also a $\mathcal{S}$-enriched category. ⌟

6 Diagram Categories

[Lur09]A.2.8. A.3.3., A.3.5.

Prop. (4.5.6.1) [(Injective)Projective Model Categories]. Let S be an excellent model category and $\mathcal{A}$ a combinatorial $\mathcal{S}$-enriched model category, $\mathcal{C}$ a small $\mathcal{S}$-enriched category, then there are two model structures on $\mathcal{A}^{\mathcal{C}}$:

- The **projective model category** $\mathrm{Func}(\mathcal{C}, A)_{\mathrm{Proj}}$ with
  - Fibrations: **projective fibrations** F s.t. $F(C) \to G(C)$ is a fibration in $\mathcal{A}$ for each $C \in \mathcal{C}$.
  - Weak equivalences: F s.t. $F(C) \to G(C)$ is a weak equivalence in $\mathcal{A}$ for each $C \in \mathcal{C}$.
  - Cofibrations: **projective cofibrations** determined by the above two.
- The **injective model category** $\mathrm{Func}(\mathcal{C}, A)_{\mathrm{inj}}$ with
  - Cofibrations: **injective cofibrations** F s.t. $F(C) \to G(C)$ is a cofibration in $\mathcal{A}$ for each $C \in \mathcal{C}$.
  - Weak equivalences: F s.t. $F(C) \to G(C)$ is a weak equivalence in $\mathcal{A}$ for each $C \in \mathcal{C}$.
  - Fibrations: **injective fibrations** determined by the above two.

⌟

Proof: Cf.[Lur09]P868, P828. □

Cor. (4.5.6.2). Both model categories are left/right proper iff $\mathcal{A}$ is. ⌟

Cor. (4.5.6.3). Projective cofibrations are injective cofibrations, and injective fibrations are projective fibrations. ⌟

Prop. (4.5.6.4). Let $\mathcal{C}$ be a model category and let

$$\begin{array}{ccc} A & \xrightarrow{j} & A_1 \\ \downarrow{\scriptstyle i} & & \downarrow \\ A_0 & \longrightarrow & A_0 \coprod_A A_1 \end{array}$$

be a pushout diagram, then it is a homotopy pushout diagram if either of the following is satisfied:

- j is a cofibration and A, A_0 are cofibrant.
- j is a cofibration and $\mathcal{C}$ is left proper.

⌟

Proof:

□

Reedy Model Categories

Homotopy Colimits and Limits

Should be redone in the general language of diagram categories.?

Def. (4.5.6.5) [Homotopy Colimits and Limits]. In a model category $\mathcal{M}$, for any diagram $A_0 \leftarrow A \to A_1$, there exists a commutative diagram

$$\begin{array}{ccccc} A_0' & \xleftarrow{i} & A' & \xrightarrow{j} & A_1' \\ \downarrow & & \downarrow & & \downarrow \\ A_0 & \longleftarrow & A & \longrightarrow & A_1 \end{array}.$$

such that A' is cofibrant, and i, j are both cofibrant, and the vertical arrows are weak equivalences.

Then it can be shown that $A_0' \coprod_{A'} A_1'$ only depends on $A_0 \leftarrow A \to A_1$ up to weak equivalence. Then a commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & A_1 \\ \downarrow & & \downarrow \\ A_0 & \longrightarrow & C \end{array}$$

is called a **homotopy colimit** if for any such cofibrant replacement,

$$A_0' \coprod_{A'} A_1' \to A_0 \coprod_{A} A_1 \to C$$

is a weak equivalence.

Dually we can define homotopy limits. ⌟

Proof: ? □

Cor. (4.5.6.6). Weakly equivalent diagrams induce weakly equivalent homotopy colimits. ⌟

Prop. (4.5.6.7). In a model category $\mathcal{M}$, a diagram

$$\begin{array}{ccc} A & \xrightarrow{j} & A_1 \\ \downarrow & & \downarrow \\ A_0 & \longrightarrow & A_0 \coprod_A A_1 \end{array}$$

is a homotopy limit if j is cofibrant, and either

- A, A_0 are cofibrant, or
- $\mathcal{M}$ is left proper.

⌟

Proof: ? □

7 Model Structures on $\mathcal{C}at_{\mathcal{S}}$

Def. (4.5.7.1) [Homotopy Category]. Let $\mathcal{S}$ be a monoidal model category, then there is a natural monoidal structure on the homotopy category $h\mathcal{S}$(4.5.1.14), and the functor $S \mapsto h\mathcal{S}$ is monoidal, thus we can transfer from a category $\mathcal{C}$ enriched over $\mathcal{S}$ to an $h\mathcal{S}$-enriched category, called the **homotopy category** of $\mathcal{C}$. ⌟

Def. (4.5.7.2) [Weak Equivalences of Enriched Categories]. Let $\mathcal{S}$ be a monoidal model category and $\mathcal{C}at_{\mathcal{S}}$ be the category of categories enriched over $\mathcal{S}$, then a morphism $F : \mathcal{C} \to \mathcal{D} \in \mathcal{C}at_{\mathcal{S}}$ is called a **weak equivalence** if it induced an isomorphism of their homotopy categories, or equivalently,

- F is essentially surjective,
- For any $X, Y \in \mathcal{C}$, $\mathrm{Map}_{\mathcal{C}}(X, Y) \to \mathrm{Map}_{\mathcal{D}}(FX, FY)$ is a weak equivalence in $\mathcal{S}$.

⌟

Def. (4.5.7.3) [Generating Cofibrations in $\mathcal{C}at_{\mathcal{S}}$]. Let $\mathcal{S}$ be a monoidal model category, A is an object of $\mathcal{S}$, then we can denote $[1]_A$ the $\mathcal{S}$-enriched category consists of objects $\{X, Y\}$ and that $\mathrm{Hom}(X, X) = \mathrm{Hom}(Y, Y) = 1_{\mathcal{S}}, \mathrm{Hom}(X, Y) = A, \mathrm{Hom}(Y, X) = \varnothing$. And if 1_S is the initial object of $\mathcal{S}$, then we denote $[1]_{1_{\mathcal{S}}}$ by $[1]_{\mathcal{S}}$. Also we denote $[0]_{\mathcal{S}}$ the $\mathcal{S}$-enriched category consisting of one element and the morphism space is $1_{\mathcal{S}}$.

Let $[1]_{\mathcal{S}}^{\sim}$ be the category consisting of two objects $\{X, Y\}$ that $\mathrm{Hom}(Z_1, Z_2) = 1_{\mathcal{S}}$ for any $Z_1, Z_2 \in \mathcal{S}$.

Let C_0 be the class of morphisms in $\mathcal{C}at_{\mathcal{S}}$ consisting of

- $\varnothing \to [0]_{\mathcal{S}}$.
- The induced map $[1]_S \to [1]_{S'}$ where $S \to S'$ ranges over a generating class of cofibrations of $\mathcal{S}$.

⌟

Prop. (4.5.7.4) [Model Category on $\mathcal{C}at_{\mathcal{S}}$]. Let $\mathcal{S}$ be a combinatorial monoidal model category that every object of $\mathcal{S}$ is cofibrant and the collection of weak equivalences of $\mathcal{S}$ is stable under filtered colimits, then there exists a left proper combinatorial model structure on $\mathcal{C}at_{\mathcal{S}}$ that

- The class of cofibrations in $\mathcal{C}at_{\mathcal{S}}$ is the smallest weakly saturated class generated by C_0 defined in(4.5.7.3),
- The weak equivalences are as defined in(4.5.7.2).

⌟

Proof: Cf.[HTT, P856]. □

Cor. (4.5.7.5). Let

$$f : \mathcal{S} \rightleftarrows \mathcal{S}' : g$$

be a Quillen adjunction between monoidal model categories satisfying conditions in(4.5.7.4), then they induces a Quillen adjunction

$$F : \mathcal{C}at_{\mathcal{S}} \rightleftarrows \mathcal{C}at_{\mathcal{S}'} : G$$

and this is a Quillen equivalence if (f, g) is. ⌟

Proof:

□

Prop. (4.5.7.6). Let $\mathcal{C}, \mathcal{D}$ be $\mathcal{S}$-enriched model categories and

$$F : \mathcal{C} \underset{\text{Quillen}}{\rightleftarrows} \mathcal{D} : G$$

is a Quillen adjunction of underlying model categories. Assume every objects of $\mathcal{C}$ is cofibrant and the maps $\beta_{X,S} : S \otimes F(X) \to F(S \otimes X)$ is a weak equivalence for $X \in \mathcal{C}, S \in \mathcal{S}$ cofibrant, then the following are equivalent:

- (F, G) is a Quillen equivalence.
- G determines a weak equivalence(4.5.7.2) of the underlying $\mathcal{S}$-enriched categories $\mathcal{D}_{cf} \to \mathcal{C}_{cf}$.

⌟

Proof: Cf.[HTT, P853]. □

Def. (4.5.7.7) [Local Fibrations]. Let $\mathcal{C}$ be an $\mathcal{S}$-enriched category where $\mathcal{S}$ is a monoidal model category, then a morphism $f \in \mathcal{C}$ is called an **equivalence** if it maps to an isomorphism in $h\mathcal{C}$.

$\mathcal{C}$ is called **locally fibrant** if for any $X, Y \in \mathcal{C}$, the mapping space $\mathrm{Map}(X, Y)$ is fibrant in $\mathcal{S}$.

An $\mathcal{S}$-enriched functor $F : \mathcal{C} \to \mathcal{C}'$ is called a **local fibration** if the following conditions are satisfied:

- for any $X, Y \in \mathcal{C}$, the induced map $\mathrm{Map}(X, Y) \to \mathrm{Map}(FX, FY)$ is a fibration in $\mathcal{S}$.
- the induced map $h\mathcal{C} \to h\mathcal{C}'$ is a quasi-fibration of categories.

⌟

Def. (4.5.7.8) [Invertibility Hypothesis]. We say a monoidal model category $\mathcal{S}$ satisfies the **invertibility hypothesis** if: For any cofibrant morphism $[1]_{\mathcal{S}} \to \mathcal{C}$(4.5.7.3) of $\mathcal{S}$-enriched categories, and maps to a morphism f which is invertible in the homotopy category $h\mathcal{C}$, take the pushout:

$$\begin{array}{ccc} [1]\,\mathcal{S} & \xrightarrow{i} & \mathcal{C} \\ \downarrow & & \downarrow j \\ [1]_{\mathcal{S}}^{\sim} & \longrightarrow & \mathcal{C}\langle f^{-1}\rangle \end{array} .$$

then j is a weak equivalence of $\mathcal{S}$-enriched categories(4.5.7.2). ⌟

Def. (4.5.7.9) [Excellent Model Category]. An **excellent model category** is a monoidal model category $\mathcal{S}$ that The monoidal structure is symmetric.

- $\mathcal{S}$ is combinatorial,
- Every monomorphism in $\mathcal{S}$ is a cofibration, and the collection of cofibrations is stable under products,
- The class of weak equivalences in $\mathcal{S}$ is stable under filtered colimits,
- $\mathcal{S}$ satisfies the invertibility condition(4.5.7.8)

⌟

Lemma (4.5.7.10). Let $T : \mathcal{S} \to \mathcal{S}'$ be a monoidal functor between monoidal model categories satisfies axioms besides invertibility hypothesis, that is also a left Quillen functor, then if S' satisfies invertibility hypothesis, so does S. ⌟

Proof: Cf.[HTT, P862].**?** □

Prop. (4.5.7.11) [Fibration and Local Fibration]. If $\mathcal{S}$ is an excellent model category, then

- An $\mathcal{S}$-enriched category $\mathcal{C}$ is a fibrant object in $\mathcal{C}at_{\mathcal{S}}$ iff it is locally fibrant(4.5.7.7).
- Let $F : \mathcal{C} \to \mathcal{D}$ be an $\mathcal{S}$-enriched functor and $\mathcal{D}$ is fibrant in $\mathcal{C}at_{\mathcal{S}}$, then F is fibrant in $\mathcal{C}at_{\mathcal{S}}$ iff it is a local fibration.

⌟

Proof: Cf.[HTT, P863]. □

Path Spaces

Homotopy Colimits of Enriched Categories

8 Examples

Prop. (4.5.8.1) [Kan-Quillen Model Structure]. By(4.6.3.48), $s\,\mathcal{S}et$ is a combinatorial left and right proper Kan-Quillen model category with

- Weak equivalences: weak equivalences,
- Cofibrations: inclusions,
- Fibrations: Kan fibrations.

⌟

Prop. (4.5.8.2) [Dwyer, Kan]. $s\,\mathcal{S}et$ has an excellent model category with the Kan model structure and the Cartesian monoidal structures. ⌟

Proof: □

Prop. (4.5.8.3) [q-Model Structure]. For a unital ring R, then the category $\mathrm{Ch}_{\mathbb{N}}\,R$ has the structure of a model category with a morphism $f : M_\bullet \to N_\bullet$ being

- a weak equivalence if $H_n(f)$ is isomorphism for any n.
- a fibration if $M_n \to N_n$ is surjective for any $n \geq 1$.
- a cofibration if $M_n \to N_n$ is injective with projective cokernel for any $n \geq 0$.

⌟

Proof: [Model category and simplicial methods, P5] or [Homotopy Theories and Model Categories]. □

Prop. (4.5.8.4) [Serre-Quillen]. By(4.13.6.28), the category $\mathcal{CG}$ can be given a **Serre-Quillen model structure** with

- Weak equivalences: weak homotopy equivalence,
- Fibrations: Serre fibrations,
- Cofibrations: Retracts of morphisms $X \to Y$ where Y is obtained from X by attaching cells.

And this restricts to a model category on the category $\mathcal{CGH}$ of compactly generated weak Hausdorff spaces. ⌟

Prop. (4.5.8.5) [Hurewicz-Str∅m]. The category $\mathcal{T}op$ can be given a **Hurewicz-Str∅m model structure** with

- Weak equivalences: homotopy equivalences.
- Cofibrations: closed Hurewicz cofibrations.

- Fibrations: Hurewitz fibrations.

⌟

Proof: See(4.13.6.31). □

Prop. (4.5.8.6) [Derived Categories Model Structure]. If $\mathcal{A}$ is an Abelian category with enough injectives, then $K^+(\mathcal{A})$ is a model category with

- Weak equivalence: quasi-isomorphisms,
- Fibration: epimorphisms with ker in $K^+(\mathcal{I})$,
- Cofibration: monomorphisms.

⌟

Proof: □

Prop. (4.5.8.7) [Joyal Model Structures]. By(4.6.4.19), there is a Joyal Model category structure on $s\,\mathcal{S}\mathrm{et}$ with

- Cofibrations: monomorphisms.
- Weak equivalences: categorical equivalences defined in(4.6.4.12).
- Fibrations: **categorical fibrations** or **Joyal fibrations** which has the right lifting property w.r.t. trivial cofibrations.

⌟

Prop. (4.5.8.8) [Reedy Model Structures]. Cf.[HTT, A.2.9]. ⌟

Prop. (4.5.8.9) [Bergner-Model Structure]. There is a Bergner model structure on $s\,\mathcal{C}\mathrm{at}$**?**.(4.6.4.4) ⌟

4.6 Simplicial Homotopy Theory

Main references are [Jardine Simplicial Homotopy Theory], [Lur09].

Notation (4.6.0.1).
- Use notations from Model Categories.

⌟

1 Simplicial Objects

Def. (4.6.1.1) [Simplex Category]. The **simplex category** Δ consists of simplicial objects $[n]$ for each $n \geq 0$ and there maps are order-preserving maps.

Δ has a subcategory Δ_+ consisting of the same objects but the morphisms are all surjective order-preserving maps.

For $\mathcal{C} \in \mathcal{T}\text{op}$, a **simplicial object** in $\mathcal{C}$ is a functor $\Delta^{op} \to \mathcal{C}$. A **cosimplicial object** in $\mathcal{C}$ is a simplicial object in $\mathcal{C}^{\mathrm{op}}$. The category of simplicial objects in $\mathcal{C}$ is denoted by $s\mathcal{C}$.

Given a simplicial or cosimplicial object in $\mathcal{A}$, its **underlying degeneracy map** is defined to be**?** ⌟

Prop. (4.6.1.2). If $\mathcal{C}$ is complete or cocomplete, then so is $s\mathcal{C}$. ⌟

Def. (4.6.1.3). Δ^n is the simplicial set $\Delta^n([m]) = \mathrm{Hom}([m], [n])$. ⌟

Def. (4.6.1.4) [Augmentation]. If X is a simplicial object in a category, then an **augmentation** of X is a morphism $d : A \to X$ that $dd_0 = dd_1$. In case $\mathcal{C}$ is $\mathcal{M}\text{od}_R$, this is equivalent to a morphism $\pi_0(X) \to A$(5.8.2.2). ⌟

Def. (4.6.1.5)[s-Free Simplicial Objects]. $X \in s\mathcal{C}$ is called **s-free** if the underlying category $\Delta_+^{\mathrm{op}} \to \mathcal{C}$ is Δ^{op}-free(4.1.3.16).

Equivalently, an s-free object is a simplicial object X that there are objects $Z_n \in \mathcal{C}$ that $X_n = \coprod_{\varphi:[n]\twoheadrightarrow[k]} \varphi^* Z_k$. Moreover, a simplicial morphism of simplicial objects are called s-free if the underlying diagram $X_+ \to Y_+$ is of the form $X_+ \to X_+ \coprod Y_0$ where Y_0 is s-free. ⌟

Prop. (4.6.1.6) [$s\mathcal{C}$ is a Simplicial Category]. Let $s\mathcal{C}$ be the category of simplicial $\mathcal{C}$-objects, then it can be made into a simplicial category which is also tensored and cotensored(4.2.2.7) over $s\,\mathcal{S}\text{et}$. ⌟

Proof: We define first a action of $s\,\mathcal{S}\text{et}$ on $s\mathcal{C}$:

$$\otimes : s\,\mathcal{S}\text{et} \times s\mathcal{C} \to s\mathcal{C} : (K, X) \mapsto (K \otimes X)_n = \coprod_{K_n} X_n,$$

with the simplicial maps determined by that of K and X.

Also there is a action of $s\,\mathcal{S}\text{et}^{\mathrm{op}}$ on $s\mathcal{C}$:

$$(-)^{-} : s\,\mathcal{S}\text{et}^{op} \times s\mathcal{C} \to s\mathcal{C} : (K \otimes X)_n = \prod_{K_n} X_n$$

with the simplicial maps determined by that of K and X.

Then there is an adjointness

$$\mathrm{Hom}_{s\mathcal{C}}(K \otimes X, Y) \cong \mathrm{Hom}_{s\mathcal{C}}(X, Y^K)$$

for any simplicial set K.

Next we define $\mathrm{Map}_{s\mathcal{C}}(X,Y) \subset \mathcal{S}\mathrm{et}_\Delta$ as $(\mathrm{Map}_{s\mathcal{C}}(X,Y))_n = \mathrm{Hom}_{s\mathcal{C}}(X \otimes \Delta^n, Y)$, then there are functorial isomorphisms

$$\mathrm{Map}_{s\mathcal{C}}(K \otimes X, Y) \cong \mathrm{Map}_{s\mathcal{C}}(X, Y^K) \cong \mathrm{Map}_{\mathcal{S}\mathrm{et}_\Delta}(K, \mathrm{Map}_{s\mathcal{C}}(X,Y))$$

(easy to check). So we are done. □

Remark (4.6.1.7) [Realization Functor]. For $\mathcal{C} \in \mathcal{C}\mathrm{at}$ that has countable colimits, there is a **simplicial realization functor**

$$|-|: s\mathcal{C} \to \mathcal{C} : X \mapsto \varinjlim_{\Delta_+^{\mathrm{op}}} X_n.$$

⌟

2 Topological Categories

Def. (4.6.2.1) [Topological Categories]. A **topological category** is a category that is enriched over the category $\mathcal{CG}$ of compactly generated and Hausdorff spaces. The category of topological categories is denoted by $\mathcal{C}\mathrm{at}_{\mathcal{CG}}$.

Two topological categories is called **strongly equivalent** if they are equivalent as enriched categories. ⌟

Def. (4.6.2.2) [Homotopy Category of a Topological Category]. Given a topological category $\mathcal{C}$, the **homotopy category** $h\mathcal{C}$ of $\mathcal{C}$ is defined to be the category transferred from $\mathcal{C}$(4.2.2.4) by the right-lax monoidal functor π_0(4.1.5.14). ⌟

Def. (4.6.2.3) [Homotopy Category of Spaces]. Let $\mathcal{C}$ be the category of CW complexes that the morphisms are given the compact-open topology, then its homotopy category $\mathscr{H}$ is called the **homotopy category of spaces**. ⌟

3 Simplicial Sets

Simplicial Sets

Remark (4.6.3.1). The fact that any simplicial set X is a colimit of Δ^n (4.1.3.13) is important in proving properties of constructions of simplicial set. ⌟

Def. (4.6.3.2) [Objects and Morphisms]. Given a simplicial set S, its **objects** are just objects in $S([0])$, and its **morphisms** are objects in $S([1])$. ⌟

Def. (4.6.3.3) [Simplicial Sets and Categories]. There is an embedding $\Delta \to \mathcal{C}\mathrm{at} : [n] \to [n]$ regarding $[n]$ as a category, which by Yoneda extension(4.1.3.14) and(4.1.1.46) corresponds to an adjunction

$$\tau_1 : s\,\mathcal{S}\mathrm{et} \rightleftarrows \mathcal{C}\mathrm{at} : N$$

where τ_1 is called the **fundamental category functor** and $N : \mathcal{C}\mathrm{at} \to s\,\mathcal{S}\mathrm{et}$ is the **nerve functor**. ⌟

Prop. (4.6.3.4) [Nerve Functor is Fully Faithful]. The nerve functor $N : \mathcal{C}\mathrm{at} \to s\,\mathcal{S}\mathrm{et}$ is fully faithful. Equivalently, by(4.1.1.31), for any $\mathcal{C} \in \mathcal{C}\mathrm{at}$, there is a natural isomorphism $\tau_1(N(\mathcal{C})) \cong \mathcal{C}$. ⌟

Prop. (4.6.3.5) [Natural Transformation and Homotopy]. A natural transformation will induce homotopic nerve map. thus a pair of adjoint functors will induce a simplicial homotopy between their nerve. ⌟

Proof: □

Prop. (4.6.3.6) [Characterizing Nerves]. For $K \in s\mathcal{S}\mathrm{et}$,

- there exists $\mathcal{C} \in \mathcal{C}\mathrm{at}$ that $K \cong N(\mathcal{C})$ iff for each $0 < i < n$ and each diagram

$$\begin{array}{ccc} \Lambda_i^n & \longrightarrow & K \\ \downarrow & \nearrow & \\ \Delta^n & & \end{array}$$

  there exists uniquely a dotted arrow.

- there exists $\mathcal{C} \in \mathcal{G}\mathrm{rpd}$ that $K \cong N(\mathcal{C})$ iff for each $0 \le i \le n$ and each diagram

$$\begin{array}{ccc} \Lambda_i^n & \longrightarrow & K \\ \downarrow & \nearrow & \\ \Delta^n & & \end{array}$$

  there exists uniquely a dotted arrow.

⌟

Proof: [HTT, P9]. □

Def. (4.6.3.7) [Fundamental Groupoid Functor]. Let $\pi_1 = \mathcal{G}\mathrm{rp} \circ \tau_1 : s\mathcal{S}\mathrm{et} \to \mathcal{G}\mathrm{rpd}$, called the **fundamental groupoid functor**, then by(4.6.3.3) and(4.1.1.35), there is an adjunction

$$\pi_1 : s\mathcal{S}\mathrm{et} \rightleftharpoons \mathcal{G}\mathrm{rpd} : N$$

⌟

Def. (4.6.3.8) [Topological Realization Functor]. There is a functor $\Delta \to \mathcal{CG} : [n] \mapsto \Delta^n$, which by Yoneda extension(4.1.3.14) corresponds to an adjunction

$$|\cdot| : s\mathcal{S}\mathrm{et} \rightleftharpoons \mathcal{CG} : \mathrm{Sing}$$

called the **topological geometrization** functor and the singular complex functor. ⌟

Def. (4.6.3.9) [Classifying Spaces of a Category]. For $\mathcal{C} \in \mathcal{C}\mathrm{at}$, the **classifying space** of $\mathcal{C}$ is defined to be $\mathbb{B}\mathcal{C} = |N(\mathcal{C})| \in \mathcal{CG}$. ⌟

Prop. (4.6.3.10). The geometrization as a functor from $s\mathcal{S}\mathrm{et} \to \mathcal{CG}$ preserves finite limits.

The three kinds of geometrization of a bisimplicial set is the same: geometrization the diagonal simplicial set, the twice geometrization of left(resp. right) simplicial set. ⌟

Proof: Cf.[Jardine P9].? □

Def. (4.6.3.11) [Weak (Homotopy) Equivalences]. A morphism of simplicial sets $S \to T$ is called a **weak equivalence** if the induced map $|S| \to |T|$(4.6.3.8) is a weak homotopy equivalence. ⌟

Constructing Simplicial Sets

Def. (4.6.3.12)[Opposite Simplicial Sets]. There is an involution in the simplex category $\iota : \Delta \to \Delta$ that maps any ordered set to its reverse order. Then for any simplicial set $S : \Delta^{\mathrm{op}} \to \mathcal{S}\mathrm{et}$, there is another simplicial set $S^{\mathrm{op}} = S \circ \iota$, called the **opposite simplicial set**. ⌟

Prop. (4.6.3.13). For $\mathcal{C} \in \mathcal{C}\mathrm{at}$, there is a natural isomorphism of simplicial sets $N(\mathcal{C})^{\mathrm{op}} \cong N(\mathcal{C}^{\mathrm{op}})$. ⌟

Def. (4.6.3.14) [Mapping Spaces]. For $X, Y \in s\,\mathcal{S}\mathrm{et}$, the **mapping space** $\mathrm{Map}(X, Y)$ or Y^X is a simplicial set s.t.

$$\mathrm{Map}(X, Y)_n = \mathrm{Hom}_{s\,\mathcal{S}\mathrm{et}}(\Delta^n \times X, Y).$$

⌟

Prop. (4.6.3.15) [Closed Cartesian Monoidal Structure]. $s\,\mathcal{S}\mathrm{et}$ is a closed Cartesian monoidal category, and for any $X, Y, Z \in s\,\mathcal{S}\mathrm{et}$, there is an isomorphism of simplicial sets

$$\mathrm{Map}(X, \mathrm{Map}(Y, Z)) \cong \mathrm{Map}(X \times Y, Z).$$

⌟

Proof:

□

Prop. (4.6.3.16). For $\mathcal{A}, \mathcal{B} \in \mathcal{C}\mathrm{at}$, then there is a natural isomorphism of simplicial sets $N(\mathrm{Func}(\mathcal{A}, \mathcal{B})) \cong \mathrm{Map}(N(\mathcal{A}), N(\mathcal{B}))$. ⌟

Proof: There are natural bijections

$$\begin{aligned} N(\mathrm{Func}(\mathcal{A}, \mathcal{B}))_n &= \mathrm{Func}([n] \times \mathcal{A}, \mathcal{B}) \\ (4.6.3.4) &\cong \mathrm{Map}(N([n] \times \mathcal{A}), N(\mathcal{B})) \\ &\cong \mathrm{Map}(\Delta^n \times N(\mathcal{A}), N(\mathcal{B})) \\ &= \mathrm{Map}(N(\mathcal{A}), N(\mathcal{B}))_n, \end{aligned}$$

and they form an isomorphism of simplicial sets. □

Cor. (4.6.3.17). For any $x \in S_m, x' \in S'_n$, there is a unique $y \in (S * S')_{m+n+1}$ s.t. $y|_{[0,\ldots,m]} \cong x, y|_{[m+1,\ldots,m+n+1]} \cong x'$. ⌟

Def. (4.6.3.18) [Joins]. Let $S, S' \in s\,\mathcal{S}\mathrm{et}$, then the **join** of S, S' is defined to be the simplicial set that for all any finite ordered set J,

$$(S \star S')(J) = \cup_{J = I \coprod I'} S(I) \times S(I').$$

where I, I' satisfies $i < i'$ for any $i \in I, i' \in I'$. And the glueing is natural. ⌟

Prop. (4.6.3.19).

- $\Delta^i \star \Delta^j \cong \Delta^{i+j+1}$.
- The join operation is a functor $s\,\mathcal{S}\mathrm{et} \to s\,\mathcal{S}\mathrm{et}$ that preserves colimits in each coordinate,
- $s\,\mathcal{S}\mathrm{et}$ is a symmetric monoidal category under the join operation.
- If $\mathcal{C}, \mathcal{C}' \in \mathcal{C}\mathrm{at}$, there is a natural isomorphism $N(\mathcal{C}) \star N(\mathcal{C}') \cong N(\mathcal{C} \star \mathcal{C}')$.

⌟

Proof: All these are clear. □

Def. (4.6.3.20) [Cones]. For a simplicial set K, the **left/right cone** of K are defined to be the join $K^{\triangleleft} = \Delta^0 \star K$ and $K^{\triangleright} = K \star \Delta^0$.

For a map $f : X \to S$, the **left/right cone** of f are defined to be $S \coprod_X X^{\triangleleft}$ and $S \coprod_X X^{\triangleright}$. ⌟

Example (4.6.3.21). $(\Lambda^2_2)^{\triangleleft} \cong (\Lambda^2_0)^{\triangleright} \cong \Delta^1 \times \Delta^1$. ⌟

Def. (4.6.3.22) [Overcategories and undercategories]. For $p : K \to S \in s\mathcal{S}\mathrm{et}$, there is a simplicial set $S_{/p}$ that

$$\mathrm{Hom}(Y, S_{/p}) \cong \mathrm{Hom}_p(Y \star K, S) \stackrel{\Delta}{=} \mathrm{Hom}_{s\mathcal{S}\mathrm{et}_{K/}}(Y \star K, S)$$

And dually we can define the **undercategories**.

There are canonical maps $S_{/p} \to S$ and $S_{p/} \to S$. ⌟

Proof: We just define $(S_{/p})_n = \mathrm{Hom}_p(K \star \Delta^n, S)$, then the condition holds for Δ^n, and use the fact every simplicial set is a colimit of Δ^ns(4.6.3.1), and both sides commutes with colimits in Y by(4.6.3.19). □

Def. (4.6.3.23). For $\mathcal{C}_0 \subset \mathcal{C} \in s\mathcal{S}\mathrm{et}$ and any diagram $p : K \to \mathcal{C}$, denote $\mathcal{C}^0_{/p} = \mathcal{C}^0 \times_{\mathcal{C}} \mathcal{C}_{/p}$. ⌟

Prop. (4.6.3.24). For $p : A \to B \in \mathcal{C}\mathrm{at}$, there is a natural isomorphism of simplicial sets

$$N(B_{/p}) \cong N(B)_{/N(p)}.$$

⌟

Proof: There is a natural map from LHS to RHS, and we also have natural isomorphisms

$$\begin{aligned} N(B_{/p})_n &= \mathrm{Hom}([n], B_{/p}) \\ &= \mathrm{Hom}_{\mathcal{C}\mathrm{at}_{A/}}(A \to [n] \star A, A \xrightarrow{p} B) \\ \text{(4.6.3.4)} &= \mathrm{Hom}_{s\mathcal{S}\mathrm{et}_{N(A)/}}(N(A) \to N([n] \star A), N(A) \xrightarrow{N(p)} N(B)) \\ \text{(4.6.3.19)} &= \mathrm{Hom}_{s\mathcal{S}\mathrm{et}_{N(A)/}}(N(A) \to \Delta^n \star N(A), N(A) \xrightarrow{N(p)} N(B)) \\ &= \mathrm{Hom}_{s\mathcal{S}\mathrm{et}}(\Delta^n, N(B)_{/N(p)}) = (N(B)_{/N(p)})_n \end{aligned}$$

□

Prop. (4.6.3.25) [Generating Simplicial Sets]. Let $\mathcal{U}$ be a collection of simplicial sets that:

- $\mathcal{U}$ is stable under isomorphisms,
- $\mathcal{U}$ is stable under disjoint union,
- $\Delta^n \subset \mathcal{U}$ for any n,
- If there is a pushout diagram $\begin{array}{ccc} X & \longrightarrow & X' \\ \downarrow f & & \downarrow \\ Y & \longrightarrow & Y' \end{array}$ and $X, X', Y \in \mathcal{U}$ and f is a monomorphism, then $Y' \in \mathcal{U}$,

- suppose we are given a sequence of monomorphisms between objects in $\mathcal{U}$ indexed over $\mathbb{N}$, then the colimit belongs to $\mathcal{U}$.

Then $\mathcal{U} = s\,\mathcal{S}\mathrm{et}$. ⌟

Proof: Use induction on the dimension of S, and notice S is glued together using their simplexes. □

Fibrations and Anodynes

Def. (4.6.3.26) [Fibrations]. A morphism of simplicial sets is called a

- **Kan fibration** iff it has right lifting property w.r.t all $\Lambda^n_i \to \Delta^n, 0 \le i \le n$.
- **left fibration** iff it has right lifting property w.r.t. all inclusions $\Lambda^n_i \subset \Delta^n, 0 \le i < n$.
- **right fibration** iff it has right lifting property w.r.t all inclusions $\Lambda^n_i \subset \Delta^n, 0 < i \le n$.
- **inner fibration** iff it has right lifting property w.r.t all inclusions $\Lambda^n_i \subset \Delta^n, 0 < i < n$.

So a morphism between topological spaces $X \to Y$ is a Serre fibration iff $S(X) \to S(Y)$ is a Kan fibration(4.6.3.8). ⌟

Def. (4.6.3.27) [Anodynes]. A morphism of simplicial set is called a

- **anodyne** iff it has left lifting property w.r.t. all Kan fibrations.
- **left anodyne** iff it has left lifting property w.r.t. all left fibrations.
- **right anodyne** iff it has left lifting property w.r.t all right fibrations.
- **inner anodyne** iff it has right lifting property w.r.t all inner fibrations.

⌟

Def. (4.6.3.28) [Trivial (Kan)Fibrations]. A morphism $X \to S$ of simplicial sets that has right lifting property w.r.t. all inclusions $\partial\Delta^n \to \Delta^n$ is called a **trivial fibration**.

A **cofibration** is a morphism that has left lifting property w.r.t all trivial fibrations. By(4.2.2.15) a cofibration of simplicial sets is just an inclusion. ⌟

Lemma (4.6.3.29) [Join and Anodynes]. If $f : A_0 \subset A$ and $g : B_0 \subset B$ are inclusions of simplicial sets, then

$$h : (A_0 \star B) \coprod_{A_0 \star B_0} (A \star B_0) \subset A \star B$$

is a(n)

- inner anodyne if either f is right anodyne or g is left anodyne, then
- left anodyne if f is left anodyne.

⌟

Proof: 1: By symmetry we assume f is right anodyne. Notice the class of all morphisms f that the conclusion holds is weakly saturated because $\star$ commutes with colimits, so it suffice to check for $f : \Lambda^n_j \subset \Delta^n$. Then similarly it suffices to check for $g : \partial\Delta^m \subset \Delta^m$, but then the inclusion is just $\Lambda^{m+n+1}_j \subset \Delta^{m+n+1}$, which is left anodyne.

2 is similar. □

Prop. (4.6.3.30) [Anodynes].

- The saturated class generated by either of the following three classes of monomorphisms are both left anodynes:

1. $\Lambda^n_k \subset \Delta^n$, $0 \le k < n$.
2. $(\Delta^m \times \{0\} \coprod (\partial\Delta^m \times \Delta^1) \subset \Delta^m \times \Delta^1$.
3. $(S' \times \{0\}) \coprod (S \times \Delta^1) \subset S' \times \Delta^1$, where $S \subset S'$.

Similar conclusion holds for right anodynes and together implies the similar conclusion for anodynes.

•

⌟

Proof:

- 2 and 3 are equivalence because any inclusion comes from attaching cells(4.6.3.3).
  Now inclusions in 2 are compositions of pushouts of inclusions $\Lambda^{n+1}_k \subset \Delta^{n+1}$, where $0 \le k \le n$, thus it is generated by 1. Conversely, $\Lambda^n_i \subset \Delta^n$ is a retract of $(\Delta^n \times \{0\}) \coprod (\Lambda^n_i \times \Delta^1) \subset \Delta^n \times \Delta^1$: Cf.[HTT, P64].
-

□

Cor. (4.6.3.31) [Products and Anodynes]. Let $A \subset A'$ be a(n) left(inner) anodyne and $B \subset B'$, then so does the induced map

$$(A \times B') \coprod_{A\times B} (A' \times B) \to A' \times B'.$$

⌟

Proof: For left anodyne, the proof is similar to that of(4.6.3.29), just check for classes 3 of(4.6.3.30), and use the fact

$$(S' \times \Delta^1) \times B \coprod (S' \times \{0\} \coprod S \times \Delta^1) \times B' \to (S' \times \Delta^1) \times B'$$

is just

$$(S' \times B \coprod S \times B') \times \Delta^1 \coprod (S' \times B') \times \{0\} \to (S' \times B') \times \Delta^1.$$

which is left(inner) anodyne. And similarly for inner anodynes. □

Left Fibration

Remark (4.6.3.32) [Left and Right Fibrations Dual]. The theory of left fibrations is dual to the theory of right fibrations, thus we don't study right fibrations. ⌟

Prop. (4.6.3.33) [Left Fibration and CoFibered in Groupoids]. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor, then $\mathcal{C}$ is a category cofibered in groupoids over $\mathcal{D}$ iff the induced functor $N(F) : N(\mathcal{C}) \to N(\mathcal{D})$ is a left fibration of simplicial sets. ⌟

Proof: By(4.6.3.6), $N(F)$ is an inner fibration, thus it suffices to check for $\Lambda^n_0 \to \Delta^n$. For $n = 1$, this is the definition of cofibered category(4.2.3.10), and $n = 2$ is just the surjectivity of the map defining CoCartesian arrows(4.2.3.7), and $n = 3$ is equivalent to the injectivity of the map defining Cocartesian arrows. And for $n > 3$, then extension is automatic for nerves. □

Remark (4.6.3.34) [Right Fibrations and Fibered Categories]. The (left)right fibration is the ∞-categorial analogue of (co)fibered categories in usual category theory. ⌟

Remark (4.6.3.35). Given a left fibration $X \to S$ is more or less similar to given a functor from the homotopy category hS to the ∞-category $\mathcal{H}$ of spaces. ⌟

Proof: Cf.[HTT, P58].? □

Prop. (4.6.3.36) [Over(Under)categories and Fibrations]. Given a digram of simplicial sets:

$$A \subset B \xrightarrow{p} X \xrightarrow{q} S.$$

Let $r = q \circ p$, $p_0 = p|_A, r_0 = r|_A$, and q is an inner fibration, then

- the induced map $X_{p/} \to X_{p_0/} \times_{S_{r_0/}} S_{r/}$ is a left fibration. And dual argument holds for overcategories.
- If q is a left fibration or $A \subset B$ is right anodyne, then $X_{p/} \to X_{p_0/} \times_{S_{r_0/}} S_{r/}$ is a trivial fibration.
- If q is moreover a left fibration, then the induced map $X_{/p} \to X_{/p_0} \times_{S_{/r_0}} S_{/r}$ is a left fibration.

⌟

Proof: These just follow from(4.6.3.29). □

Prop. (4.6.3.37) [Homotopy Extension Lifting Property]. Let $p : X \to S$ be a map of simplicial sets and $i : A \subset B$, consider the map

$$q : X^B \to X^A \times_{S^A} S^B.$$

- If p is a left fibration, then q is a left fibration.
- If p is a left fibration i is a left anodyne, then q is a trivial fibration.
- If $i : \{0\} \subset \Delta^1$, then p is a left fibration iff q is a trivial fibration.
- If p is an inner fibration, then q is an inner fibration.
- If p is an inner fibration and i is an inner anodyne, then q is a trivial fibration.

⌟

Proof: First notice that a right lifting of q w.r.t a map $Z \to Z'$ is equivalent to a right lifting of p w.r.t the map $Z \times B \coprod Z' \times A \to Z' \times B$. Then the conclusions follow from(4.6.3.31) and(4.6.3.30).
□

Prop. (4.6.3.38) [Homotopy Section and Left Fibration]. Let $p : X \to S \in s\mathcal{S}\mathrm{et}$ and $s : S \to X$ be section of p, and let $h \in \mathrm{Hom}_S(X \times \Delta^1, X)$ that $h|_{X \times \{0\}} = s \circ p$ and $h|_{X \times \{1\}} = \mathrm{id}$, then s is a left anodyne. ⌟

Proof: Cf.[HTT, P65]. □

Prop. (4.6.3.39) [Left Fibration and Functor to Spaces]. Let $X \to S$ be a left fibration, then the fibers are all Kan complexes by(4.7.1.27), and for any edge $f : s \to s' \in S$, we can solve the lifting diagram

$$\begin{array}{ccc} \{0\} \times X_s & \longrightarrow & X \\ \big\downarrow & \nearrow & \big\downarrow \\ \Delta^1 \times X_s \longrightarrow \Delta^1 & \xrightarrow{f} & S \end{array}$$

because the left hand side is left anodyne by(4.6.3.31), thus getting a morphism $f_! : X_s \to X_{s'}$.

Then this determines a functor from hS to $\mathcal{H}$ the homotopy category of spaces. ⌟

Proof: First notice $f_!$ is uniquely defined up to homotopy: given to dotted arrow solving the diagram, we can use the lifting property w.r.t. the map

$$\Delta^1 \times \partial\Delta^1 \times X_s \coprod_{\{0\}\times\partial\Delta^1\times X_s} \{0\} \times \Delta^1 \times X_s \to \Delta^1 \times \Delta^1 \times X_s$$

which is a left anodyne by(4.6.3.31), to get a homotopy between them.

Next if $\eta \in \mathrm{Hom}_{\mathcal{H}}(K, X_s), \eta' \in \mathrm{Hom}_{\mathcal{H}}(K, X_{s'})$, then $\eta' = f_! \circ \eta$ iff there is a map $q : K \times \Delta^1 \to X$ that $q \circ p$ is given by the mapping $X_s \times \Delta^1 \to \Delta^1 \xrightarrow{f} S$, and $p|_{K\times\{0\}}, p|_{K\times\{1\}}$ have homotopy types η, η' resp..

Then for any $g \circ f \cong h \in S$, which is depicted by a 2-complex, we can use the left anodyne $X_u \times \{0\} \subset X_u \times \Delta^2$ to get a morphism $p : X_u \times \Delta^2 \to X$, then $p|_{X_u\times\{1\}} \cong f_!$, $p|_{X_u\times\{2\}} \cong h_!$, and the map $p|_{X_u\times\Delta^{\{1,2\}}}$ witnesses the fact $g_! \circ f_! \cong h_!$. □

Kan Fibrations

Remark (4.6.3.40) [Kan Complexes and Groupoids]. Kan complexes are ∞-categorical analogy of groupoids, by(4.7.1.27) and(4.6.3.6). ⌟

Lemma (4.6.3.41). If a left fibration $p : S \to T$ is a weak homotopy equivalence of Kan complexes, then it is a surjection on vertices. ⌟

Proof: Because it is homotopy equivalence, for any $t \in T$, there is a morphism $p(s) \to t$ for some $s \in S$(Kan complex used), thus it lifts to a morphism in S, so surjective on vertices. □

Lemma (4.6.3.42) [Fibrations of Kan Complexes]. If $S \to T$ is a left fibration and T is a Kan complex, then p is a Kan fibration. ⌟

Proof: Firstly S is a Kan complex. Let $A \subset B$ be anodyne morphisms, we need to show $p : S^B \to S^A \times_{T^A} T^B$ is surjective on vertices. Since S, T are complexes, $S^B \to S^A$ and $T^B \to T^A$ are trivial fibrations by(4.6.3.37). Cf.[HTT, P66].?

Notice this is an immediate consequence of(4.6.3.47), because the homotopy category of a Kan complex is a groupoid, by(4.7.1.27), so $f_!$ must be isomorphisms. □

Prop. (4.6.3.43) [Examples of Kan Complexes].

- The singular complex of topological space is a Kan complex.
- The nerve of a category is a Kan complex iff the category is a groupoid, by(4.6.3.33).
- Simplicial R-module are Kan complexes, by(5.8.1.1).

⌟

Proof:

□

Prop. (4.6.3.44). The bar resolution BG is a Kan fibration for every group G. ⌟

Proof: □

Prop. (4.6.3.45). A principal G fibration, i.e. $X \to X/G$ where X is a simplicial object of G-sets that G acts freely on X_n, is a Kan fibration. ⌟

Lemma (4.6.3.46) [Left Fibrations and Trivial Kan Fibrations]. Let $p : S \to T \in s\,\mathcal{S}\text{et}$ be a left fibration that all the fibers are contractible, then p is a trivial Kan fibration. ⌟

Proof: By duality, it suffices to prove for right fibrations. Because fiber is nonempty, it has right lifting property w.r.t $\varnothing \subset \Delta^0$, and for $n > 0$, let $\partial\Delta^n \to S$ be any map, then to show the lifting property, we may take fiber product and assume $T = \Delta^n$, thus S is an ∞-category. Cf.[HTT, P66]. □

Prop. (4.6.3.47) [Characterizing Kan Fibrations]. Let $p : S \to T$ be a left fibration of simplicial sets, then p is a Kan extension iff the morphism $f_!$ defined in(4.6.3.39) is an isomorphism in $\mathscr{H}$ for any morphism $f \in T$. ⌟

Proof: Cf.[HTT, P66]. □

Def. (4.6.3.48) [Kan-Quillen Model Structure]. There is a combinatorial left and right proper model structure on $s\,\mathcal{S}\text{et}$ called the **Kan-Quillen model structure** with

- Weak equivalences: weak equivalences(4.6.3.11).
- Cofibrations: inclusions,
- Fibrations: Kan fibrations.

⌟

Proof: Cf.[Jardine P62].**?** □

Prop. (4.6.3.49) [Quillen]. The geometrization functor and the singular complex functor(4.6.3.8) defines a Quillen equivalence:

$$|\cdot| : s\,\mathcal{S}\text{et} \rightleftarrows \mathcal{CG} : \text{Sing}$$

where the RHS is Serre-Quillen model category(4.13.6.28) and the LHS is the Kan-Quillen model category(4.6.3.48).

The functor $|-| \circ \text{Sing}$ is also denoted by $\Gamma : \mathcal{CG} \to \mathcal{CG}$. ⌟

Proof: Cf.[May, P125].**?** □

Cor. (4.6.3.50). The localized category of $\mathcal{CG}$ and $s\,\mathcal{S}\text{et}$ at weak homotopy equivalence classes are the same, and it is just the homotopy category of spaces $\mathscr{H}$, by(4.5.2.7). ⌟

Cor. (4.6.3.51). By(4.6.3.43), for any $S \in s\,\mathcal{S}\text{et}$, $S \to \text{Sing}\,|S|$ is a fibrant replacement w.r.t. the Kan-Quillen model category. ⌟

Marked Simplicial Sets

Def. (4.6.3.52) [Marked Simplicial Sets]. A **marked simplicial set** is a pair $(X, \mathcal{E}_X)$ where X is a simplicial set and $\mathcal{E}_X \subset X_1$ is a set of edges containing all the degenerate ones. The category of simplicial sets is denoted by $s\,\mathcal{S}\text{et}^+$. ⌟

4 Simplicial Categories

Def. (4.6.4.1) [Simplicial Categories]. The category $s\,\mathcal{C}\text{at}$ of **simplicial categories** consists of categories enriched over the Cartesian monoidal category $s\,\mathcal{S}\text{et}$. $s\,\mathcal{C}\text{at}$ is complete and cocomplete, by(4.2.2.3) and(4.6.3.15)(4.6.1.2). ⌟

Def. (4.6.4.2)[Homotopy Category]. There are singular complex functor and geometrization functor that induce isomorphism of $h(s\,\mathcal{S}\text{et}) \cong h(\mathcal{CG})$ by(4.6.3.50), thus the theory of simplicial categories and topological categories are the same. ⌟

Bergner Model Structure

Def. (4.6.4.3) [Dwyer-Kan Equivalences]. A **Dwyer-Kan equivalence of simplicial categories** is a weak equivalence of simplicial categories as enriched categories(4.6.4.16). ⌟

Def. (4.6.4.4) [Bergner Model Structure]. There is a left proper combinatorial model structure **Bergner model structure** on $s\,\mathcal{C}\mathrm{at}$ called the **Bergner model structure** with

- Weak equivalences: Dwyer–Kan equivalences(4.6.4.3).
- Fibrations: $F : \mathcal{C} \to \mathcal{D}$ that is an quasi-fibration(4.2.3.9) and for any $x, y \in \mathcal{C}$, $\mathrm{Map}_{\mathcal{C}}(x, y) \to \mathrm{Map}_{\mathcal{D}}(Fx, Fy)$ is a Kan-fibration.
- Cofibrations:

⌟

Proof: ? Cf.[Bergner. A model category structure on the category of simplicial categories] or [Lurie]. □

Simplicial Nerves

Def. (4.6.4.5) [Thickened Finite Ordered Sets]. Let J be a finite ordered set, define a simplicial category $\mathfrak{C}[\Delta^J]$ as follows:

- The objects are elements of J.
- For $i, j \in J$, $\mathrm{Mor}(i, j) = N(P_{i,j})$, where $P_{i,j}$ is the poset $\{I \subset [i, j] | i, j \in I\}$.
- The composition of simplicial sets is induced by the union of partially ordered sets $P_{i,j} \times P_{j,k} \subset P_{i,k}$.

⌟

Def. (4.6.4.6) [Coherent Nerves]. by Yoneda extension and(4.6.4.1), the functor $\Delta \to s\,\mathcal{C}\mathrm{at} : [n] \mapsto \mathfrak{C}[\Delta^n]$ corresponds to an adjunction

$$\mathfrak{C} : s\,\mathcal{S}\mathrm{et} \rightleftarrows s\,\mathcal{C}\mathrm{at} : N_\Delta$$

where N_Δ is called the **coherent nerve** functor, and

$$(N_\Delta(\mathcal{C}))_n = \mathrm{Hom}_{\mathcal{C}\mathrm{at}_\Delta}(\mathfrak{C}[\Delta^n], \mathcal{C}).$$

If $\mathcal{C}$ is a topological category, then define the **topological nerve** to be the simplicial nerve of $\mathrm{Sing}(\mathcal{C})$.

By the definition and the adjointness of(4.6.3.8), the nerve functor N_Δ is right adjoint to the functor $|\cdot| \circ \mathfrak{C}$ or $\mathfrak{C}$. ⌟

Remark (4.6.4.7). It should be checked that to give a 2-complex in $N_\Delta(\mathcal{C})$ is equivalent to giving morphisms $f, g, h \in \mathcal{C}$ and a path from $g \circ f$ to h. ⌟

Thm. (4.6.4.8) [$\mathfrak{C} : s\,\mathcal{S}\mathrm{et} \underset{}{\overset{\text{Quillen}}{\rightleftarrows}} s\,\mathcal{C}\mathrm{at} : N_\Delta$]. The adjunction(4.6.4.6) is a Quillen adjunction w.r.t. the Joyal model category on $s\,\mathcal{S}\mathrm{et}$(4.6.4.19) and the Bergner model category on $s\,\mathcal{C}\mathrm{at}$(4.6.4.4).

In particular, a theory of $(\infty, 1)$-categories given by the model of simplicial sets and the model of simplicial categories are the same?. ⌟

Proof: Cf.[HTT, P89].**?**

Firstly we show $\mathfrak{C}$ preserves cofibrations. It suffices to show that $\mathfrak{C}[\partial\Delta^n] \subset \mathfrak{C}[\Delta^n]$ is a cofibration(4.5.7.4). But notice this two simplicial category only differ at $\mathrm{Hom}_{\mathfrak{C}[\partial\Delta^n]}(0,n)$ is the boundary of the simplicial cube $(\Delta^1)^{n-1} \cong \mathrm{Hom}_{\mathfrak{C}[\Delta^n]}(0,n)$, thus the inclusion is a pushout of the inclusion $[1]_{\partial(\Delta^1)^{n-1}} \subset [1]_{(\Delta^1)^{n-1}}$, which is a cofibration by(4.5.7.3).

Left properness is clear(4.5.0.9). $\mathfrak{C}$ preserves weak equivalences by(4.6.4.12) and(4.5.7.4), so $(\mathfrak{C}, N)$ is a Quillen adjunction. To show it is a Quillen equivalence: It suffices to check for each simplicial set S and fibrant simplicial category $\mathcal{C}$, a map $u : S \to N(\mathcal{C})$ is a categorical equivalence iff the adjoint map $v : \mathfrak{C}[S] \to \mathcal{C}$ is an equivalence of simplicial categories. But v factors as

$$\mathfrak{C}[S] \xrightarrow{\mathfrak{C}[u]} \mathfrak{C}[N(\mathcal{C})] \xrightarrow{w} \mathcal{C}$$

and the counit map w is an equivalence by(4.6.4.14). □

Cor. (4.6.4.9). The coherent nerve of a Bergner-fibrant(4.6.4.4) simplicial category is an ∞-category. ⌟

Prop. (4.6.4.10)[Kan Fibrations Nerve Inner Fibrations]. Let $F : \mathcal{C} \to \mathcal{D}$ be a a map of simplicial categories that for any $C, C' \in \mathcal{C}$, $\mathrm{Map}(C,C') \to \mathrm{Map}(F(C),F(C'))$ is a Kan fibration, then the induced map of simplicial sets $N(\mathcal{C}) \to N(\mathcal{D})$ is an inner fibration. ⌟

Proof: This is because a lifting of $N(\mathcal{C}) \to N(\mathcal{D})$ w.r.t. $\lambda^n_j \subset \Delta^n$ is equivalent to a lifting of $\mathcal{C} \to \mathcal{D}$ w.r.t $\mathfrak{C}[\Lambda^n_j] \subset \mathfrak{C}[\Delta^n]$. But this lifting is equivalent to a lifting of $\mathrm{Map}(F(0),F(n)) \to \mathrm{Map}(F'(0),F'(n))$ w.r.t. the anodyne map $\mathrm{Map}_{\mathfrak{C}[\Lambda^n_j]} \subset \mathrm{Map}_{\mathfrak{C}[\Delta^n]}$, which is a cube removing the interior and a face. □

Cor. (4.6.4.11). The topological nerve of a topological category $\mathcal{C}$ is an ∞-category, as the singular complex of a topological space is always a Kan complex, by(4.6.3.43). ⌟

Def. (4.6.4.12) [Homotopy Category]. For $S \in s\mathcal{S}\mathrm{et}$, the **homotopy category** hS is defined to be the homotopy category(4.6.3.50) of the simplicial category $\mathfrak{C}[S]$(4.6.4.6), which is an $\mathscr{H}$-enriched category. A map of simplicial sets is called a **categorical equivalence** if their homotopy categories are equivalent as $\mathscr{H}$-enriched categories. ⌟

Remark (4.6.4.13). $f : S \cong T \in s\mathcal{S}\mathrm{et}$ is a categorical equivalence iff $\mathfrak{C}(f) : \mathfrak{C}[S] \to \mathfrak{C}[T]$ is a Dwyer-Kan equivalence(4.6.4.3). ⌟

Lemma (4.6.4.14). Let $\mathcal{C}$ be fibrant simplicial category, then the counit map $u : \mathrm{Map}_{\mathfrak{C}[N_\Delta(\mathcal{C})]}(x,y) \to \mathrm{Map}_{\mathcal{C}}(x,y)$ is a weak homotopy equivalence of simplicial sets. ⌟

Proof: Cf.[HTT, P72]. □

Lemma (4.6.4.15). Let $\mathcal{C}$ be a topological category, then the counit map $|\mathfrak{C}(N(\mathcal{C}))| \cong \mathcal{C}$(4.6.4.6) is an equivalence of topological categories. ⌟

Proof: By the Quillen equivalence between $s\mathcal{S}\mathrm{et}$ and $\mathcal{CG}$(4.6.3.49), this follows from(4.6.4.14), as by(4.5.7.11) and(4.6.3.43), $\mathrm{Sing}(\mathcal{C})$ is a fibrant simplicial category. □

Prop. (4.6.4.16) [Topological Category and ∞-Category Equivalent]. The adjunction pair $(|\mathfrak{C}[\cdot]|, N)$ defines a bijection between equivalent classes of topological(or simplicial) categories and ∞-categories. ⌟

Proof: It suffices to show the units and counits are equivalences:

$$|\mathfrak{C}[N(\mathcal{C})]| \cong \mathcal{C}, \quad S \mapsto N(|\mathfrak{C}[S]|).$$

The first is(4.6.4.15), and the second follows from the first by remark(4.6.4.13). □

Prop. (4.6.4.17). For $S, S' \in s\,\mathcal{S}\mathrm{et}$, the natural map $\mathfrak{C}[S \times S'] \to \mathfrak{C}[S] \times \mathfrak{C}[S']$ is an equivalence of simplicial categories. ⌟

Proof: If S, S' are nerves of fibrant simplicial categories $\mathcal{C}, \mathcal{C}'$, then we have a diagram $\mathfrak{C}[S \times S'] \to \mathfrak{C}[S] \times \mathfrak{C}[S'] \to \mathcal{C} \times \mathcal{C}'$. Then by the two out of three axiom, the assertion follows from the fact that for any fibrant simplicial category $\mathcal{D}$, $\mathfrak{C}[N(\mathcal{D})] \to \mathcal{D}$ is an equivalence(4.6.4.15).

Now for general S, S', we can find a categorical equivalences $S \to N(|\mathfrak{C}[S]|) = T$, and then $S \times S' \to T \times T'$ is also categorical equivalence by(4.6.4.17), and we are done, by(4.6.4.19). □

Joyal Model Structure

Lemma (4.6.4.18) [Inner Anodyne is Categorical Equivalence]. Every inner anodyne map $A \to B$ of simplicial sets is a categorical equivalence. ⌟

Proof: The class of morphisms f that $\mathfrak{C}(f)$ is a trivial cofibration is weakly saturated(because $\mathfrak{C}$ is a left adjoint(4.6.4.6) and(4.5.0.5)), then it suffices to check for $\Lambda^n_j \subset \Delta^n$. Then $\mathfrak{C}[\Lambda^n_j] \subset \mathfrak{C}[\Delta^n]$ is a pushout of $[i]_K \subset [1]_{(\Delta^1)^{n-1}}$, where K is obtained form $(\Delta^1)^{n-1}$ by moving a face and the interior. Thus it is a trivial cofibration(4.5.7.4). □

Prop. (4.6.4.19) [Joyal Model Structure]. There is a left proper combinatorial model structure called **Joyal model structure** on $s\,\mathcal{S}\mathrm{et}$, with:

- Cofibrations: monomorphisms.
- Weak equivalences: categorical equivalences defined in(4.6.4.12).
- Fibrations: **categorical fibrations** or **Joyal fibrations** which has the right lifting property w.r.t. trivial cofibrations.

⌟

Proof: Cf.[HTT, P89].**?** □

Cor. (4.6.4.20). if $K, A, B \in s\,\mathcal{S}\mathrm{et}$ and $f : A \to B$ is a categorical equivalence, then $A \times K \to B \times K$ is also a categorical equivalence. ⌟

Proof: Choose a factorization $B \to Q$, which is an inner anodyne and Q is an ∞-category, by small object argument(4.2.2.13), then $B \times K \to Q \times K$ is also an inner anodyne map(4.6.3.31), hence a categorical equivalence(4.6.4.18), so we can assume B is an ∞-category. Similarly we can reduce to the case A, K are also ∞-categories.

For the rest, Cf.[HTT, P92]. □

Prop. (4.6.4.21) [∞-Category Fibrant in Joyal Model]. $C \in s\,\mathcal{S}\mathrm{et}$ is Joyal-fibrant iff it is an ∞-category. ⌟

Proof: Fibrant objects are ∞-categories, by(4.6.4.18). For the converse, fix an ∞-category and an inclusion $A \subset B$, given a map $A \to \mathcal{C}$, the inclusion $\mathcal{C} \subset C \coprod_A B$ is also a categorical equivalence because Joyal model structure is left proper(4.6.4.19), thus $\mathcal{C}$ is a retract of $\mathcal{C} \coprod_A B$ by(4.6.4.22), which gives an extension $B \to \mathcal{C}$. □

Lemma (4.6.4.22). Let $\mathcal{C} \subset \mathcal{D} \in s\,\mathcal{S}\mathrm{et}$ be a categorical equivalence and $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$, then $\mathcal{C}$ is a retract of $\mathcal{D}$. ⌟

Proof: Include $\mathcal{D}$ into an ∞-category by small object argument and(4.6.4.18), we may assume $\mathcal{D}$ is also an ∞-category. So we finish by applying(4.7.1.25) for $A = \mathcal{C}$ and $B = \mathcal{D}$. □

Cor. (4.6.4.23). Any $S \in s\,\mathcal{S}\mathrm{et}$ is weakly equivalent to an ∞-category. ⌟

Def. (4.6.4.24) [Joyal Joins]. For $X, Y \in s\,\mathcal{S}\mathrm{et}$, define the **Joyal Join**

$$X \diamond Y = X \coprod_{X\times Y\times\{0\}} (X \times Y \times \Delta^1) \coprod_{X\times Y\times\{1\}} Y = (X \coprod Y) \coprod_{X\times Y\times\partial\Delta^1} (X \times Y \times \Delta^1).$$

By(4.5.6.7), this is a homotopy colimit w.r.t. the Joyal model cateogry, so if $X \to X', Y \to Y'$ are categorical equivalences, $X \diamond Y \to X' \diamond Y'$ is also a categorical equivalence(4.5.6.6). ⌟

Prop. (4.6.4.25). There is a projection map $X \diamond Y \to \Delta^1$, and a map $X \times Y \times \Delta^1 \to X \star Y$ that is compatible with projection onto Δ^1, thus inducing a map

$$X \diamond Y \to X \star Y$$

that is compatible with projection onto Δ^1. Then this map is a categorical equivalence. ⌟

Proof: Because both $\diamond$ and $\star$ commutes with filtered colimits, by(4.5.3.3), it suffices to show for X with only f.m. non-degenerate simplexes. Then we use induction. The case $X = \varnothing$ is trivial, and if $X = X' \coprod_{\partial\Delta^n} \Delta^n$, because Joyal model category is left proper(4.6.4.19), by(4.5.6.7), $X \diamond Y \to X \star Y$ is a homotopy pushout of $X' \diamond Y \to X' \star Y$. Then it suffices to show for $X = \Delta^n$.

By similar reason, because $\Delta^{\{0,1\}} \coprod_{\{1\}} \Delta^{\{1,2\}} \coprod_{\{2\}} \coprod \cdots \coprod_{\{n-1\}} \Delta^{\{n-1,n\}} \to \Delta^n$ is an anodyne**?**, and anodyne are categorical equivalences(4.6.4.18), and homotopy limits of categorical equivalences are categorical equivalences by(4.5.6.6), it suffices to prove for $X = \Delta^0$ or $X = \Delta^1$. The same argument then shows it suffices to prove for $Y = \Delta^0$ or $Y = \Delta^1$. And in each case the desired map is an isomorphism. □

Cor. (4.6.4.26). If $S \to S', T \to T'$ are categorical equivalences, then $S \star T \to S' \star T'$ is also a categorial equivalence, by(4.6.4.24). ⌟

Cor. (4.6.4.27). For $X, Y \in s\,\mathcal{S}\mathrm{et}$, there is a natural equivalence of simplicial categories

$$\mathfrak{C}[X \star Y] \cong \mathfrak{C}[X] \star \mathfrak{C}[Y].$$

⌟

Proof: Cf.[Lur09]P240. □

5 Simplicial Model Categories

Def. (4.6.5.1) [Simplicial Model Categories]. A **simplicial model category** is a $s\,\mathcal{S}\mathrm{et}$-enriched model category(4.5.5.3). ⌟

Prop. (4.6.5.2) [Simplicial Model Category Criterion]. Let $\mathcal{C}$ be a simplicial category that is equipped with a model structure that every object of $\mathcal{C}$ is cofibrant and the collection of weak equivalences in stable under filtered colimits, then $\mathcal{C}$ is a simplicial model category iff the following conditions holds:

- $\mathcal{C}$ is both tensored and cotensored over $\mathcal{S}\mathrm{et}_\Delta$.
- Given a cofibration of simplicial sets $i : K \to L$ and a cofibration $C \to D \in \mathcal{C}$, the induced map $(C \otimes L) \coprod_{C\otimes K} D \otimes K \to D \otimes L$ is a cofibration in $\mathcal{C}$.
- The natural map $C \otimes \Delta^n \to C \otimes \Delta^0 \cong C$ is a weak equivalence in $\mathcal{C}$.

⌟

Proof: Cf.[HTT, P850]. □

Prop. (4.6.5.3). Let $\mathcal{C}$ be a simplicial model category and X cofibrant and Y fibrant, then $K = \mathrm{Map}(X,Y)$ is a Kan complex, and there is a canonical bijection $\pi_0 K \cong \mathrm{Hom}_{\mathrm{Ho}(\mathcal{C})}(X,Y)$. ⌟

Proof: Use(4.5.5.4). □

Model-Categorical Yoneda Extensions

Def. (4.6.5.4) [$U(\mathcal{C})$]. For $\mathcal{C} \in \mathcal{C}\mathrm{at}$, denoted $U(\mathcal{C}) = \mathcal{PS}\mathrm{h}(\mathcal{C}, s\,\mathcal{S}\mathrm{et})_{\mathrm{Proj}}$, which is a left and right proper combinatorial model category, by(4.6.3.48) and(4.5.6.1)(4.5.6.2). And there is a natural functor

$$s\,よ : \mathcal{C} \mapsto \mathcal{PS}\mathrm{h}(\mathcal{C}, \mathcal{S}\mathrm{et}) \to \mathcal{PS}\mathrm{h}(\mathcal{C}, s\,\mathcal{S}\mathrm{et}).$$

⌟

Prop. (4.6.5.5) [Model-Categorical Yoneda Extensions]. Let $\mathcal{C} \in \mathcal{C}\mathrm{at}$, $\mathcal{M}$ be a model category, then for any functor $Q : \mathcal{C} \to \mathcal{M}$, there is a Quillen adjunction $(L,R) : U(\mathcal{C}) \underset{\longleftarrow}{\overset{\text{Quillen}}{\longrightarrow}} \mathcal{M}$ together with a natural weak equivalence $L \circ s\,よ \cong Q \in \mathrm{Func}(\mathcal{C},\mathcal{M})$. And the category of such extensions is contractible. ⌟

Proof: Cf.[D. Dugger. Universal homotopy theories]. □

Exponentiation in Model Categories

Localizations and Presentations

Def. (4.6.5.6) [S-Local and S-Equivalences]. ⌟

Prop. (4.6.5.7) [Localizations of Simplicial Model Categories]. Let $\mathcal{M}$ be a left proper combinatorial simplicial model category and $S \subset \mathrm{Cof}(M)$ be a small subset, then there is a left proper combinatorial simplicial model category $S^{-1}\mathcal{M}$ with the same underlying category as $\mathcal{M}$ and

- Cofibrations: $\mathrm{Cof}(\mathcal{M})$.
- Weak Equivalences: S-equivalences in $\mathcal{M}$.
- Fibrations: defined by the above two.

And $X \in \mathcal{M}$ is fibrant in $S^{-1}A$ iff X is S-local and fibrant in $\mathcal{M}$. ⌟

Proof: Cf.[Lur09]P906. □

Prop. (4.6.5.8). Let $\mathcal{M}$ be a left proper combinatorial simplicial model category, then

- Any combinatorial Bousfield localization(4.5.4.3) of $\mathcal{M}$ is of the form $S^{-1}\mathcal{M}$, where $S \subset \mathrm{Cof}(\mathcal{M})$ is a small subset.
- For any two small subset $S, T \subset \mathrm{Cof}(\mathcal{M})$, $S^{-1}\mathcal{M}$ and $T^{-1}\mathcal{M}$ coincide iff the class of S-local objects and T-local objects coincide.

⌟

Proof: Cf.[Lur09]P908. □

Prop. (4.6.5.9) [Combinatorial Model Categories have Presentations]. Every combinatorial model category $\mathcal{M}$ has a presentation, i.e. there exists a $\mathcal{C} \in \mathcal{C}at$ a set S of morphisms in $U(A)$ and a Quillen equivalence

$$U(\mathcal{C})[S^{-1}] \xrightarrow{\text{Quillen}} \mathcal{M}(4.6.5.7).$$

⌟

Proof: [D. Dugger. Combinatorial model categories have presentations]. □

6 Covariant Model Structure

Prop. (4.6.6.1) [Covariant Model Structure]. For $S \in s\,\mathcal{S}$et, a map $X \to Y \in (\mathcal{S}\mathrm{et}_\Delta)_{/S}$ is called a

- **covariant cofibration** if it is a monomorphism.
- **covariant equivalence** if the induced map $X^\triangleleft \coprod_X S \to Y^\triangleleft \coprod_Y S$ is a categorical equivalence(4.6.4.12).

Then these define a left proper combinatorial model structure on $(\mathcal{S}\mathrm{et}_\Delta)_{/S}$. ⌟

Proof: Cf.[HTT, P69]. □

Lemma (4.6.6.2). Every left anodyne map in $(\mathcal{S}\mathrm{et}_\Delta)_{/S}$ is a covariant equivalence. ⌟

Proof: Cf.[HTT, P69]. □

Prop. (4.6.6.3) [Covariant Model Structure]. $(\mathcal{S}\mathrm{et}_\Delta)_{/S}$ is a simplicial model category with the contravariant model structure and the simplicial structure where

$$\mathrm{Map}(X, Y) = Y^X \times_{S^X} \{\varphi\} \in \mathcal{S}\mathrm{et}_\Delta$$

where $\varphi : X \to S$ is the structure map. ⌟

Proof: We use(4.6.5.2), it suffices to check that $X \times \Delta^n \to X \times \Delta^0$ is a covariant equivalence. But it has a section, which is a left anodyne by(4.6.3.31), thus it is a covariant equivalence by(4.6.6.2). □

Cor. (4.6.6.4)[Contravariant Model Structure]. Let S be a simplicial set, then the covariant model is usually not self-dual, and we can define a **contravariant model structure** as follows:

- A **contravariant cofibration** is a monomorphism of simplicial sets.
- f is a **contravariant equivalence** in $(\mathcal{S}\mathrm{et})_{/S}$ iff f^{op} is a covariant equivalence in $(\mathcal{S}\mathrm{et})_{/S^{op}}$.
- f is a **contravariant fibration** in $(\mathcal{S}\mathrm{et})_{/S}$ iff f^{op} is a covariant fibration in $(\mathcal{S}\mathrm{et})_{/S^{op}}$.

⌟

Prop. (4.6.6.5) [Base Change]. Let $S \to S'$ be a map of simplicial sets, then the forgetful functor and base change functor $j_!, j^*$ defines a Quillen adjunction of covariant models:

$$j_! : (\mathcal{S}\mathrm{et}_\Delta)_{/S} \xrightarrow{\text{Quillen}} (\mathcal{S}\mathrm{et}_\Delta)_{/S'} : j^*$$

⌟

Proof: it is clearly a pair of adjoints, and $j_!$ preserves cofibrations. $j_!$ also preserves covariant equivalences: Cf.[HTT, P71]?. Thus it is a Quillen adjunction. □

Lemma (4.6.6.6). Let $S' \subset S$ be simplicial sets, let $p : X \to S$ be a map and $q : Y \to S$ be a right fibration. Let $X' = X \times_S S', Y' = Y \times_S S'$, then the restriction map

$$\varphi : \mathrm{Map}_{(\mathcal{S}\mathrm{et}_\Delta)_{/S}}(X, Y) \to \mathrm{Map}_{(\mathcal{S}\mathrm{et}_\Delta)_{/S'}}(X', Y')$$

is a Kan fibration. ⌟

Proof: Firstly it is a right fibration because it has right lifting property w.r.t. right anodyne inclusion $A \to B$: this is because $(A \times X') \coprod (A \times X) \subset B \times X$ is also a right anodyne(4.6.3.31). Next we apply this to the inclusion $\varnothing \subset S'$ to see that $\mathrm{Map}_{(\mathcal{S}\mathrm{et}_\Delta)_{/S'}}(X', Y')$ is a Kan complex(4.7.1.27), and then φ is a Kan fibration by(4.6.3.42). □

Lemma (4.6.6.7). Let $p : X \to S$ be an object of $(\mathcal{S}\mathrm{et}_\Delta)_{/S}$, then p is a right fibration iff it is a covariant fibrant object in $(\mathcal{S}\mathrm{et}_\Delta)_{/S}$. ⌟

Proof: Cf.[HTT, P85]. □

Def. (4.6.6.8) [Pointwise Equivalence]. Let $X \to Y$ be a map in $RFib(S)$, then f is called a **pointwise equivalence** iff the induced map $X_s \to Y_s$ is a homotopy equivalence of Kan complexes(4.7.1.27) for any $s \in S$. ⌟

Lemma (4.6.6.9). Let $f : X \to Y$ be a morphism in $RFib(S)$, then the following are equivalent:

- f is a pointwise equivalence.
- f is an equivalence in the simplicial category $(\mathcal{S}\mathrm{et})_{/S}$.
- For any $A \in (\mathcal{S}\mathrm{et})_{/S}$, f induces a homotopy equivalence of Kan complexes: $\mathrm{Map}_{(\mathcal{S}\mathrm{et}_\Delta)_{/S}}(A, X) \to \mathrm{Map}_{(\mathcal{S}\mathrm{et}_\Delta)_{/S}}(A, Y)$.

⌟

Proof: Cf.[HTT, P82]. □

Prop. (4.6.6.10) [Equivalences]. In the situation of(4.6.6.8), f is a pointwise equivalence iff it is a contravariant equivalence iff it is a categorical equivalence. ⌟

Proof: Cf.[HTT, 2.2.3.13, 3.3.1.5]?. □

Prop. (4.6.6.11) [Contravariant Fibration as Right Fibration]. Let $f : X \to Y$ be a map in $RFib(S)$, then f is a contravariant fibration in $(s\,\mathcal{S}\mathrm{et})_{/S}$ iff it is a right fibration. ⌟

Proof: Cf.[HTT, P86]. □

Straightening and Unstraightening

Def. (4.6.6.12) [Straightening and Unstraightening]. Fix a simplicial set S, a simplicial category $\mathcal{C}$ and a functor $\mathfrak{C}[S] \to \mathcal{C}^{op}$. Given an object $X \in (\mathcal{S}\mathrm{et}_\Delta)_{/S}$, let v be the cone point of $X^{\triangleright}$. Then the simplicial category $\mathcal{M} = \mathfrak{C}[X^{\triangleright}] \coprod_{\mathfrak{C}[X]} \mathcal{C}^{op}$ can be viewed as a correspondence? between $\mathcal{C}^{\mathrm{op}}$ and Δ^0, thus giving a simplicial functor

$$\mathrm{St}_\varphi X : \mathcal{C} \to \mathcal{S}\mathrm{et}_\Delta : C \mapsto \mathrm{Map}_{\mathcal{M}}(C, v).$$

Then St_φ is called the **straightening functor** associated to φ. And we denote by St_S the functor St_φ where $\varphi : \mathrm{id}_{\mathfrak{C}[S]}$.

By the adjoint functor theorem(4.1.1.34), St_φ has a left adjoint called **unstraightening functor** $UnSt_\varphi$**?**. ⌟

Prop. (4.6.6.13). Let S be a simplicial set, $\mathcal{C}$ a simplicial category and $\varphi : \mathfrak{C}[S] \to \mathcal{C}^{\mathrm{op}}$ a simplicial functor, then the straightening and unstraightening functor determines a Quillen adjunction

$$\mathrm{St}_\varphi : (\mathcal{S}\mathrm{et}_\Delta)_{/S} \overset{\text{Quillen}}{\rightleftarrows} \mathcal{S}\mathrm{et}_\Delta^{\mathcal{C}} : UnSt_\varphi$$

determines a Quillen adjunction, where the LHS has the contravariant model structure and the RHS has the projective model structure. And if φ is an equivalence of simplicial categories, then $(St_\varphi.Un_\varphi)$ is a Quillen equivalence. ⌟

Proof: □

<u>**Unstraightening of Right Fibrations**</u>

Prop. (4.6.6.14). For every simplicial set S, the unstraightening Un_S induces an equivalence of simplicial categories

$$(\mathcal{S}\mathrm{et}_\Delta^{\mathfrak{C}[S]^{op}})_{cf} \to RFib(S).$$

(4.5.5.5), where the RHS is the category of fibrations $X \to S$. ⌟

Proof: Cf.[HTT, P83]. □

7 Cartesian Fibrations

Remark (4.6.7.1). The theory of Cartesian fibrations is an analogue of the theory of fibered categories3. ⌟

Def. (4.6.7.2) [p-Cartesian]. Let $p : X \to S$ be an inner fibration and $f : x \to y$ is an edge of X, then f is called a p-**Cartesian** if the induced map

$$X_{/f} \to X_{/y} \times_{S_{/p(y)}} S_{/p(f)}$$

is a trivial Kan fibration. ⌟

Remark (4.6.7.3). For $\mathcal{C} \in \mathcal{C}\mathrm{at}$ and $p : N(\mathcal{C}) \to \Delta^1 \in s\,\mathcal{S}\mathrm{et}$, a morphism $f \in \mathcal{C}$ is p-Cartesian iff it is Cartesian in the usual sense. ⌟

Prop. (4.6.7.4) [Characterization of Cartesian Fibrations]. Let $p : \mathcal{C} \to \mathcal{D}$ be an inner fibration of ∞-categories, then an edge $f : Y \to Z \in \mathcal{C}$ is p-Cartesian iff for every object $X \in \mathcal{C}$, there is a Cartesian diagram

$$\begin{array}{ccc} \mathrm{Map}(X,Y) & \longrightarrow & \mathrm{Map}(X,Z) \\ \downarrow & & \downarrow \\ \mathrm{Map}(p(X),p(Y)) & \longrightarrow & \mathrm{Map}(p(X),p(Z)) \end{array}.$$

⌟

Proof: Cf.[HTT, P131]. □

Cartesian Fibrations

Def. (4.6.7.5) [Cartesian Fibration]. A **Cartesian fibration** is an inner anodyne map $p : X \to S$ that for any edge $f : x \to y \in S$ and a vertex $\widetilde{y}$ mapping to y, there is a p-Cartesian edge $\widetilde{f}$ with $p(\widetilde{f}) = f$. The dual of a Cartesian fibration is called a **coCartesian fibration**. ⌟

Prop. (4.6.7.6). The class of Cartesian fibrations is stable under compositions and base change. ⌟

Prop. (4.6.7.7) [Cartesian Fibration and Right Fibration]. Let $p : X \to S$ be an inner fibration, then the following are equivalent:

- p is a Cartesian fibration and the every edge of X is p-Cartesian.
- p is a right fibration.
- p is a Cartesian fibration and every fiber X_s is a Kan complex.

⌟

Proof: Cf.[HTT, P122].**?** □

Def. (4.6.7.8) [Locally Cartesian Fibration]. A map $X \to S$ of simplicial sets is called a **locally Cartesian fibration** if it is an inner fibration and for every edge $\Delta^1 \to S$, the pullback $X \times_S \Delta^1 \to \Delta^1$ is a Cartesian fibration. ⌟

Prop. (4.6.7.9) [Cartesian and Locally Cartesian]. Let $p : X \to S$ be a locally Cartesian fibration, then the following are equivalent:

- p is a Cartesian fibration.
- Given a composition $fg \cong h$ in the homotopy category, if f, g are both locally p-Cartesian, then h is also locally p-Cartesian.
- Every locally p-Cartesian edge in X is p-Cartesian.

⌟

Proof: Cf.[HTT, P124]. □

Prop. (4.6.7.10). Given maps of ∞-categories: $\mathcal{C} \xrightarrow{p} \mathcal{D} \xrightarrow{q} \mathcal{E}$, if $q, q \circ p$ are both locally Cartesian fibrations and p maps locally $(q \circ p)$-Cartesian maps to locally q-Cartesian maps and for any $Z \in \mathcal{E}$, p induces a categorial equivalence $\mathcal{C}_Z \to \mathcal{D}_Z$, then p is a categorical equivalence. ⌟

Proof: Cf.[HTT, P132].**?** □

Prop. (4.6.7.11). Categorical equivalences between ∞-categories are stable under base change of Cartesian fibrations of ∞-categories. ⌟

Proof: Cf.[HTT, P132]. □

8 Simplicial Homology

Prop. (4.6.8.1). For a Kan fibration X, there can be defined a homotopy groups π_n that they agree with $\pi_i(|X|)$ thus also $\pi_i(S|X|)$, Cf.[Weibel P263]. Thus we see that $|BG|$ is truly the Eilenberg-Maclane spaces BG. ⌟

9 Cyclic Homology Theory(欧阳恩林)

Combinatorial Category

Def. (4.6.9.1). The **Segal category** Fin_* is the category of pointed finite sets. A morphism is called **inert** iff $|f^{-1}(\{i\})| = 1$ for all $i \neq *$. It is called **active** iff $f^{-1}(\{*\}) = \{*\}$.

A morphism can be uniquely factorized as a composition gh, where h is inert and g is active. ⌟

Prop. (4.6.9.2). There is a morphism $\mathrm{Cut} : \Delta^{op} \to \mathrm{Fin}_*$ where we interpret $[n] \in \mathrm{Fin}_*$ as the set of cut in $[n]$, and

$$\mathrm{Cut}(\alpha)(i) = \begin{cases} j & \text{if there are } j \text{ s.t. } \alpha(j-1) < i \leq \alpha(j) \\ 0 & \text{otherwise} \end{cases}$$

⌟

Prop. (4.6.9.3). The category of functors from the $E_\infty = \mathrm{Fin}_*$ to $\mathcal{C}at$ that

$$X([n]) \xrightarrow{\prod_{i=2}^n X(\rho^i)} \prod_{i=1}^n X([1]) \quad n \geq 0$$

and $X([0])$ is the final object, is equivalent to the category of symmetric unital monoidal categories with base category $(X([1]))$. (Because the commutativity of morphisms encodes the fact that the tensor action is symmetric).

Similarly, the category of functors from the Δ^{op} to Cat that

$$X([n]) \xrightarrow{\prod_{i=2}^n X(\rho^i)} \prod_{i=1}^n X([1]) \quad n \geq 0$$

is equivalent to the category of symmetric unital monoidal categories $(X([1]))$. And it is symmetric iff it factors through Cut:$\Delta^{\mathrm{op}} \to \mathrm{Fin}_*$. ⌟

Def. (4.6.9.4). The **Conne cyclic category** Δ_C is a category containing Δ that $\mathrm{Aut}_{\Delta C}([n])$ is C_{n+1}. And every morphism $[n] \to [m]$ in Δ_C can be uniquely written as the form φg, where $\varphi \in \mathrm{Hom}_\Delta([n],[m])$ and $g \in \mathrm{Aut}_{\Delta_C}([n])$.

Δ_C^{op} is isomorphic to Δ_C Cf.[杨恩林循环同调 P31], thus Δ and Δ^{op} are all subcategories of Δ_C. ⌟

Def. (4.6.9.5). The category Δ_S is the category that $\mathrm{Aut}_{\Delta_S}([n]) \cong S^n$ and every morphism $[n] \to [m]$ in Δ_S can be uniquely written as the form φg, where $\varphi \in \mathrm{Hom}_\Delta([n],[m])$ and $g \in \mathrm{Aut}_{\Delta_S}([n])$. ⌟

Def. (4.6.9.6). For a category C, a **cyclic object** in C is a functor $\Delta_C^{op} \to C$.

For example, the functor that maps $[n]$ to C_{n+1} and the functor maps to the pull back of the order of the cyclic, is a cyclic object. ⌟

Hochschild Homology(Jeremy Hahn)

Def. (4.6.9.7)[Hochschild Homology Group]. Let R be a commutative ring and A a flat R-algebra, $A^{env} = A \otimes_R A^{op}$. Then an A^{env}-module is equivalent to an (A, A)-bimodule.

If M is an (A, A)-bimodule, then we define **Hochschild homology group** $HH_n(A/R, M) = \mathrm{Tor}_n^{env}(M, A)$. And also we denote $HH_n(A/R) = HH_n(A/R, M)$.

$H_n(A, M)$ is a $Z(A)$ module by the action of $Z(A)$ on M and HH_* defines a functor $\mathcal{CR}\mathrm{ing}_R \to \mathcal{M}\mathrm{od}_R$. ⌟

Def. (4.6.9.8)[Hochschild Complex]. Let R be a commutative ring and A a flat R-algebra, we define $A^{env} == A\otimes^L_R A^{op}$, and $HH(A/R)=A\otimes^L_{A^{env}} A\in D(A)$. ⌟

Def. (4.6.9.9) [Flat Case]. For a flat R-algebra A and a (A,A)-bimodule M, there is a simplicial module $C(A,M)$ called the **Hochschild complex** of A with coefficient in M, with $M_n=M\otimes A^n$ that

$$d_i(m,a_1,\ldots,a_n)=\begin{cases}(m_0a_1,a_2,\ldots,a_n) & i=0\\ (a_nm_0,a_1,\ldots,a_{n-1}) & i=n\\ (m_0,a_1,\ldots,a_ia_{i+1},\ldots,a_n) & \text{otherwise}\end{cases}$$

$$s_j(m,a_1,\ldots,a_n)=(m,a_1,\ldots,a_{j-i},1,a_{j+1},\ldots,a_n)$$

The homology group of the Moore complex associated to the Hochschild complex is just $HH_n(A,M)$. The Moore complex is of the form

$$\ldots\to M\otimes A\otimes A\otimes A\xrightarrow{\partial_3}M\otimes A\otimes A\xrightarrow{\partial_2}M\otimes A\xrightarrow{\partial_1}M\xrightarrow{\partial_0}0\to 0\to\ldots$$

where

$$\partial_1(m\otimes a)=ma-am,\quad \partial_2(m\otimes a_1\otimes a_2)=ma_1\otimes a_2-m\otimes a_1a-2+a_2m\otimes a_1$$

$$\partial_3(m\otimes a_1\otimes a_2\otimes a_3)=ma-1\otimes a_2\otimes a_3-m\otimes a_1a_2\otimes a_3+m\otimes a_1\otimes a_2a_3-a_3m\otimes a_1\otimes a_2.$$

⌟

Proof: □

Example (4.6.9.10).

- $HH_n(R,R)=R$ if $n=0$ and 0 otherwise.
- $HH_0(A/R,A/R)=A^{ab}$.
- If A is commutative, $HH_1(A,A)\cong\Omega^1_{A/R}$ giving by $a\otimes x\mapsto adx$ by(5.4.3.4).
- For a symmetric (A,A)-module M, thus we have $H_1(A,M)=M\otimes_A A^{ab}$ and $H_1(A,M)=M\otimes_A\Omega^1_{A/R}$. And if M is flat, $H_n(A,M)=M\otimes_A H_n(A,A)$.**?**
- $HH_n(R[X]/R)=\begin{cases}R[X] & n=0\\ \Omega^1_{R[X]/R} & n=1\\ 0 & \text{otherwise}\end{cases}$.

⌟

Example (4.6.9.11) [$HH(\mathbb{F}_p/\mathbb{Z})$]. Because $\mathbb{F}_p\otimes^L_{\mathbb{Z}}\mathbb{F}_p=(\mathbb{F}_p\xrightarrow{0}\mathbb{F}_p)$.**?**

$$HH_*(\mathbb{F}_p,\mathbb{Z})\cong\mathbb{F}_p[X_1,X_2,\ldots,]/(X_iX_j=\binom{i+j}{i}X_{i+j})$$

where $\deg(X_i)=2i,\partial X_i=0$. ⌟

Prop. (4.6.9.12). Suppose A,B are R-algebras, then

$$HH(A\otimes^L_R B/R)=HH(A/R)\otimes^L_R HH(B/R).$$

⌟

Cor. (4.6.9.13). $HH(R[X_1,\dots,X_n]/R)=\Omega^*_{R[X_1,\dots,X_n]/R}$. ⌟

Prop. (4.6.9.14). If A is a commutative R-algebra, then $HH(A/R)$ is naturally a commutative dga. In particular, $HH_*(A/R)$ is a graded ring. ⌟

Prop. (4.6.9.15) [Spectral Sequence]. For a commutative ring A and a symmetric A-bimodule M, there is a spectral sequence

$$E^2_{pq}=\mathrm{Tor}^R_p(H_p(A,A),M)\Rightarrow H_{p+q}(A,M).$$

⌟

<u>**Hochschild Homology**</u>

Prop. (4.6.9.16) [Hochschild-Kostant-Rosenberg]. The isomorphism $\Omega^1_{A/R}\cong HH_1(A)$ extends to a graded ring map

$$\Psi:\Omega^*_{A/k}\to H_*(A,A)$$

. If A/R be smooth algebra and R Noetherian, then Ψ is an isomorphism of graded algebra. Cf.[Weibel P322], [阳恩林循环同调 P133]. ⌟

Def. (4.6.9.17) [Tsygan's Double Complex]. For a cyclic objec M in an Abelian category, let t_* be the cyclic morphism and $\partial_n=\sum_{i=0}^n(-1)^i d_i$, $\partial'_n=\sum_{i=0}^{n-1}(-1)^i d_i$, $N_n=\sum_{k=0}^n((-1)^n t_n)^k$, then there is a double complex $CC(M)$:

$$\begin{array}{ccccccc}
\downarrow{\scriptstyle\partial} & & \downarrow{\scriptstyle -\partial'} & & \downarrow{\scriptstyle\partial} & & \\
M_1 & \xleftarrow{1-(-1)^1 t} & M_1 & \xleftarrow{N} & M_1 & \xleftarrow{1-(-1)^1 t} & \\
\downarrow{\scriptstyle\partial} & & \downarrow{\scriptstyle -\partial'} & & \downarrow{\scriptstyle\partial} & & \\
M_0 & \xleftarrow{1-(-1)^0 t} & M_0 & \xleftarrow{N} & M_0 & \xleftarrow{1-(-1)^0 t} &
\end{array}$$

That the column are 2-cyclic. Cf.[Weibel P337]. The first column is called the **Hochschild complex of** M: $C^h(M)$, the second column is called **acyclic complex of** M(4.6.9.18) $C^a(M)$. And we can even augment a cokernel column on the left, which is the complex of M modulo the cyclic action, called the **Conne complex** $C^\lambda(M)$.

We define the **Cyclic Homotopy Group** $HC_n(M)=H_n(\mathrm{Tot}CC(M))$ and when M is the cyclic module $C(A)$(4.6.9.9), denote $CC(C(A))=CC(A)$, $HC_n(A)=HC_n(C(A))$. ⌟

Lemma (4.6.9.18). The second column is exact and $h=t_{n+1}s_n$ is a null-homotopy. Cf.[阳恩林循环同调 P122]. ⌟

Lemma (4.6.9.19). Notice the rows are in fact a group homology $\mathrm{Hom}(\mathbb{Z}/(n+1)\mathbb{Z},M_n)$, thus when $\mathbb{Q}\in R$, we have the rows are acyclic because the group homology is killed by $|G|$(8.7.1.7), thus $HC_*(M)\cong H^\lambda_*(M)$ are isomorphisms by spectral sequence. ⌟

Prop. (4.6.9.20) [Conne SBI Sequence]. For a cyclic module M, there is a long exact sequence

$$\cdots\to HH_n(M)\xrightarrow{I}HC_n(M)\xrightarrow{S}HC_{n-2}(M)\xrightarrow{B}HH_{n-1}(M)\to\cdots$$

⌟

Proof: shift the diagram 2 column right, then there is an exact sequence of double complexes and notice the second column is exact(4.6.9.18), thus we have the kernel is quasi-isomorphic to $C^h(M)$. So the sequence follows. $\square$

Cor. (4.6.9.21). $HC_0(A) = HH_0(A) = A^{ab}$.

When A is commutative, $HC_1(A) = \mathrm{Coker}(HC_0(A) \xrightarrow{B} HH_1(A)) = \Omega^1_{A/R}/dA$ as a R module, because we can verify that $B(a) = a \otimes 1 - 1 \otimes A$. ⌟

Cor. (4.6.9.22). For a morphism of two cyclic objects, $HH_*(M) \cong HH_*(M')$ iff $HC_n(M) \cong HC_n(M')$. (Use five lemma). ⌟

Def. (4.6.9.23). A **mixed complex** (M, b, B) is a complex with $b : M_n \to M_{n-1}$ and $B : M_n \to M_{n+1}$ that makes M into a double chain complex. And there is a **Conne double complex** associated with this mixed complex. And similarly there is a same SBI sequence associated to the following diagram:

$$\begin{array}{ccccc}
\downarrow & & \downarrow & & \downarrow \\
M_2 & \xleftarrow[B]{} & M_1 & \xleftarrow[B]{} & M_0 \\
\downarrow{\scriptstyle b} & & \downarrow{\scriptstyle b} & & \\
C_1 & \xleftarrow[B]{} & C_0 & & \\
\downarrow{\scriptstyle b} & & & & \\
C_0 & & & &
\end{array}$$

From a cyclic object M, we notice that the $2k$-th column is acyclic(4.6.9.18), thus there is a snake-like connection homomorphism B that makes M into a mixed complex BM. Cf.[Weibel P344]. And the Conne double complex will compute the same cyclic homology with previous defined cyclic homology, Cf.[Weible P345].

Notice for this B, B_* on homology is exactly the composition BI. ⌟

Prop. (4.6.9.24). Let R be a unital commutative ring and A is a commutative R-algebra and M is a A-module, then there is a natural morphism

$$M \otimes_A \Omega^n_{A/R} \xrightarrow{\varepsilon_n} H_n(A, M) \xrightarrow{\pi_n} M \otimes_A \Omega^n_{A/R}.$$

such that $\pi_n \circ \varepsilon_n = n!$.

We first define a map $\varepsilon_n : M \otimes \wedge^n A \to H_n(A, M)$ that

$$\varepsilon_n(m, a_1, \ldots, a_n) = \sum \mathrm{sgn}(\sigma)(m, a_{\sigma^{-1}(1)}, \ldots, a_{\sigma^{-1}(n)})$$

then define $\varepsilon_n(m \otimes x da_1 \wedge \cdots \wedge da_n) = \varepsilon_n(mx, a_1, \ldots, a_n)$. And we verify that this map is well-defined and maps into $Z_n(C(A, M))$,Cf.[阳恩林循环同调 P99].

Then we define $\pi_n(m, a_1, \ldots, a_n) = m \otimes da_1 \wedge \cdots \wedge da_n$ and verify easily that this vanish on $B_n(C(A, M))$. And it is easy to verify $\pi_n \circ \varepsilon_n = n!$. ⌟

Prop. (4.6.9.25). When A is a unital R-algebra, there is a commutative diagram

$$\begin{array}{ccc}
\Omega^n_{A/R} & \overset{(n+1)d}{\underset{d}{\rightrightarrows}} & \Omega^{n+1}_{A/R} \\
{\scriptstyle \pi_n}\big\uparrow\big\downarrow{\scriptstyle \varepsilon_n} & & {\scriptstyle \pi_{n+1}}\big\uparrow\big\downarrow{\scriptstyle \varepsilon_{n+1}} \\
HH_n(A) & \xrightarrow{B_*} & HH_{n+1}(A)
\end{array}$$

⌟

Proof: We notice $B = (1-(-1)^n t)sN$:

$$(m, a_1, \ldots, a_n) \mapsto \sum_{i=0}^{n}(-1)^{in}(1, a_i, \ldots, a_n, m, a_1, \ldots, a_{i-1}) - \sum_{i=0}^{n}(-1)^{in}(a_i, 1, a_{i+1}, \ldots, a_n, m, a_1, \ldots, a_{i-1}).$$

Cf.[阳恩林循环同调 P128]. □

Cor. (4.6.9.26). For a commutative unital R-algebra A, there is a functorial $\varepsilon_n : \Omega^n_{A/R}/d\Omega^{n-1}_{A/R} \to HC_n(A)$ making the following diagram commutative:

$$\begin{array}{ccccccccc}
\xrightarrow{0} & \Omega^{n-1}/d\Omega^{n-2} & \xrightarrow{d} & \Omega^n & \longrightarrow & \Omega^n/d\Omega^{n-1} & \xrightarrow{0} & \Omega^{n-2}/d\Omega^{n-3} & \longrightarrow \cdots \\
 & \downarrow{\scriptstyle \varepsilon_{n-1}} & & \downarrow{\scriptstyle \varepsilon_n} & & \downarrow{\scriptstyle \varepsilon_n} & & \downarrow{\scriptstyle \varepsilon_{n-2}} & \\
\longrightarrow & HC_{n-1} & \xrightarrow{B} & HH_n & \xrightarrow{I} & HC_n & \xrightarrow{S} & HC_{n-2} & \xrightarrow{B} \cdots
\end{array}$$

which is induced by the cokernel. Cf.[阳恩林循环同调 P130]. When $\mathbb{Q} \in R$, ε_n is a split injection. ⌟

Prop. (4.6.9.27). When $\mathbb{Q} \in R$, $\frac{1}{n!}\pi_n$ induces a morphism of mixed complexes $(BA, \partial, B) \to (\Omega^*_{A/R}, 0, d)$ by(4.6.9.24), thus there is a natural map

$$HC_n(A) \to \Omega^n_{A/R}/d\Omega^{n-1}_{A/R} \bigoplus_{i>0} H^{n-2i}_{dR}(A).$$

⌟

Prop. (4.6.9.28) [Morita Invariance]. $Tr : HH_*(M_r(A), M_r(M)) \cong HH_*(A, M)$ by the trace and inclusion functors. Cf.[阳恩林循环同调 Morita Invariance]. In particular, there is an isomorphism $HH_*(M_r(A)) \cong HH_*(A)$, thus also $HC_*(M_r(A)) \cong HC_*(A)$ by(4.6.9.20). ⌟

Prop. (4.6.9.29) [Karoubi]. BG is a cyclic group, and then the cyclic homology group $HC_n(G, A) \cong \bigoplus_{k\geq 0} H_{n-2k}(G, A)$. Cf.[Weibel P339]. ⌟

4.7 ∞-Categories

References are [Joy02], [Lur09], [Lur11], [Infinity Categories from Scratch], [A whirlwind tour of the world of $(\infty,1)$-categories], [Gro15], [Introduction to ∞-Categories].

Notation (4.7.0.1).
- Use notations defined in Simplicial Homotopy Theory.

⌟

1 ∞-Categories

Def. (4.7.1.1) [∞-Category]. An **∞-category** is a simplicial set that has lifting property w.r.t any $\Lambda^n_i \to \Delta^n$, where $0 < i < n$. ⌟

Cor. (4.7.1.2). By(4.6.3.6), the nerve of a category is an ∞-category. ⌟

Def. (4.7.1.3)[Sub$-\infty$-Categories]. Let $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$ and $\mathcal{D}_0 \subset \mathcal{C}_0$ be a subset of vertices, then there is a sub-simplicial set $\mathcal{D} \subset \mathcal{C}$ consisting of simplexes with all vertices in $\mathcal{C}$. Then it is also an ∞-category, called the **∞-category spanned by** $\mathcal{D}_0$. ⌟

Prop. (4.7.1.4) [Characterizing ∞-Categories]. $\mathcal{C} \in s\,\mathcal{S}\mathrm{et}$ is an ∞-category iff the restriction map

$$\mathrm{Map}(\Delta^2, \mathcal{C}) \to \mathrm{Map}(\Lambda^2_1, \mathcal{C})$$

is a trivial Kan fibration. ⌟

Proof: This follows immediately from(4.6.3.30). □

Def. (4.7.1.5) [Homotopy Categories of ∞-Categories]. For $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$, the homotopy category of $\mathcal{C}$(4.6.4.12) has a simpler description: Let $f, g : X \to Y \in \mathcal{C}$ be called **homotopic maps** if there is a 2-complex of the form $\begin{array}{ccc} & X & \\ {\scriptstyle \mathrm{id}}\nearrow & & \searrow{\scriptstyle f} \\ X & \xrightarrow{\ g\ } & Y \end{array}$. $f : X \to Y$ is called an **equivalence** if there exists a map $g : Y \to X$ s.t. $f \circ g \cong \mathrm{id}_Y$ and $g \circ f \cong \mathrm{id}_X$.

Then the homotopy relation is an equivalence relation, and the composition of homotopic maps are homotopic, and we get a category $\mathrm{Ho}(\mathcal{C})$. Then this category is naturally isomorphic to $\tau_1(\mathcal{C})$(4.6.3.3). ⌟

Proof: [Lur09]P32. □

Prop. (4.7.1.6) [Equivalence of ∞-Categories]. Categorical equivalence(4.6.4.12) between ∞-categories is an equivalence relation(4.6.4.12), by Joyal model category(4.6.4.19). ⌟

Def. (4.7.1.7)[Underlying ∞-Categories of Simplicial Model Categories]. Let $\mathcal{M}$ be a simplicial model category(4.6.5.1), then $N_\Delta(\mathcal{M}_{cf})$ is an ∞-category by(4.6.4.4)**?**, called the **underlying ∞-category** of $\mathcal{M}$. ⌟

Lemma (4.7.1.8). Let $\mathcal{S} = s\,\mathcal{S}\mathrm{et}$, then the map $\beta_{X,S}$ is a weak equivalence for every cofibrant object $X \in \mathcal{C}$. ⌟

Proof: Cf.[HTT, P853]. □

Prop. (4.7.1.9) [Quillen Equivalent Simplicial Model Categories Give Equivalent Underlying ∞-Categories]. Let $\mathcal{C},\mathcal{D}$ be simplicial model categories and

$$F:\mathcal{C}\xrightarrow{\text{Quillen}}\mathcal{D}:G$$

is a Quillen equivalence, every element of $\mathcal{C}$ is cofibrant, and G is a simplicial functor, then G induces an equivalence of their underlying ∞-categories $N_\Delta(\mathcal{D}_{cf})\cong N_\Delta(\mathcal{C}_{cf})$. ⌟

Proof: This is because $G:\mathcal{D}_{cf}\to\mathcal{C}_{cf}$ is an equivalence of simplicial categories, by(4.5.7.6) and (4.7.1.8), and then(4.6.4.16) shows $N_\Delta(G):N_\Delta(\mathcal{D}_{cf})\to N_\Delta(\mathcal{C}_{cf})$ is an equivalence of ∞-categories. □

Def. (4.7.1.10) [Homotopy Coherent Diagrams]. Let $\mathcal{C}\in\mathcal{C}\mathrm{at}_\infty$ and $\mathcal{I}\in\mathcal{C}\mathrm{at}$, then a **homotopy coherent $\mathcal{I}$-diagram** is a map $N(\mathcal{I})\to\mathcal{C}\in s\,\mathcal{S}\mathrm{et}$. ⌟

Categorical Constructions

Def. (4.7.1.11) [Categorical Constructions]. A **categorical construction** is a functorial construction $T:(s\,\mathcal{S}\mathrm{et})^m\times(s\,\mathcal{S}\mathrm{et}^{\mathrm{op}})^n\to s\,\mathcal{S}\mathrm{et}$ s.t.

- For $\mathcal{C}_i\in\mathcal{C}\mathrm{at}\subset s\,\mathcal{S}\mathrm{et}$, $T(\mathcal{C}_1,\ldots,\mathcal{C}_n)\subset\mathcal{C}\mathrm{at}\subset\mathcal{C}\mathrm{at}_\infty$.
- For $\mathcal{C}_i\in\mathcal{C}\mathrm{at}_\infty\subset s\,\mathcal{S}\mathrm{et}$, $T(\mathcal{C}_1,\ldots,\mathcal{C}_n)\subset\mathcal{C}\mathrm{at}_\infty$.
- If for each i, $\mathcal{C}_i,\mathcal{D}_i\in\mathcal{C}\mathrm{at}_\infty\subset s\,\mathcal{S}\mathrm{et}$ are categorically equivalent, then $T(\mathcal{C}_1,\ldots,\mathcal{C}_n)$ and $T(\mathcal{D}_1,\ldots,\mathcal{D}_n)$ are equivalent ∞-categories.

⌟

Prop. (4.7.1.12) [Opposite ∞-Categories]. For $\mathcal{C},\mathcal{D}\in\mathcal{C}\mathrm{at}_\infty$,

- The opposite(4.6.3.12) $\mathcal{C}^{\mathrm{op}}$ is also an ∞-category.
- If $\mathcal{C}\to\mathcal{D}$ is a categorical equivalence, then $\mathcal{C}^{\mathrm{op}}\to\mathcal{D}^{\mathrm{op}}$ is also a categorical equivalence.

Thus the opposite construction is a categorical construction, by(4.6.3.13). ⌟

Proof: □

Prop. (4.7.1.13) [Mapping Spaces of ∞-Categories]. Let $\mathcal{C},\mathcal{D}\in\mathcal{C}\mathrm{at}_\infty$ and $K,K'\in s\,\mathcal{S}\mathrm{et}$, then

- $\mathrm{Map}(K,\mathcal{C})$ is also an ∞-category.
- If $f:\mathcal{C}\to\mathcal{D}$ is a categorical equivalence, then the induced map $\mathrm{Map}(K,\mathcal{C})\to\mathrm{Map}(K,\mathcal{D})$ is also a categorical equivalence.
- If $g:K\to K'$ is a categorical equivalence, then the induced map $\mathrm{Map}(K',\mathcal{C})\to\mathrm{Map}(K,\mathcal{C})$ is also a categorical equivalence.

In particular, mapping space is a categorical construction, by(4.6.3.16). ⌟

Proof: 1 follows from(4.6.3.31). 2, 3 follow from [HTT, P94].**?** □

Prop. (4.7.1.14) [Joins of ∞-Categories]. Let $\mathcal{C},\mathcal{D}\in\mathcal{C}\mathrm{at}_\infty$, then

- The join(4.6.3.18) $\mathcal{C}*\mathcal{D}$ is also an ∞-category.
- If $\mathcal{C}\to\mathcal{C}',\mathcal{D}\to\mathcal{D}'\in\mathcal{C}\mathrm{at}_\infty$ are categorical equivalences, then $\mathcal{C}*\mathcal{D}\to\mathcal{C}'*\mathcal{D}'$ is also a categorical equivalence.

In particular, the join is a categorial construction by(4.6.3.19). ⌟

Proof: 1: Given a morphism $p : \Lambda_i^n \to S \star S'$, if the image is in S or S', then it can be extended to Δ^n by hypothesis. Thus we may assume that it maps $\{0, \ldots, j\}$ into S and $\{j+1, \ldots, n\}$ into S', then we restricts p to get a morphism $\Delta^{\{0,\ldots,j\}} \to S, \Delta^{\{j+1,\ldots,n\}} \to S'$, which determines a map $\Delta^n \cong \Delta^j * \Delta^{n-j-1}$(4.6.3.19) $\to S \star S'$, and it extends p by(4.6.3.17).

2 follows from(4.6.4.26). □

Prop. (4.7.1.15) [Homotopic Maps]. If X is an ∞-category, then so does X^B for any simplicial set B, by(4.6.3.37).

And we can call two maps in $\mathrm{Map}(B, X)$ **homotopic** if they are equivalent as vertices in X^B(4.7.1.5). ⌟

Lemma (4.7.1.16). Let $p : \mathcal{C} \to \mathcal{D}$ be a left fibration of ∞-categories and $f : X \to Y$ be a morphism that $p(f)$ is an equivalence in $\mathcal{D}$, then f is an equivalence in $\mathcal{D}$. Compare with(4.2.3.8). ⌟

Proof: Let $\overline{g}$ be a homotopy inverse to f, then there is a 2-complex

$$\begin{array}{ccccc} & & p(Y) & & \\ & {}^{p(f)}\nearrow & & \searrow^{\overline{g}} & \\ p(X) & & \longrightarrow & & p(X) \end{array}$$

and by left fibration property lifts to a 2-complex

$$\begin{array}{ccccc} & & Y & & \\ & {}^{f}\nearrow & & \searrow^{g} & \\ X & & \longrightarrow & & X \end{array}.$$

So f admits a left homotopy inverse, and by the same reason, g admits a left homotopy inverse, thus g has a left homotopy inverse, and it can be chosen to be f. □

Lemma (4.7.1.17) [Equivalence Lifts via Left Fibrations]. Let $p : \mathcal{C} \to \mathcal{D}$ be a left fibration of ∞-categories, if $\overline{X} \in \mathcal{D}$ and $Y \in \mathcal{C}$ and $\overline{f} : \overline{X} \to p(Y)$ is an equivalence, then $\overline{f}$ can be lifted to a morphism in $\mathcal{C}$.(Which is also an equivalence by(4.7.1.16)). ⌟

Proof: □

Prop. (4.7.1.18) [Equivalence and Left Extension]. Let $\mathcal{C}$ be an ∞-category and φ an edge, then φ is an equivalence iff for any $n \geq 2$ and every map $\Lambda_0^n \to \mathcal{C}$ that $f_0|\Delta^{\{0,1\}} = \varphi$, there exists an extension of f_0 to Δ^n. ⌟

Proof: If φ is an equivalence, then consider the diagram

$$\begin{array}{ccc} \{0\} & \longrightarrow & \mathcal{C}/\Delta^{n-2} \\ \big\downarrow & \nearrow & \big\downarrow q \\ \Delta^1 & \xrightarrow{\varphi'} & \mathcal{C}/\partial\Delta^{n-2} \end{array}$$

Because $\mathcal{C}/\partial\Delta^{n-2} \to \mathcal{C}$ is right fibration(4.6.3.36), and by the dual of(4.7.1.16), φ' is an equivalence, thus by the dual of(4.7.1.17) the dotted arrow exists.

Conversely, if the condition holds, then we can use a diagram $\Lambda_0^2 \to \mathcal{C}$ to find a morphism ψ that $\psi \circ \varphi \cong \mathrm{id}$, and we can also use a diagram $\Lambda_0^3 \to \mathcal{C}$ to witness the fact $\varphi \circ \psi \cong \mathrm{id}$, so φ is an equivalence. □

Cor. (4.7.1.19). An equivalence in $\mathrm{Map}(K, \mathcal{C})$ is equivalent to a map $K \times \Delta^1 \to \mathcal{C}$ that $\{x\} \times \Delta$ are all mapped to equivalences in $\mathcal{C}$. ⌟

Proof: ? Cf.[HTT, P106]. □

Def. (4.7.1.20) [Space of Morphisms]. For vertices x, y in a simplicial set S, we want to defines a representative for $\mathrm{Map}_{hS}(x, y)$ other than $\mathrm{Map}_{\mathfrak{C}[S]}(x, y)$. We define the **space of right morphisms**

$$\mathrm{Hom}^R_S(x, y) = S_{/y} \times_S \{x\}.$$

The definition is not symmetric, instead, we define the **space of left morphisms** $\mathrm{Hom}^L_S(x, y) = (\mathrm{Hom}^R_{S^{op}}(x, y))^{op}$.

Also we can define $\mathrm{Hom}_S(x, y) = \{x\} \times_S S^{\Delta^1} \times_S \{y\}$, then there are natural inclusions:

$$\mathrm{Hom}^R_S(x, y) \hookrightarrow \mathrm{Hom}_S(x, y) \hookleftarrow \mathrm{Hom}^L_S(x, y) .$$

⌟

Prop. (4.7.1.21). If $\mathcal{C} \in \mathcal{C}at_\infty$ and $x, y \in \mathcal{C}$, then $\mathrm{Hom}^R_{\mathcal{C}}(x, y)$ is a Kan complex, and the inclusions defined in(4.7.1.20) are weak equivalences. ⌟

Proof: This is obvious, because the right lifting diagram w.r.t. $\Lambda^n_j \subset \Delta^n, 0 < j \le n$ is equivalent to an extension $\Lambda^n_j \star \Delta^0 \subset \Delta^{n+1}$ that satisfies $\widetilde{u}|_{\Delta\{0,\ldots,n\}} = x$. It can be solved by a two-step extension where the first is by identity extension and then extend using inner fibration property.

For the last assertion, Cf.[HTT, 4.2.1.8].? □

Prop. (4.7.1.22). Let $p : \mathcal{C} \to \mathcal{D}$ be an inner fibration of ∞-categories, then the the induced maps on the spaces of right morphisms are Kan fibrations. ⌟

Proof: Since p is an inner fibration, the induced map $\widetilde{\varphi} : \mathcal{C}_{/Y} \to \mathcal{D}_{/p(Y)} \times_{\mathcal{D}} \mathcal{C}$ is a right fibration by(4.6.3.36), and the morphism on $\mathrm{Hom}^R_{\mathcal{C}}(X, Y)$ is obtained from $\widetilde{\varphi}$ by restricting to fiber over X, thus also a right fibration. And by(4.7.1.21) and(4.6.3.42). □

Lemma (4.7.1.23). Let $\mathcal{C} \to \mathcal{D}$ be a fully faithful map of ∞-categories and $p : K \to \mathcal{C} \in s\mathcal{S}\mathrm{et}$, then the map of ∞-categories(4.7.1.24)

$$\mathcal{C}_{j/} \times_{\mathcal{C}} \{x\} \to \mathcal{D}_{pj/} \times_{\mathcal{D}} \{p(x)\}$$

is a homotopy equivalence. ⌟

Proof: Cf.[HTT, P134]. □

Prop. (4.7.1.24) [Overcategories and Undercategories].

- If $\mathcal{C}$ be an ∞-category and $p : K \to \mathcal{C}$ be an morphism, then the projection $\mathcal{C}_{p/} \to \mathcal{C}$ is a left fibration. In particular, $\mathcal{C}_{p/}$ is itself an ∞-category. Dually, $C_{/p}$ is also an ∞-category.
- Let $p : \mathcal{C} \to \mathcal{D} \in \mathcal{C}at_\infty$ be an equivalence of ∞-categories and let $j : K \to \mathcal{C} \in s\mathcal{S}\mathrm{et}$, then the induced map $\mathcal{C}_{j/} \to \mathcal{D}_{pj/}$ is an equivalence of ∞-categories. The dual holds for undercategories.

In particular, the overcategories and undercategories are categorial constructions, by(4.6.3.24). ⌟

Proof: 1: We use the proposition(4.6.3.36) in case $S = \Delta^0, A = \varnothing, X = \mathcal{C}$.

2: There is a factorization $\mathcal{C}_{j/} \xrightarrow{f} \mathcal{D}_{pj/} \times_{\mathcal{D}} \mathcal{C} \xrightarrow{g} \mathcal{D}_{pj/}$. (4.7.1.23)(4.7.1.24) shows $C_{j/}$ and $\mathcal{D}_{pj/} \times_{\mathcal{D}} \mathcal{C}$ are fiberwise equivalent left fibrations over $\mathcal{C}$, thus by(4.6.7.7) and(4.6.7.10), f is a categorical equivalence. Also, g is a categorical equivalence by(4.6.7.11). So we are done. **?**Cf.[HTT, P135]. □

Prop. (4.7.1.25)[Lifting of Homotopies]. Let $p : \mathcal{C} \to \mathcal{D}$ be a categorical equivalence of ∞-categories and $A \subset B$ be an inclusion of simplicial sets. Let $f_0 : A \to \mathcal{C}, g : B \to \mathcal{D}$ be any maps that $h_0 : A \times \Delta^1 \to \mathcal{D}$ be an equivalence between $g|_A$ and $p \circ f_0$, then there exists a map $B \to \mathcal{C}$ and an equivalence $h : B \times \Delta^1 \to \mathcal{D}$ between g and $p \circ f$ that $h_0 = h|_{A \times \Delta^1}$. ┘

Proof: Working with simplexes, it suffices to prove for $A = \partial\Delta^n \subset B = \Delta^n$. The case $n = 0$ is true because categorical equivalence is essentially surjective. For $n > 0$, we need to construct h from $h|_{\Delta^n \times \{0\} \coprod \partial\Delta^n \times \Delta^1}$, and this is a composition of pushout of $\Lambda^{n+1}_k \subset \Delta^{n+1}$. For $k \neq 0$, the extension is clear because $\mathcal{D}$ is ∞-category, and for $k = 0$, we need to use [HTT, P136]. □

∞-Groupoids(or Kan Complexes/Spaces)

Def. (4.7.1.26) [∞-Groupoid]. An **∞-groupoid** or an **anima** is an ∞-category $\mathcal{C}$ that $\mathrm{Ho}(\mathcal{C})$ is a groupoid(4.7.1.5), or equivalently, all morphisms are equivalences. The full subcategory of $\mathcal{C}at_\infty$ consisting of ∞-groupoids are denoted by $\mathcal{G}rpd_\infty$. ┘

Prop. (4.7.1.27) [∞-Groupoids $\iff$ Kan Complex]. For $\mathcal{C} \in s\,\mathcal{S}et$, the following are equivalent:

- $\mathcal{C}$ is an ∞-groupoid.
- $\mathcal{C} \to \Delta^0$ is a left fibration.
- $\mathcal{C} \to \Delta^0$ is a right fibration.
- $\mathcal{C}$ is a Kan complex.

┘

Proof: 1, 2 are equivalent by(4.7.1.18), and dually 1, 3 are equivalent, and $4 = 2 + 3$. □

n-Categories

Def. (4.7.1.28) [n-Categories]. For $\mathcal{C} \in s\,\mathcal{S}et$ and $n \geq -1$, then $\mathcal{C}$ is called an n-**category** if it is an ∞-category and:

- Given any maps $f, f' : \Delta^n \to \mathcal{C}$ that are homotopic(4.7.1.15) relative to $\partial\Delta^n$, then $f = f'$.
- For any $m > n$ and maps $f, f' : \Delta^m \to \mathcal{C}$ that coincide on $\partial\Delta^m$, then $f = f'$.

Also $\mathcal{C}$ is called an (-2)-category iff it is isomorphic to Δ^0.

The definition of an n-category is equivalent to the following: if $f, f' : K \to \mathcal{C}$ satisfies $f|_{sk^n K}$ is homotopic to $f'|_{sk^n K}$ relative to $\mathrm{sk}^{n-1} K$, then $f = f'$. ┘

Cor. (4.7.1.29). If $\mathcal{C}$ is an n-category and $m > n$, then the restriction map $\mathrm{Hom}(\Delta^m, \mathcal{C}) \to \mathrm{Hom}(\partial\Delta^m, \mathcal{C})$ is bijective.(use ∞-category property to extend). ┘

Prop. (4.7.1.30). A (-1)-category is seen to be isomorphic to $\varnothing$ or Δ^0. A 0-category is equivalent to the nerve of a partially ordered set. ┘

Proof: □

Prop. (4.7.1.31) [$\mathcal{C}at$ and $\mathcal{C}at_1$]. For a simplicial set S, the following are equivalent:

- $u : S \to N(hS)$(4.6.3.3) is an isomorphism of simplicial sets.
- There is a small category $\mathcal{C}$ that $S \cong N(\mathcal{C})$.
- S is a 1-category.

⌟

Proof: It suffices to show 3 → 1: we induct on the dimension: $n = 0$ is trivial and $n = 1$ follows from the definition of 1-category(4.7.1.28). For $n > 1$, the injectivity of u follows from induction hypothesis and(4.7.1.28), and for surjectivity, for a map $\Delta^n \to N(hS)$, choose $0 < i < n$ and let lift Λ_i^n to S, then use the fact S is an ∞-category to lift to Δ^n, and now it coincide on $N(hS)$ because it is a nerve of a category. □

Prop. (4.7.1.32). If $\mathcal{C}$ is an n-category, then for any simplicial set X, $\mathcal{C}^X$ is also an n-category. ⌟

Proof: This is because $sk^p(K \times X) \subset sk^p(K) \times X$ for any simplicial set K and integer p, and use(4.7.1.28). □

Prop. (4.7.1.33). Let $n \geq 1$ and $\mathcal{C}$ an ∞-category, then $\mathcal{C}$ is an n-category iff it satisfies the unique lifting property w.r.t. the inclusion $\Lambda_i^m \subset \Delta^m$, where $0 < i < m$. ⌟

Proof: Cf.[HTT, P109]. □

Def. (4.7.1.34) [n-Truncated Kan Complexes]. Let X be a Kan complex and $k \geq -1$, then a Kan complex is called **k-truncated** if for every $i > k$ and every point $x \in X$, we have $\pi_i(X, x) \cong *$. And it is called (-2)**-truncated** if it is contractible. ⌟

Prop. (4.7.1.35). A (-1)-truncated Kan complex is either empty or contractible. A 0-contractible Kan complex is a Kan complex that $X \to \pi_0(X)$ is a homotopy equivalence. ⌟

Proof: ?. □

Prop. (4.7.1.36) [Equivalent to an n-Category]. Let $\mathcal{C}$ be an ∞-category and $n \geq -1$, then the following conditions are equivalent:

- There is a minimal model $\mathcal{C}' \subset \mathcal{C}$ that is n-truncated.
- $\mathcal{C}$ is categorically equivalent to an n-truncated category.
- For any $X, Y \in \mathcal{C}$, the mapping space $\mathrm{Map}(X, Y)$ is $(n-1)$-truncated.

⌟

Proof: Cf.[HTT, P112]. □

Cor. (4.7.1.37). A Kan complex is categorically equivalent to an n-category iff it is n-truncated. ⌟

Proof: Cf.[HTT, P113]?. □

Cor. (4.7.1.38). Let $\mathcal{C}$ be an ∞-category and K a simplicial set, if $\mathrm{Map}(C, D)$ is n-truncated for any objects $C, D \in \mathcal{C}$, then the ∞-category $\mathcal{C}^K$ has the same property. ⌟

Proof: Cf.[HTT, P114]. □

2 ∞-Category of ∞-Categories

Def. (4.7.2.1) [Models on $s\,\mathcal{S}\mathrm{et}^+$]. There is a simplicial model structure on $s\,\mathcal{S}\mathrm{et}^+$(4.6.3.52) s.t. the fibrant and cofibrant objects are exactly objects of the form $\mathcal{C}^\natural$ where $\mathcal{C}$ is an ∞-category, and $\mathcal{C}^\natural = (\mathcal{C}, \mathcal{E}_\mathcal{C})$ where $\mathcal{E}_\mathcal{C}$ is the set of equivalences in $\mathcal{C}$(4.7.1.5). ⌟

Proof: ? □

Def. (4.7.2.2) [$\mathcal{C}\mathrm{at}_\infty$]. The underlying ∞-category $\mathcal{C}\mathrm{at}_\infty = N_\Delta(s\,\mathcal{S}\mathrm{et}^+_{cf})$ of $s\,\mathcal{S}\mathrm{et}^+$ is called the **∞-category of ∞-category of ∞-categories**. It can be verified that the fundamental category of $\mathcal{C}\mathrm{at}_\infty$ consists of equivalent classes of ∞-categories. ⌟

Def. (4.7.2.3) [Relative Mapping Spaces]. Let $p : X \to S, q : Y \to S \in s\,\mathcal{S}\mathrm{et}$, then define $\mathrm{Map}_S(X,Y) = \mathrm{Map}_{\mathcal{C}\mathrm{at}_\infty/T}(X,Y) \in s\,\mathcal{S}\mathrm{et}$. ⌟

(∞, n)-Categories

Def. (4.7.2.4) [(∞, n)-Categories]. For $n \in \mathbb{N}$, an (∞, n)-category is an ∞-category s.t. for $k > n$, any k-maps is invertible?. In particular, an $(\infty, 0)$-category is just an ∞-groupoid. ⌟

Def. (4.7.2.5) [$\mathcal{G}\mathrm{rpd}_\infty$]. The underlying ∞-category $N_\Delta(\mathrm{Kan})$ of $s\,\mathcal{S}\mathrm{et}$ with the Joyal model structure(4.6.4.19) is denoted by $\mathcal{G}\mathrm{rpd}_\infty$. Then it is an sub-$\infty$-category of $\mathcal{C}\mathrm{at}_\infty$, and it is an $(\infty, 1)$-category. ⌟

Proof: ? □

3 Limits and Colimits

Remark (4.7.3.1) [Universal Properties]. The objects in an ∞-category characterized by a universal property will be a contractible Kan complex. ⌟

Def. (4.7.3.2) [Final Objects]. For $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$, $x \in \mathcal{C}$ is called a **final object** if the canonical map $\mathcal{C}_{/x} \to \mathcal{C} \in s\,\mathcal{S}\mathrm{et}$ is a trivial Kan fibration. Equivalently, for any $y \in \mathcal{C}$, $\mathrm{Map}^R_\mathcal{C}(y,x)$ is a contractible Kan complex. It is clear that the sub-∞-category of final objects in $\mathcal{C}$ is either empty or a contractible Kan complex.

Dually we can define initial objects. ⌟

Proof: If x is a final object, then $\mathrm{Map}^R_\mathcal{C}(y,x)$ is the fiber of $\mathcal{C}_{/x} \to \mathcal{C}$ over x(4.7.1.20), so it is a contractible Kan-complex by(4.7.1.27). The converse follows from(4.6.3.46). □

Cor. (4.7.3.3). For $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$ with a final object $*$, we fix a final object, then there is a section $\mathcal{C} \to \mathcal{C}_{/*}$, which maps each $C \in \mathcal{C}$ to a morphism $C \to * \in \mathcal{C}$. We fix such a morphism. The dual is true for initial objects. ⌟

Prop. (4.7.3.4). If $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$ and $* \in \mathcal{C}$ is final, then for any diagram $p : K \to \mathcal{C}$, $*$ is also final in $\mathcal{C}_{p/}$.? ⌟

Def. (4.7.3.5) [Limits and Colimits]. For $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$ and $p : K \to \mathcal{C} \in \mathcal{C}\mathrm{at}$, a **colimit** of p is defined to be an initial object of $\mathcal{C}_{p/}$, and a **limit** of p is defined to be a final object of $\mathcal{C}_{/p}$. By(4.7.3.2), (co)limits are defined up to a contractible choice, and we may use $(\varinjlim_p)\ \varprojlim_p$ to denote any one of them. ⌟

Def. (4.7.3.6). For $\mathcal{C}, \mathcal{D} \in \mathcal{C}at_\infty$, let $\mathrm{Func}^L(\mathcal{C}, \mathcal{D})$ denote the sub-∞-category of $\mathrm{Func}(\mathcal{C}, \mathcal{D})$ consisting of functors preserving colimits, and let $\mathrm{Func}^R(\mathcal{D}, \mathcal{C})$ denote the sub-∞-category of $\mathrm{Func}(\mathcal{D}, \mathcal{C})$ consisting of functors preserving limits. ⌟

Prop. (4.7.3.7). For $\mathcal{C}, \mathcal{D} \in \mathcal{C}at_\infty$, there is a natural equivalence of ∞-categories $\mathrm{Func}^L(\mathcal{C}, \mathcal{D}) \cong \mathrm{Func}^R(\mathcal{D}, \mathcal{C})^{\mathrm{op}}$. ⌟

Proof: Cf.[Lur09]P356. □

Cofinal Diagrams

Def. (4.7.3.8) [Cofinal Maps]. A **cofinal map** $p : S \to T \in s\,\mathcal{S}\mathrm{et}$ is a map s.t. for any right fibration $X \to T \in s\,\mathcal{S}\mathrm{et}$,

$$\mathrm{Map}_T(T, X) \to \mathrm{Map}_T(S, X) \in s\,\mathcal{S}\mathrm{et}(4.7.2.3)$$

is a homotopy equivalence. ⌟

Prop. (4.7.3.9) [Cofinal Maps give Same Colimits]. For $v : K' \to K \in s\,\mathcal{S}\mathrm{et}$, the following are equivalent:

- v is cofinal.
- for any $\mathcal{C} \in \mathcal{C}at_\infty$ and $p : K \to \mathcal{C} \in s\,\mathcal{S}\mathrm{et}$, the induced map $\mathcal{C}_{p/} \to \mathcal{C}_{p\circ v/}$ is an equivalence of ∞-categories.

⌟

Proof: Cf.[Lur09]P226. □

Computing Diagrams

Prop. (4.7.3.10) [Reducing to Coherent Colimits]. For any $K \in s\,\mathcal{S}\mathrm{et}$, there exists a category $\mathcal{I} \subset \mathcal{C}at$ and a cofinal map $N(\mathcal{I}) \to K \in s\,\mathcal{S}\mathrm{et}$. ⌟

Proof: Cf.[Lur09]P255. □

Prop. (4.7.3.11) [Colimits in Overcategories]. Let $\mathcal{C} \in \mathcal{C}at_\infty$ and $q : T \to \mathcal{C} \in s\,\mathcal{S}\mathrm{et}, p : K \to \mathcal{C}_{/q}$, and $p_0 : K \xrightarrow{p} \mathcal{C}_{/q} \to \mathcal{C}$. If p_0 has a colimit, then

- p also has a colimit, and the colimit is preserved by the $\mathrm{pr} : \mathcal{C}_{/q} \to \mathcal{C}$.
- $x \in \mathcal{C}_{/q}$ is a colimit of p iff $\mathrm{pr}(x) \in \mathcal{C}$ is a colimit of p_0.

⌟

Proof: Cf.[Lur09]P48. □

Cor. (4.7.3.12) [Colimits in Diagram Categories]. For $K, S \in s\,\mathcal{S}\mathrm{et}$, let $\mathcal{C}$ be an ∞-category that admits K-indexed colimits, then

- the ∞-category $\mathrm{Func}(S, \mathcal{C})$(4.7.1.13) also admits K-indexed colimits.
- $p : K^{\triangleright} \to \mathrm{Func}(S, \mathcal{C})$ is a colimit diagram iff for each $C \in \mathcal{C}$, the evaluation $p_C : K^{\triangleright} \to \mathcal{C}$ is a colimit diagram.

⌟

Proof: Cf.[Lur09]P315. □

Kan Extensions

Def. (4.7.3.13) [p-Left Kan Extensions]. For a commutative diagram of ∞-categories

$$\begin{array}{ccc} \mathcal{C}^0 & \xrightarrow{F_0} & \mathcal{D} \\ \big\downarrow & \overset{F}{\nearrow} & \big\downarrow p \\ \mathcal{C} & \longrightarrow & \mathcal{D}' \end{array},$$

F is called a **p-left Kan extension** of F_0 if for any $C \in \mathcal{C}$, the induced diagram

$$\begin{array}{ccc} \mathcal{C}^0_{/C} & \xrightarrow{F_C} & \mathcal{D} \\ \big\downarrow & \overset{F}{\nearrow} & \big\downarrow p \\ (\mathcal{C}^0_{/C})^{\triangleright} & \longrightarrow & \mathcal{D}' \end{array},$$

exibits C as a p-colimit? of F_C. ⌟

Lemma (4.7.3.14) [Existence of p-Left Kan Extensions]. Given a commutative diagram of ∞-categories

$$\begin{array}{ccc} \mathcal{C}^0 & \xrightarrow{F_0} & \mathcal{D} \\ \big\downarrow & \overset{F}{\dashrightarrow} & \big\downarrow p \\ \mathcal{C} & \longrightarrow & \mathcal{D}' \end{array},$$

then there exists a p-left Kan extension F iff for any $C \in \mathcal{C}$ the composition

$$\mathcal{C}^0_{/p} \to \mathcal{C}^0 \xrightarrow{F_0} \mathcal{D}$$

admits a p-colimit. ⌟

Proof: Cf.[Lur09]P282. □

Lemma (4.7.3.15). Let $\mathcal{C} \to \mathcal{D}' \overset{p}{\leftarrow} \mathcal{D} \in \mathcal{C}at_\infty$ where p is a Joyal-fibration, and $\mathcal{C}^0 \subset \mathcal{C}$ a full subcategory, the the restriction functor

$$i^* : \mathrm{Func}_{\mathcal{D}'}(\mathcal{C}, \mathcal{D}) \to \mathrm{Func}_{\mathcal{D}'}(\mathcal{C}^0, \mathcal{D})$$

has right lifting property w.r.t. all $\partial\Delta^n \to \Delta^n$ s.t. the map $\partial\Delta^n$ maps $\{0\}$ to a functor $F : \mathcal{C} \to \mathcal{D}$ which is a p-left Kan extension(4.7.3.13) of $F|_{\mathcal{C}^0}$, ⌟

Proof: Cf.[Lur09]P279. □

Prop. (4.7.3.16). Let $\mathcal{C} \to \mathcal{D}' \overset{p}{\leftarrow} \mathcal{D} \in \mathcal{C}at_\infty$ where p is a Joyal-fibration, and $\mathcal{C}^0 \subset \mathcal{C}$ a full subcategory. Let

- $\mathcal{K} \subset \mathrm{Func}_{\mathcal{D}'}(\mathcal{C}, \mathcal{D})$ be the full subcategory of functors $F : \mathcal{C} \to \mathcal{D}$ which are p-left Kan extensions(4.7.3.13) of $F|_{\mathcal{C}^0}$,
- $\mathcal{K}' \subset \mathrm{Func}_{\mathcal{D}'}(\mathcal{C}^0, \mathcal{D})$ be the category of functors $F_0 : \mathcal{C}^0 \to \mathcal{D}$ s.t. for any $C \in \mathcal{C}$, the induced functor $\mathcal{C}^0_{/C} \to \mathcal{D}$ has a p-colimit.

Then the restriction functor $i^* : \mathcal{K} \to \mathcal{K}'$ is a trivial Kan fibration. ⌟

Proof: This follows immediately from(4.7.3.14) and(4.7.3.15). □

Cor. (4.7.3.17) [Functorial Left Kan Extensions]. Let $\mathcal{C} \to \mathcal{D}' \xleftarrow{p} \mathcal{D} \in \mathcal{C}\mathrm{at}_\infty$ where p is a Joyal-fibration, and $\mathcal{C}^0 \subset \mathcal{C}$ a full subcategory. Suppose that every functor $F_0 : \mathcal{C}^0 \to \mathcal{D}$ over $\mathcal{D}'$ admits a p-left Kan extension(4.7.3.13), then the restriction

$$i^* : \mathrm{Func}_{\mathcal{D}'}(\mathcal{C}, \mathcal{D}) \to \mathrm{Func}_{\mathcal{D}'}(\mathcal{C}^0, \mathcal{D})$$

admits a section $i_!$ whose essential image are exactly those F which are p-left Kan extension of $F|_{\mathcal{C}^0}$. Any such $i_!$ is called the **left Kan extension functor**. Moreover, this $i_!$ is left adjoint to i^*:

$$i^* : \mathrm{Func}_{\mathcal{D}'}(\mathcal{C}, \mathcal{D}) \rightleftarrows \mathrm{Func}_{\mathcal{D}'}(\mathcal{C}^0, \mathcal{D}) : i_!$$

⌟

Proof: Cf.[Lur09]P284. □

4 Adjunctions

Correspondences

Def. (4.7.4.1) [Correspondence]. Let $\mathcal{C}, \mathcal{D}$ be ∞-categories, an **correspondence** between $\mathcal{C}, \mathcal{D}$ is defined to be an ∞-category $\mathcal{M}$ and a map $\mathcal{M} \to \Delta^1$ s.t. $\mathcal{C} \cong \mathcal{M}_0$ and $\mathcal{D} \cong \mathcal{M}_1$. ⌟

Adjunctions

Def. (4.7.4.2) [Adjunctions]. An **adjunction** between ∞-categories $\mathcal{C}, \mathcal{D} \in \mathcal{C}\mathrm{at}_\infty$ is a map $q : \mathcal{M} \to \Delta^1 \in s\mathcal{S}\mathrm{et}$ that is both Cartesian fibration and coCartesian fibration, together with equivalences $\mathcal{M}_{\{0\}} \cong \mathcal{C}, \mathcal{M}_{\{1\}} \cong \mathcal{D}$.

If $\mathcal{M} \to \Delta^1$ is an adjunction and $f : \mathcal{C} \to \mathcal{D}, g : \mathcal{D} \to \mathcal{C}$ are the associated functors, then f is said to be **left adjoint** to g and g is said to be **right adjoint** to f. ⌟

Def. (4.7.4.3) [Unit Transformations]. For a pair of functors $f : \mathcal{C} \to \mathcal{D}, g : \mathcal{D} \to \mathcal{C}$ between ∞-categories, a **unit transformation** for (f, g) is a morphism $u : \mathrm{id} \to g \circ f \in \mathrm{Func}(\mathcal{C}, \mathcal{C})$ s.t. for any $C \in \mathcal{C}, D \in \mathcal{D}$, the composition

$$\mathrm{Map}_{\mathcal{D}}(f(C), D) \xrightarrow{g} \mathrm{Map}_{\mathcal{C}}(gf(C), g(D)) \xrightarrow{u(C)} \mathrm{Map}_{\mathcal{C}}(C, g(D))$$

is a homotopy equivalence. ⌟

Prop. (4.7.4.4) [Unit Transformations and Adjunctions]. For a pair of functors $f : \mathcal{C} \to \mathcal{D}, g : \mathcal{D} \to \mathcal{C}$, f is left adjoint to g iff there is a unit transformation $u : \mathrm{id} \to g \circ f$. ⌟

Proof: Cf.[Lur09]P339. □

Prop. (4.7.4.5)[Adjunction and Limits]. Left adjoints between ∞-categories preserve small colimits and right adjoints between ∞-categories preserves small limits. ⌟

Proof: Cf.[Lur09]P345. □

Localizations

Def. (4.7.4.6) [Localization of ∞-Categories]. A functor $\mathcal{C} \to \mathcal{D} \in \mathcal{C}\mathrm{at}_\infty$ is called a **localization of ∞-category** if it admits a fully faithful right adjoint. ⌟

5 Presentable ∞-Categories

∞-Categories of Presheaves

Def. (4.7.5.1) [∞-Category of Presheaves]. For $S \in s\,\mathcal{S}\mathrm{et}$, there exists an ∞-category $\mathcal{PS}\mathrm{h}_\infty^{\mathcal{S}\mathrm{et}}(S) = \mathrm{Func}(S^{\mathrm{op}}, \mathcal{S}) \subset \mathcal{C}\mathrm{at}_\infty$ by(4.7.1.13), called the **∞-category of presheaves on** S. More generally, for any $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$, $\mathcal{PS}\mathrm{h}_\infty^{\mathcal{S}\mathrm{et}}(S; \mathcal{C}) = \mathrm{Func}(S^{\mathrm{op}}, \mathcal{C})$ is called the **∞-category of $\mathcal{C}$-valued presheaves on** S. ⌟

Prop. (4.7.5.2) [Cocompleteness]. For $S \in s\,\mathcal{S}\mathrm{et}$ and $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$ that is cocomplete, then $\mathcal{PS}\mathrm{h}(S; \mathcal{C})$ is also cocomplete by(4.7.3.12). In particular, $\mathcal{PS}\mathrm{h}_\infty^{\mathcal{S}\mathrm{et}}(S)$ is cocomplete. ⌟

Def. (4.7.5.3) [Yoneda Embedding]. For $K \in s\,\mathcal{S}\mathrm{et}$, let $\mathcal{C} = \mathfrak{C}[K]$, then the mapping space construction defines a map

$$\mathcal{C}^{\mathrm{op}} \times \mathcal{C} \to \mathrm{Kan} : (X, Y) \mapsto \mathrm{Sing}\,|\,\mathrm{Map}_{\mathcal{C}}(X, Y)|$$

by(4.6.3.43). And there is a natural map $\mathfrak{C}[K^{\mathrm{op}} \times K] \to \mathcal{C}^{\mathrm{op}} \times \mathcal{C}$, so we have a map

$$\mathfrak{C}[K^{\mathrm{op}} \times K] \to \mathrm{Kan}$$

which corresponds to a map

$$K^{\mathrm{op}} \times K \to N_\Delta(\mathrm{Kan}) = \mathcal{G}\mathrm{rpd}_\infty\,.$$

and induces a map

$$よ_\Delta : K \mapsto \mathrm{Func}(K^{\mathrm{op}}, \mathcal{G}\mathrm{rpd}_\infty) = \mathcal{PS}\mathrm{h}_\infty^{\mathcal{S}\mathrm{et}}(K),$$

When $\mathcal{C} \in \mathcal{C}\mathrm{at}$ and $K = N(\mathcal{C})$ this is compatible with the usual Yoneda embedding composed with simplicial enhencement, so it is called the the **Yoneda embedding**. ⌟

Prop. (4.7.5.4) [∞-Categorical Yoneda Lemma]. For $K \in s\,\mathcal{S}\mathrm{et}$, the Yoneda embedding(4.7.5.3) $よ : K \to \mathcal{PS}\mathrm{h}_\infty^{\mathcal{S}\mathrm{et}}(K)$ is fully faithful. ⌟

Proof: Cf.[Lur09]P316. □

Prop. (4.7.5.5). let $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$, then $よ_\Delta : \mathcal{C} \to \mathcal{PS}\mathrm{h}_\infty^{\mathcal{S}\mathrm{et}}(\mathcal{C})$ preserves all small limits. ⌟

Proof: Cf.[Lur09]P316. □

Lemma (4.7.5.6). Let $S \in s\,\mathcal{S}\mathrm{et}$, and $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$, then

- Any functor $F : \mathcal{PS}\mathrm{h}_\infty^{\mathcal{S}\mathrm{et}}(S) \to \mathcal{C}$ is a left Kan extension of $f|_S$ iff f preserves all small colimits.
- If $\mathcal{C}$ is cocomplete, then any functor $S \to \mathcal{C}$ has a left Kan extension $\mathcal{PS}\mathrm{h}_\infty^{\mathcal{S}\mathrm{et}}(S) \to \mathcal{C}$.

⌟

Proof: Cf.[Lur09]P322. □

Thm. (4.7.5.7) [∞-Categorical Yoneda Extensions]. Let $S \in s\,\mathcal{S}\mathrm{et}$ and $\mathcal{C}$ be a cocomplete ∞-category, the Yoneda embedding $よ_\Delta : S \to \mathcal{PS}\mathrm{h}_\infty^{\mathcal{S}\mathrm{et}}(S)$ induces an equivalence of ∞-categories

$$\mathrm{Func}^L(\mathcal{PS}\mathrm{h}_\infty^{\mathcal{S}\mathrm{et}}(S), \mathcal{C}) \cong \mathrm{Func}(S, \mathcal{C}).$$

⌟

Proof: This follows from(4.7.3.17) and(4.7.5.6). □

Cor. (4.7.5.8). For $S \in s\mathcal{S}\mathrm{et}$, $\mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}_\infty(S)$ is generated by S under small colimits. In particular, $\mathcal{G}\mathrm{rpd}_\infty$ is generated by Δ^0 under small colimits. ⌟

Proof: If $\mathcal{C} \subset \mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}_\infty(S)$ is a strictly full subcategory stable under small colimits containing $よ_\Delta(S)$, then $\mathcal{C}$ is cocomplete by(4.7.5.2), and then $よ_\Delta : S \to \mathcal{C}$ is of the form $F \circ よ_\Delta$ by(4.7.5.7) where $F : \mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}_\infty(S) \to \mathcal{C}$ preserves small colimits. Then we can regard F as a self-map of $\mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}_\infty(S)$ that is identity on $\mathrm{id} : S \to S$. Thus by(4.7.5.7) again, F is equivalent to id_S. Thus every object of $\mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}_\infty(S)$ is equivalent some elements in $\mathcal{C}$, so $\mathcal{C} = \mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}_\infty(S)$. □

Accessible ∞-Categories

Presentable ∞-Categories

Def. (4.7.5.9) [Presentable ∞-Category]. An ∞-category is called a **presentable ∞-category** if it is accessible and cocomplete. ⌟

Prop. (4.7.5.10) [Simpson]. For $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$ is presentable iff it is an accessible reflective localization**?** of an $\mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}_\infty(\mathcal{D})$ for some $\mathcal{D} \in \mathcal{C}\mathrm{at}_\infty$. ⌟

Proof: Cf.[HTT, P5.5.1.1]. □

Prop. (4.7.5.11). A presentable ∞-category is complete. ⌟

Proof: Cf.[HTT, P5.5.2.4]. □

Prop. (4.7.5.12) [Presentable ∞-Categories as Simplicial Model Categories]. $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$ is presentable iff it is equivalent to the underlying category $N_\Delta(\mathcal{M}_{cf})$ for some combinatorial simplicial model category $\mathcal{M}$. ⌟

Proof: □

Thm. (4.7.5.13) [Adjoint Functor Theorem]. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor between presentable ∞-categories, then

- F admits a right adjoint iff it preserves small colimits.
- F admits a left adjoint iff it preserves small limits and κ-filtered colimits for some regular cardinal κ.

⌟

Proof: [HTT. 5.5.2.9]. □

Compactly Generated ∞-Categories

Def. (4.7.5.14). ⌟

6 ∞-Topoi

7 Topological Cyclic Homology(Scholze)

4.8 Abelian Categories and Triangulated Categories

References are [Sta], [Ver96] and [G-M03].

1 Additive Categories

Def. (4.8.1.1) [Preadditive Categories]. a **preadditive category** is a category A that satisfies:

- **A1**: $\mathcal{A}$ is enriched over the Cartesian category of Abelian groups.

⌟

Def. (4.8.1.2) [Zero Element]. Let $\mathcal{A}$ be a preadditive category and $x \in \mathcal{A}$, then the following are equivalent:

- x is initial.
- x is final.
- $\mathrm{id}_x = 0 \in \mathrm{Mor}(x, x)$.

Such an element is called a **zero element** in $\mathcal{A}$, denoted by 0. If 0 exists, then a morphism $\alpha : x \to y$ factors through 0 iff $\alpha = 0$. ⌟

Proof: Cf.[Sta]00ZZ. □

Cor. (4.8.1.3). An additive functor transforms a zero object to a zero object. ⌟

Prop. (4.8.1.4) [Finite Direct Sums]. If $\mathcal{A}$ is a preadditive category and $x, y \in \mathcal{A}$. If one of $x \times y$ and $x \coprod y$ exists, then so does the other, and they are isomorphic, called the **direct sum** of x, y. ⌟

Proof: Cf.[Sta]0101. □

Def. (4.8.1.5) [Additive Functors]. A functor between preadditive categories $F : \mathcal{C} \to \mathcal{D}$ is called an **additive functor** if it is a morphism of $\mathcal{A}b$-enriched categories. ⌟

Def. (4.8.1.6) [Kernels, Cokernels, Images and Coimages]. Let $\mathcal{A}$ be a preadditive category and $f : X \to Y$ is a map, then

- the **kernel** of f is the fiber product $\begin{array}{ccc} \ker(f) & \longrightarrow & X \\ \downarrow & & \downarrow f \\ 0 & \longrightarrow & Y \end{array}$.
- the **cokernel** of f is the fiber pushforward $\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Coker}(f) \end{array}$.
- the **image** of f is the cokernel of the kernel.
- the **coimage** of f is the kernel of the cokernel.

⌟

Cor. (4.8.1.7). If they exist, then kernel and coimage are monomorphisms, and cokernel and image are epimorphisms, by general non-sense. ⌟

Prop. (4.8.1.8). If the image and coimage of f exist, then there is a natural decomposition $f : X \to \mathrm{Im}(f) \to \mathrm{Coim}(f) \to Y$, by the universal property. ⌟

Def. (4.8.1.9) [Exact Sequence]. A diagram $X \xrightarrow{f} Y \xrightarrow{g} Z$ is an **exact sequence** if f is the kernel of g and g is the cokernel of f. ⌟

Additive Categories

Def. (4.8.1.10) [Additive Categories]. A preadditive category $\mathcal{A}$ is called an **additive category** iff moreover it satisfies

- **A2**:There exists an element that is both initial and final, called the **zero element**.
- **A3**: $\mathcal{A}$ admits finite sums and finite products, and they are equal. Also, the sum induce the Abelian structure of $\mathrm{Hom}(X, Y)$.

We use the symbol $\mathcal{A} \in \mathcal{A}dd\,\mathcal{C}at$ to mean that $\mathcal{A}$ is an additive category. ⌟

Prop. (4.8.1.11) [Characterizing Direct Sum Decompositions]. If $\mathcal{A}$ is a preadditive category with zero object, $x, y, z \in \mathcal{A}$, then z is the product and sum of x, y in $\mathcal{A}$ iff there are four morphism that satisfies some identities. ⌟

Proof: Cf.[Sta]0102. □

Cor. (4.8.1.12). An additive functor between additive categories transforms finite direct sums to direct sums. ⌟

Def. (4.8.1.13) [Kernel of an Additive Functor]. The **kernel of an additive functor**(4.8.1.5) between additive categories is is the full subcategory of objects that are mapped to 0. ⌟

Def. (4.8.1.14) [Compact Object]. Let $\mathcal{D}$ be an additive category with arbitrary direct sums, then a **compact object** $K \in \mathcal{D}$ is an object that

$$\bigoplus_i \mathrm{Hom}(K, E_i) \to \mathrm{Hom}(K, \bigoplus_i E_i)$$

is bijective for any set I and objects $E_i \in \mathcal{D}$. ⌟

Karoubian Categories

Def. (4.8.1.15) [Karoubian Categories]. A **Karoubian category** is an additive category(4.8.1.10) $\mathcal{A}$ that satisfies the following equivalent conditions:

- Every idempotented endomorphism of an object of $\mathcal{A}$ has a kernel.
- Every idempotented endomorphism of an object of $\mathcal{A}$ has a cokernel.
- Every idempotented endomorphism $p : z \to z$ induces a direct sum decomposition $z = x \oplus y$(exists by A3) that p corresponds to the projection $z \to x$.

⌟

Proof: $1 \to 3$: Let $p : z \to z$ be an idempotent, let $x = \ker(p), y = \ker(1 - p)$, then there are maps $x \to z, y \to z$. Then $p : z \to z$ factors through $z \to y \to z$. Similarly $(1 - p) : z \to z$ factors through $z \to x \to z$. Then it can be verified that $z = x \oplus y$ is a direct sum decomposition(4.8.1.11).

$2 \to 3$ is dual.

$3 \to 1, 3 \to 2$ are easy by(4.8.1.11). □

Prop. (4.8.1.16). Let $\mathcal{D}$ be a preadditive category,

- if $\mathcal{A}$ has countable products and kernels of morphisms that have a right inverse, then $\mathcal{A}$ is Karoubian.
- Dually, if $\mathcal{A}$ has countable coproducts and cokernels of morphisms that have a left inverse, then $\mathcal{A}$ is Karoubian.

⌟

Proof: Given any idempotented morphism $e : X \to X$, e has a kernel iff $W \mapsto \ker(\mathrm{Mor}(M,X) \xrightarrow{e} \mathrm{Mor}(M,X))$ is representable. Notice that for any Abelian group A,

$$\ker(e : A \to A) = \ker(\Phi : \prod_{\mathbb{Z}} A \to \prod_{\mathbb{Z}} A)$$

where

$$\Phi(a_1, a_2, \ldots) = (ea_1 + (1-e)a_2, ea_2 + (1-e)a_3, \ldots)$$

and it has a right inverse

$$\Psi(a_1, a_2, \ldots) = (a_1, (1-e)a_1 + ea_2, (1-e)a_2 + ea_3, \ldots)$$

thus the kernel exists. □

Coherent Functors

Def. (4.8.1.17) [Coherent Functors]. For $\mathcal{A} \in \mathcal{A}\mathrm{dd}\,\mathcal{C}\mathrm{at}$, a **coherent functor** on $\mathcal{A}$ is a functor $F \in \mathcal{PS}\mathrm{h}(\mathcal{A})$ s.t. there exists a morphism $s \to t \in \mathcal{A}$ and F is the cokernel of the map $よ(s) \to よ(t)$.

Then the class of coherent functors on $\mathcal{A}$ form an additive category with cokernels, denoted by $\mathcal{C}\mathrm{oh}(\mathcal{A})$. ⌟

Proof: Cf.[Neeman, Triangulated Categories]. □

Prop. (4.8.1.18). Any additive functor between additive categories $f : \mathcal{A} \to \mathcal{B}$ extends via Yoneda map $よ$ to a right exact functor $f^* : \mathcal{C}\mathrm{oh}(\mathcal{A}) \to \mathcal{C}\mathrm{oh}(\mathcal{B})$. ⌟

2 Exact Categories

Main references are [Exact categories, Theo].

Def. (4.8.2.1) [Exact Categories]. Let $\mathcal{C}$ be an small additive category and $\mathcal{E}$ be a set of short sequences

$$0 \to X \to Y \to Z \to 0$$

in $\mathcal{C}$. If $0 \to X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \to 0$ is in $\mathcal{E}$, then we call φ an **admissible monomorphism** and ψ an **admissible epimorphism**. then $(\mathcal{C}, \mathcal{E})$ is called an **exact category** if it satisfies:

- **Ex1**: For any complex $0 \to X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \to 0$ in $\mathcal{E}$, φ is the kernel of ψ and ψ is the cokernel of φ.
- **Ex2**: For any $X, Y \in \mathcal{C}$, $0 \to X \to X \oplus Y \to Y \to 0$ is in $\mathcal{E}$.
- **Ex3**: $\mathcal{E}$ is closed under isomorphisms.
- **Ex4**: if f, g are admissible monomorphisms, then so is gf.
- **Ex5**: If f is an admissible monomorphism, then any pushout of f exists and is an admissible monomorphism.
- **Ex6**: If g is an admissible epimorphism, then any pullback of g exists and is an admissible epimorphism.

⌟

Cor. (4.8.2.2). If $\mathcal{C}$ is an Abelian category and $\mathcal{E}$ the set of all exact sequences in $\mathcal{C}$, then $(\mathcal{C},\mathcal{E})$ is an exact category. ⌟

Cor. (4.8.2.3). If $(\mathcal{C},\mathcal{E})$ is an exact category, then

- **Ex7**: if $f: X\to Y\in\mathcal{C}$ is a morphism having a kernel and there is a morphism $g: Z\to X$ that fg is an admissible monomorphism, then so is f. Dual argument holds for admissible epimorphisms.

⌟

Proof: Cf.[Bernhard Keller, Chain complexes and stable categories, P28].? □

Def. (4.8.2.4) [Geometric Exact Categories]. A **geometric exact category** consists of an exact category $(\mathcal{C},\mathcal{E})$ and a mapping A from $\mathrm{Ob}(\mathcal{C})$ to $\mathcal{S}\mathrm{et}$ together with morphisms:

- a morphism $f^*: A(X)\to A(Y)$ for any admissible monomorphism $f: X\to Y$.
- a morphism $g_*: A(X)\to A(Z)$ for any admissible epimorphism $g: X\to Z$.

that satisfies the following axioms:

- **A1**: $A(0)=\mathrm{pt}$.
- **A2**: If i,j are admissible monomorphisms, then $(ji)^*=i^*j^*$.
- **A3**: If p,q are admissible epimorphisms, then $(qp)_*=q_*p_*$.
- **A4**: $\mathrm{id}_X^*=(\mathrm{id}_X)_*=\mathrm{id}_{A(X)}$.
- **A5**: If $f: X\to Y$ is an isomorphism, then $f^*f_*=f_*f^*=\mathrm{id}$.
- **A6**: For any Cartesian and Cocartesian diagram $\begin{array}{ccc} X & \xrightarrow{u} & Y \\ \downarrow p & & \downarrow q \\ Z & \xrightarrow{v} & W \end{array}$, if u is admissible monomorphism or q is admissible epimorphism, then $v^*q_*=p_*u^*$.
- **A7**: If $X\xrightarrow{u} Y\xrightarrow{v} Z$ is a diagram in $\mathcal{C}$ that u is an admissible epimorphism and v is an admissible monomorphism, and if $h_X\in A(X), h_Z\in A(Z)$ satisfy $u_*(h_X)=v^*(h_Z)$, then there exists $h\in A(X\oplus Z)$ that $(\mathrm{id},vu)^*(h)=h_X$ and $\pi_{2*}(h)=h_Z$. (Notice (id,vu) is an admissible monomorphism because it is composition of $X\to X\oplus Z$ with the isomorphism $(\pi_1, vu\pi_1+\pi_2): X\oplus Z\to X\oplus Z$.

For any $X\in\mathcal{C}$, an element of $A(X)$ is called a **geometric structure** on X.

Exact categories can be viewed as geometric exact categories by asserting $A(X)=\mathrm{pt}$ for all $X\in\mathcal{C}$. ⌟

Def. (4.8.2.5) [Morphisms compatible with the Geometric Structure]. Let $(\mathcal{C},\mathcal{E},A)$ be a geometric exact category, if $(X',h'),(X'',h'')$ are two geometric objects, then a morphism $f: X'\to X''$ is said to be a **morphism compatible with the geometric structure** if there exists a geometric object (X,h) and an admissible monomorphisms $u: X'\to X$ and an admissible epimorphism $v: X\to X''$ that $h'=u^*(h)$ and $h''=v_*(h)$ and $f=vu$.

The composition of two morphisms compatible with the geometric structure is also a morphism compatible with the geometric structure.

We denote $\mathcal{C}_A$ the category of geometric objects of $\mathcal{C}$, and $\mathcal{E}_A$ the set of diagrams of geometric objects $0\to X'\xrightarrow{u} X\xrightarrow{v} X''\to 0$ that the underlying diagram is in $\mathcal{E}$ and u,v are compatible with the geometric structures. ⌟

Prop. (4.8.2.6) [Hermitian Spaces]. The f.d. Hermitian spaces over $\mathbb{C}$ or f.d. normed vector spaces over $\mathbb{R}$ form a geometric exact category. ⌟

Proof: Cf.[Harder-Narasimhan Categories, P4]. □

Prop. (4.8.2.7) [F.D. Ultranormed Banach Spaces]. Let K be a complete valued field, then the category of f.d. ultranormed Banach spaces over K(14.2.4.5) is a geometric exact category. ⌟

Proof: It suffices to check axiom A7, but vu has norm≤ 1, and for any $\varphi : E \to F$ of norm≤ 1, we can endow $E \oplus F$ with the maximum norm, then in the decomposition $E \xrightarrow{(\mathrm{id},\varphi)} E \oplus F \xrightarrow{\pi_2} F$, we have $(\mathrm{id}, \varphi)^*(h) = h_E$ and $(\pi_2)_*(h) = h_F$. □

Prop. (4.8.2.8) [Filtrations in an Abelian Category]. The filtrations(4.3.3.1) in an Abelian category form a geometric exact category. ⌟

Proof: Cf.[Harder-Narasimhan Categories, P5]. □

3 Abelian Categories

Def. (4.8.3.1) [Abelian Categories]. An **Abelian category** $\mathcal{A}$ is an additive category(4.8.1.10) that satisfies the follows axiom:

- **A4**: $\mathcal{A}$ admits kernels and cokernels, and for any morphism $f \in \mathcal{A}$, the natural map $\mathrm{Im}(f) \to \mathrm{Coim}(f)$ are isomorphisms.

We use the symbol $\mathcal{A} \in \mathcal{A}b\,\mathcal{C}at$ to mean that $\mathcal{A}$ is an Abelian category. ⌟

Remark (4.8.3.2). WARNING: An additive category that epimorphism+monomorphism is isomorphism need not be an Abelian category. Cf.[https://mathoverflow.net/questions/41722/is-every-balanced-pre-abelian-category-abelian] for a counter-example. ⌟

Prop. (4.8.3.3). In an Abelian category, the functor $X \mapsto \mathrm{Hom}(X, Y)$ and $X \mapsto \mathrm{Hom}(Y, X)$ is both left exact.(Note that left and right is seen on the image). ⌟

Def. (4.8.3.4) [Injectives and Surjectives]. A morphism f is an Abelian category $\mathcal{A}$ is called an **injection** if $\ker f = 0$. It is called a **surjection** if $\mathrm{Coker}\, f = 0$. f is an injection iff it is a monomorphism, it is a surjection iff it is an epimorphism. ⌟

Prop. (4.8.3.5). Axiom A3 asserts the good existence of product and sum of objects as we wanted, and it can be used to prove that monomorphism and epimorphism are stable under pushout and pullback.

But this uses $A4$ strongly, Cf.[MacLane Categories for working mathematicians P203]. (For epimorphism, first prove $0 \to X \times_U Y \to X \times Y \to U \to 0$ is exact when $X \to U$ is epi). ⌟

Prop. (4.8.3.6). equalizer and finite product derives finite limit, thus finite limits and finite colimits exists in Abelian categories. ⌟

Prop. (4.8.3.7)[Mitchell's embedding theorem]. If $\mathcal{A} \in \mathcal{A}b\,\mathcal{C}at$ is small, then there exists $R \in \mathcal{R}ing$, not necessary commutative and a fully faithful and exact functor $\mathcal{A} \to \mathcal{M}od_R$ that preserves kernel and cokernel. WARNING: it may not preserve sum and product, let alone limits and colimits. ⌟

Proof: □

Prop. (4.8.3.8). If $\mathcal{A} \in \mathcal{A}b\,\mathcal{C}at$ and $\mathcal{C} \in \mathcal{C}at$, then $\mathcal{H}om(\mathcal{C}, \mathcal{A})$ is an Abelian category. In particular, $\mathrm{Ch}^{\mathbb{Z}}(\mathcal{A})$ is Abelian(4.8.6.1). ⌟

Localization

Prop. (4.8.3.9) [Localization Category]. If $\mathcal{C}$ is a preadditive category and S is a left or right localizing system of $\mathcal{C}$, then there exists a natural additive structure on $\mathcal{S}^{-1}\mathcal{C}$ and a localizing functor $\mathcal{C} \to S^{-1}\mathcal{C}$ that is additive. ⌟

Proof: Cf.[Sta]05QD. □

Lemma (4.8.3.10). If $\mathcal{C}$ is additive and S is localizing, let X be an element of $\mathcal{C}$, then: $Q(X) = 0$ iff there is a morphism $0 : X \to Y$ that is an element of S iff there is a morphism $0 : Z \to X$ that is an element of S iff there is a morphism $0 : Z \to X$ that is an element of S ⌟

Proof: If such $0 : X \to Y \in S$, then it maps to isomorphisms in $S^{-1}(\mathcal{C})$ by(4.1.1.58), so $Q(X) = 0$. If $Q(X) = 0$, then the morphism $0 \to X$ is mapped to an isomorphism, so by(4.1.1.60), there are g, h that $fg = hf = 0$, so $Z \to 0 \to X \in S$. Dually for the other direction. □

Prop. (4.8.3.11) [Localized Abelian Categories]. If $\mathcal{A}$ is Abelian and S is localizing, then $S^{-1}\mathcal{A}$ is an Abelian category and $\mathcal{A} \to S^{-1}\mathcal{A}$ is exact. ⌟

Proof: By(4.1.1.58) and its dual, $\mathcal{A} \to S^{-1}\mathcal{A}$ preserves finite limits and colimits. □

Serre Subcategory

Def. (4.8.3.12) [Serre Subcategories]. A **Serre subcategory** of an Abelian category is a non-empty full subcategory $\mathcal{C}$ that if

$$A \to B \to C$$

is exact and $A, C \in \mathrm{Ob}(\mathcal{C})$, then $B \in \mathrm{Ob}(C)$.

A **weak Serre subcategory** of an Abelian category is a non-empty full subcategory $\mathcal{C}$ that if

$$A \to B \to C \to D \to E$$

is exact and $A, B, D, E \in \mathcal{C}$, then $C \in \mathcal{C}$. ⌟

Prop. (4.8.3.13).

- A Serre category is equivalent to a full subcategory $\mathcal{A}$ that contains 0, all the subobjects and quotient objects of $\mathcal{A}$, and extensions of objects of $\mathcal{A}$ are in $\mathcal{A}$.
- A weak Serre category is equivalent to a full subcategory $\mathcal{A}$ that contains 0, and all the kernels, cokernels between objects in $\mathcal{A}$, and all the extensions of objects in $\mathcal{A}$.

In these cases, $\mathcal{A}$ is an Abelian category and the functor $i : \mathcal{A} \to \mathcal{C}$ is exact. ⌟

Proof: One direction of these two are trivial, it suffices to prove the converse. For the first, $0 \to \mathrm{Im}\, A \to B \to \mathrm{Im}\, B \to 0$, so $B \in \mathcal{C}$. For the second, $0 \to \mathrm{Coker}(A \to B) \to C \to \ker(D \to E) \to 0$, so $C \in \mathcal{C}$. □

Prop. (4.8.3.14) [Quotients by Serre Subcategory]. For an exact functor F between Abelian categories, the kernel of F is a Serre subcategory. And any Serre subcategory is the kernel of an essentially surjective exact functor $Q : \mathcal{A} \to \mathcal{A}/\mathcal{C}$, and this functor satisfies the universal property that any exact functor between Abelian categories $F : \mathcal{A} \to \mathcal{C}$ that $\mathcal{C} \subset \ker(F)$ factors uniquely through $\mathcal{A}/\mathcal{C}$. ⌟

Proof: The full subcategory of $\ker(F)$ is clearly a Serre subcategory by checking the definition. Conversely, consider S =all the morphisms that has kernel and cokernel in $\mathcal{C}$, first we prove it is a localizing system(4.1.1.54).

The long exact seuqence(4.8.7.4) shows that if $f, g \in S$, then $gf \in S$. For other verifications, Cf.[Sta]02MS?.

Next we construct $\mathcal{C}/\mathcal{A}$ as $S^{-1}\mathcal{C}$. Consider which objects are mapped to 0 in $\mathcal{C}/\mathcal{A}$, use(4.8.3.10) and consider the kernel and cokernel, it is easy to see that $\ker(Q) = \mathcal{C}$. If another category $\mathcal{D}$ and $F : \mathcal{C} \to \mathcal{D}$ satisfies $\mathcal{C}$ is mapped to0, then it is clear that elements in S is mapped to isomorphism, so it factors through $\mathcal{C}/\mathcal{A}$ by universal property(4.1.1.58). □

Prop. (4.8.3.15) [K_0 **Group of Serre Subcategory**]. Let $\mathcal{A}$ be an Abelian category and $\mathcal{C}$ a Serre subcategory, with $\mathcal{A}/\mathcal{C} = \mathcal{B}$(4.8.3.14). Then

- The exact functors $\mathcal{C} \to \mathcal{A} \to \mathcal{B}$ induces an exact sequence
$$K_0(\mathcal{C}) \to K_0(\mathcal{A}) \to K_0(\mathcal{B}) \to 0,$$
- The kernel of $K_0(\mathcal{C}) \to K_0(\mathcal{A})$ is generated by elements of the form
$$[\ker(\psi)/\operatorname{Im}(\varphi)] - [\ker(\varphi)/\operatorname{Im}(\psi)]$$
where $\varphi, \psi : M \to M$ are pairs of maps that $\varphi \circ \psi = \psi \circ \varphi = 0$.

⌟

Proof: Cf.[Sta]02MX. □

Artinian Abelian Categories

Def. (4.8.3.16) [Artinian Abelian Categories]. An **Artinian Abelian category** is an Abelian category that

- $\operatorname{Hom}(A, B)$ are all f.d. vector spaces over k.
- Then length of any filtrations $0 = X_0 \subset X_1 \subset \ldots \subset X_l = X$ for any object X is bounded. The maximal length is called the **length** of X.

⌟

Prop. (4.8.3.17)[Jordan-Holder]. Let $\mathcal{C}$ be an Artinian category, then any maximal length filtration of an element X has the same length, and the set of quotients X_{k+1}/X_k is the same, up to order. ⌟

Proof: □

Others

Def. (4.8.3.18)[Essential Morphism]. In an Abelian category, an injection $A \to B$ is called **essential** iff every non-zero subobject of B intersects A. A surjection is called **essential** iff every proper subobject of A is not mapped to B. ⌟

Def. (4.8.3.19) [Noetherian Abelian Category]. In a Grothendieck Abelian category $\mathcal{A}$, an object M is called **finitely generated** if for every ascending chain
$$M_1 \subset M_2 \subset \ldots \subset M$$
with $\cup_i M_i = M$, we have $M_i = M$ for some i.

$\mathcal{A}$ is called **Noetherian** iff a subobject of a f.g. object is f.g.. $\mathcal{A}$ is called **Artinian** iff every f.g. object has finite length?. ⌟

Grothendieck Abelian Category

Main references are [Rings of Quotients]

Def. (4.8.3.20) [Grothendieck Abelian Category]. A **Grothendieck Abelian category** is an Abelian category $\mathcal{A}$ satisfying the following axioms:

AB3: It is a locally small cocomplete Abelian category.

AB5: Small filtered colimits are exact. This is equivalent to { for any family of subobjects $\{A_i\}$ of A to B indexed by inclusion can induce a morphism $\sum A_i \to B$ (internal sum)}**?**

GEN: It has a **generator**, which is an object $U \in \mathcal{A}$ s.t. for any proper subobject $N \subsetneq M$, there is a map $U \to M$ that doesn't factor through N.

⌟

Def. (4.8.3.21) [Further Grothendieck Axioms]. For a Grothendieck Abelian category $\mathcal{A}$, we can also formulate the following axioms:

AB4: Arbitrary direct sums are exact.

AB6: For any index set J and filtered categories $I_j, j \in J$ and diagrams indexed over I_j, the natural map

$$\varinjlim_{i_j \in I_j} \prod_{j \in J} M_{i_j} \to \prod_{j \in J} \varinjlim_{i_j \in I_j} M_{i_j}$$

is an isomorphism.

Dual Axioms: Axioms with an * meaning that the dual category satisfies something.

⌟

Prop. (4.8.3.22). If $\mathcal{A}$ is a Grothendieck Abelian category, then so is $\mathcal{PSh}^{\mathcal{Set}}(\mathcal{A})$. ⌟

Proof: For the presheaf, the only problem is the existence of generator, for that, just construct a family of presheaves and sum them. Take $Z_X = i_{f_X}(U)$, where U is the generator of $\mathcal{A}$ and $f = \mathrm{pt} \to \mathcal{A}^C : \mathrm{pt} \to U$. Then $F(X) = \mathrm{Hom}(Z_X, F)$ by adjointness(6.1.2.9). So they are a family of generators. □

Prop. (4.8.3.23). Any Grothendieck Abelian category has a functorial injective embedding. ⌟

Proof: Cf.[Sta]079H.**?** □

Prop. (4.8.3.24) [Representability on Grothendieck Category]. A contravariant functor from a Grothendieck category to $\mathcal{S}et$ is representable iff it takes colimits to limits. ⌟

Proof: $M \oplus M \to M$ with induce a map $F(M) \times F(M) \to F(M)$ thus $F(M)$ is a semigroup, and the inverse of id_Min $\mathrm{Hom}(M, M)$ maps to a $F(M) \to F(M)$ which is the inverse, Thus in fact F is a left adjoint functor to $\mathcal{A}b$.

Let U be a generator, $A = \sum_{s \in F(U)} U$, let $s_{univ} = (s) \in F(A) = \prod_{s \in F(U)} F(U)$. let A' be the largest objects that s_{univ} restrics to 0 in A', let $\overline{s}_{univ}$ be in $F(A/A')$ that maps to s_{univ} in $F(A)$ (because F is left exact). Then we claim $(A/A', \overline{s}_{univ})$ represents F. Cf.[Sta]07D7.**?** □

Cor. (4.8.3.25) [Grothendieck Categories are Cocomplete]. Any Grothendieck category satisfies AB3*. ⌟

Proof: It suffices to show that small direct products exist. And this is because $F = \prod_i \mathrm{Hom}(-, M_i)$ commutes with colimits. □

Prop. (4.8.3.26) [Grothendieck Categories are Locally Presentable]. Any Grothendieck category is locally presentable. In fact, for an Abelian category with exact filtered colimits, it is a Grothendieck Abelian category iff it is locally presentable. ⌟

Proof: Cf.[Colimits and homological algebra, Krause]Cor5.2.**?** □

Cor. (4.8.3.27). If $F : \mathcal{C}^{op} \to \mathcal{S}et$ commutes with small colimits, then F is a left adjoint. ⌟

Proof: **?** □

Examples of Grothendieck Category

Prop. (4.8.3.28) [Modules]. For $R \in \mathcal{A}lg$, $\mathcal{M}od_R$ is a Grothendieck Abelian category. More generally, for $R, S \in \mathcal{A}lg$, $\mathcal{M}od_{R-S} = \mathcal{M}od_{R\otimes S^{op}}$ is a Grothendieck Abelian category. ⌟

Proof: This is clear, by(5.1.1.25). □

Prop. (4.8.3.29) [Sheaf of Modules]. $\mathcal{S}h(\mathcal{O})$ for a ringed site $(\mathcal{C}, \mathcal{O})$ is a Grothendieck Abelian category. ⌟

Proof: It is obviously an Abelian category and have filtered colimits as presheaves, which are exact because colimits in the category of Abelian groups are exact, and for a family of generators, take $j_!\mathcal{O}_U$ as the representative for $\Gamma(U, -)$, which is the sheaf associated to the sheaf Z_U in the proof of(4.8.3.22). □

Cor. (4.8.3.30). Let $\mathcal{C}$ be a site, the categories $\mathcal{PS}h(\mathcal{C})$ and $\mathcal{S}h(\mathcal{C})$ are Grothendieck Abelian categories. ⌟

Proof: For the presheaf, C.f(4.8.3.22). For the sheaf, it follows from (4.8.3.29). □

Remark (4.8.3.31). The category of Abelian sheaves doesn't satisfy AB4*, i.e. not every limit of epimorphisms is epimorphism. ⌟

Proof: Consider the constant sheaf $\prod_{\frac{p}{q}\in[0,1]} B(\frac{p}{q}, \frac{1}{q})$ on $[0, 1]$. □

Prop. (4.8.3.32) [Quasi-Coherent Sheaves]. For $X \in \mathcal{S}ch$, $\mathcal{QC}oh(X)$ is Grothendieck category, and there is a **coherentor** left adjoint to the forgetful functor. ⌟

Proof: Firstly by(6.5.1.3), $\mathcal{QC}oh(X)$ is an Abelian category, and on affine open set, the colimit is an Qco sheaf, thus the colimit exists in Qco and equals the colimit in the category of sheaves, thus filtered colimits is exact because $\mathcal{M}od(\mathcal{O}_X)$ is Grothendieck(4.8.3.29). The generator exists, Cf.[Sta]077P.

The coherentor exists by the fact that $h_{\mathcal{F}}$ commutes with colimits and by the property of Grothendieck category(4.8.3.24). □

4 Triangulated Categories

References are [Triangulated Categories, Neeman].

Def. (4.8.4.1) [Triangulated Categories]. A **triangulated category** is an additive category $\mathcal{T}$(4.8.1.10) with an additive automorphism $T : \mathcal{T} \cong \mathcal{T}$ denoted by $X \mapsto X[1]$ and a set of distinguished triangles $\mathrm{Tri}(\mathcal{T})$ that is stable under isomorphism, and satisfying the following axioms:

(TR1): $X \xrightarrow{\text{id}} X \to 0 \to X[1] \in \text{Tri}(\mathcal{D})$. Any morphism $X \xrightarrow{u} Y$ can be completed to some $X \xrightarrow{u} Y \to C(u) \to X[1] \in \text{Tri}(\mathcal{T})$. Such an object $C(u)$ is called the **mapping cone** of u.

(TR2): $X \to Y \to Z \to X[1] \in \text{Tri}(\mathcal{D})$ iff $Y \to Z \to X[1] \to Y[1] \in \text{Tri}(\mathcal{D})$.

(TR3): Any two consecutive morphisms of two distinguished triangles can be extended to a morphism of distinguished triangles.

(TR4): If $X \xrightarrow{f} Y \xrightarrow{g} Z$ are morphisms, then there are maps $C(f) \to C(gf)$, $C(gf) \to C(g)$ by TR3, Then $C(f) \to C(gf) \to C(gf) \to C(g) \to C(f)[1]$ is distinguished.

A **triangulated subcategory** is an additive subcategory $\mathcal{D}'$ stable under [1] and [−1] together with a subclass of triangles in $\mathcal{D}'$ that forms a triangulated category.

We use the symbol $\mathcal{A} \in \mathcal{T}\text{ri}\,\mathcal{C}\text{at}$ to denote that $\mathcal{A}$ is a triangulated category. ⌟

Def. (4.8.4.2) [Notations]. We use the tuple (X, Y, Z, f, g, h) to represent a distinguished triangle $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} X[1]$. ⌟

Prop. (4.8.4.3). Given $(X, Y, Z, f, g, h), (X', Y', Z', f', g', h')$, they are both in $\text{Tri}(\mathcal{D})$ iff $(X \oplus X', Y \oplus Y', Z \oplus Z', f \oplus f', g \oplus g', h \oplus h')$ is in $\text{Tri}(\mathcal{D})$. ⌟

Proof: [Sta]05QS. □

Cor. (4.8.4.4). $(X, X \oplus Y, Y, (1, 0), (0, 1), 0)$ is a distinguished triangle. ⌟

Prop. (4.8.4.5). There is a natural notation of a product of triangulated categories. ⌟

Def. (4.8.4.6) [Cohomological Functors and Exact Functors]. A functor from a triangulated category to an Abelian category is called a **cohomological functor** if it maps a distinguished triangle to a long exact sequence. Similarly, we can define homological functors.

Conversely, a δ**-functor** is a functor from an Abelian category to a triangulated category together with a map from the category of exact sequences to the category of distinguished triangles.

A functor F between two triangulated category is called an **exact functor** if it maps distinguished triangles to distinguished triangles, and there is an isomorphism of functors $\xi : F \circ [1] \to [1] \circ F$. ⌟

Prop. (4.8.4.7). An exact functor between triangulated categories is additive. ⌟

Proof: Cf.[Sta]05QY. □

Def. (4.8.4.8) [Bi-Exact Functors]. Let $\mathcal{D}, \mathcal{D}', \mathcal{E}$ be triangulated categories, a **bi-exact bifunctor** $F : \mathcal{D} \times \mathcal{D}' \to \mathcal{E}$ is a functor that for any $X \in \mathcal{D}$, $F(X, -) : \mathcal{D} \to E$ is an exact functor and for any $Y \in \mathcal{D}'$, $F(-, Y) : \mathcal{D} \to \mathcal{E}$ is an exact functor. By(4.8.4.7), any bi-exact functor is bi-additive. ⌟

Prop. (4.8.4.9). If $(F, G) : \mathcal{D} \rightleftharpoons \mathcal{D}'$ is an adjunction pair between triangulated categories and F is exact, then G is also an exact functor between triangulated categories. ⌟

Proof: Use adjunction, we can show that G commutes with [1], and if $A \to B \to C \to A[1] \in \text{Tri}(\mathcal{D}')$, choose a distinguished triangle $G(A) \to G(B) \to X \to G(A)[1] \in \text{Tri}(\mathcal{D})$, then by (TR3) we get a map of distinguished triangles $(F(G(A)), F(G(B)), F(X)) \to (A, B, C)$, which by adjunction defines a map of distinguished triangles $(G(A), G(B), X) \to (G(A), G(B), G(C)$, which shows $X \cong G(C)$, and then $(G(A), G(B), G(C))$ is in $\text{Tri}(\mathcal{D})$. □

Prop. (4.8.4.10). If $(F, G) : \mathcal{D} \rightleftharpoons \mathcal{D}'$ is an adjunction pair between triangulated categories and F, G are exact, F is fully faithful and $\ker(G) = 0$, then this is an equivalence of categories. ⌟

Proof: By(4.1.1.31), $u : \mathrm{id} \to gf$ is an isomorphism. Now for any $X \in \mathcal{D}'$, choose a distinguished triangle $(F(G(X)), X \to Y) \in \mathrm{Tri}(\mathcal{D}')$, which corresponds to $(G(F(G(X))), G(X), G(Y)) \in \mathrm{Tri}(\mathcal{D})$, and by(4.1.1.29), $G(X) \xrightarrow{u_X} GFG(X) \to G(X)$ is id_X, so we get an isomorphism of triangles $(G(F(G(X))), G(X), G(Y)) \cong (G(X), G(X), 0)$, so $G(Y) \cong 0$, and $Y = 0$ by hypothesis. So $v : FG \to \mathrm{id}$ is also an isomorphism, so (F, G) is an equivalence. □

Lemma (4.8.4.11). If (X, Y, Z, f, g, h) is a distinguished triangle, then $g \circ f = 0$. ⌟

Proof: By TR1 $(X, X, 0, \mathrm{id}, 0, 0)$ is a distinguished triangle, and by TR3 there is a map of distinguished triangles

$$\begin{array}{ccccccc} X & = & X & \longrightarrow & 0 & \longrightarrow & X[1] \\ \| & & \downarrow{\scriptstyle f} & & \downarrow & & \| \\ X & \xrightarrow{f} & Y & \xrightarrow{g} & Z & \xrightarrow{h} & X[1] \end{array},$$

so $g \circ f = 0$. □

Prop. (4.8.4.12) [Long Exact Sequences]. Let $\mathcal{D}$ be a triangulated category and $C \in \mathcal{D}$ be any object, $\mathrm{Hom}_{\mathcal{D}}(-, C)$ and $\mathrm{Hom}_{\mathcal{D}}(C, -)$ is (co)homological. ⌟

Proof: By(4.8.4.3), for any distinguished triangle (X, Y, Z, f, g, h), $\mathrm{Hom}(C, X) \to \mathrm{Hom}(C, Y) \to \mathrm{Hom}(C, Z)$ is 0, and if $a \in \mathrm{Hom}(C, Y)$ is mapped to $0 \in \mathrm{Hom}(C, Y)$, then the morphism $(a, 0) : (C, 0) \mapsto (Y, Z)$ extends to a morphism of distinguished triangles $(b, a, 0) : (C, C, 0, \mathrm{id}, 0, 0) \to (X, Y, Z, f, g, h)$, thus $f \circ b = a$.

The converse case is dual. □

Cor. (4.8.4.13). If $(a, b, c) : (X, Y, Z, f, g, h) \to (X', Y', Z', f', g', h')$ is a morphism of distinguished triangles that two of a, b, c are isomorphisms, then this is an isomorphism of triangles.

In particular, the completion in TR1 is unique(may up to non-unique isomorphism) by TR3. ⌟

Proof: By 5-lemma, $\mathrm{Hom}(C, X) \to \mathrm{Hom}(C, X')$ is an isomorphism, then $X \to X'$ is an isomorphism by Yoneda lemma. □

Prop. (4.8.4.14). Let $\mathcal{D}$ be a triangulated category, then $f : X \to Y \in \mathcal{D}$ is an isomorphism iff $C(f) = 0$. ⌟

Proof: There is a morphism $(\mathrm{id}_X, f, 0) : (X, X, 0, \mathrm{id}, 0, 0) \to (X, Y, C(f), f, g, h)$ by (TR1) and (TR3). By(4.8.4.13), f is an isomorphism iff $0 \to C(f)$ is an isomorphism, which is equivalent to $Z = 0$. □

Prop. (4.8.4.15). In a triangulated category $\mathcal{D}$, any commutative diagram

$$\begin{array}{ccc} X & \longrightarrow & Y \\ \downarrow & & \downarrow \\ X' & \longrightarrow & Y' \end{array}$$

can be extended to a diagram

$$\begin{array}{ccccccc}
X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & X[1] \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
X' & \longrightarrow & Y' & \longrightarrow & Z' & \longrightarrow & X'[1] \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
X'' & \longrightarrow & Y'' & \longrightarrow & Z'' & \longrightarrow & X''[1] \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
X[1] & \longrightarrow & Y[1] & \longrightarrow & Z[1] & \longrightarrow & X[2]
\end{array}$$

where the lower right is anti-commutative. ⌟

Proof: Let $(X,Y,Z),(X',Y',Z'),(X,X',X''),(Y,Y',Y''),(X,Y,A)$ be distinguished triangles, then we can find maps $a:Z\to A, b:A\to Y', a':X''\to A, b':A\to Z$ by TR3(4.8.4.1). Then TR4 says $(Z\to A,Y''),(X''\to Z\to Z')$ is distinguished.

Now let (X'',Y'',Z'') be distinguished, then we use TR4 again to (X'',A,Y''), then $(Z',Z'',Z[1])$ is distinguished, thus so does $(Z\to Z'\to Z'')$.

Now it is left to verify the anti-commutativity of the righthdown square, for this, Cf.[Sta]05R0. □

Prop. (4.8.4.16)[Kernels are Saturated Triangulated Subcategories]. Let $\mathcal{D},\mathcal{D}'$ be triangulated categories and $\mathcal{A}$ an Abelian category.

- Let $F:\mathcal{D}\to\mathcal{D}'$ be an exact functor, then the full subcategory of $\mathcal{D}$ consisting of objects X that $F(X)=0$ is a strictly full saturated triangulated subcategory of $\mathcal{D}$, called the **kernel** of F.
- Let $H:\mathcal{D}\to\mathcal{A}$ be a (co)homological functor. then the full subcategory of $\mathcal{D}$ consisting of objects X that $F(X[n])=0$ for all n is a strictly full saturated triangulated subcategory of $\mathcal{D}$, called the **kernel** of H.

⌟

Proof: Cf.[Sta]05RC, 05RD. □

Localizations of Triangulated Category

Def. (4.8.4.17) [Compatible Localizing Systems]. Let $\mathcal{D}$ be a triangulated category, a localizing system(4.1.1.54) S is said to be compatible with the triangulated structure if it satisfies the following axioms:

(LS4): For $s\in S, s[n]\in S$ for any $n\in\mathbb{Z}$.

(LS5): Any two consecutive morphisms of two distinguished triangle can be extended to a morphism of distinguished triangles by morphisms in S.

⌟

Cor. (4.8.4.18). Let $\mathcal{D}$ be a triangulated category. If a class of morphisms S satisfy (LS1), (LS5) and (LS6), then (LS2) holds as well. ⌟

Proof: Let $f : X \to Y \in \mathcal{D}$ and $s : X \to X' \in S$, we can use (TR1) and (TR2) to extend these to a morphism of distinguished triangles

$$\begin{array}{ccccccc} X & \xrightarrow{f} & Y & \longrightarrow & Z & \longrightarrow & X[1] \\ \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle s'} & & \| & & \downarrow{\scriptstyle s[1]} \\ X' & \longrightarrow & Y' & \longrightarrow & Z & \longrightarrow & X'[1] \end{array}.$$

The right extension is dual. □

Prop. (4.8.4.19) [Exact Functors and Saturated Localizing Systems]. Let $\mathcal{D}, \mathcal{D}'$ be triangulated categories and $\mathcal{A}$ an Abelian category.

- If $F : \mathcal{D} \to \mathcal{D}'$ is an exact functor and
$$S = \{f \in \mathcal{D} | F(f) \text{ is an isomorphism}\},$$
then S is a saturated localizing system compatible with the triangulated structure(4.8.4.17).
- If $H : \mathcal{D} \to \mathcal{A}$ is a (co)homological functor and
$$S = \{f \in \mathcal{D} | H^i(f) \text{ is an isomorphism}\},$$
then S is a saturated localizing system compatible with the triangulated structure(4.8.4.17).

⌟

Proof: Cf.[Sta]05R4, 05R6. □

Prop. (4.8.4.20) [Localed Triangulated Categories]. Let $\mathcal{D}$ be a triangulated category and S is a localizing system compatible with the triangulated structure, then there is a unique triangulated category structure on $S^{-1}\mathcal{D}$ that the localization functor $Q : \mathcal{D} \to S^{-1}\mathcal{D}$(4.1.1.53) is exact.

Moreover, $S^{-1}\mathcal{D}$ satisfies the following universal properties:

- If $\mathcal{A}$ is an Abelian category and $H : \mathcal{D} \to \mathcal{A}$ is a cohomological functor that $H(s)$ are isomorphisms for all $s \in S$, then the unique factorization $H' : S^{-1}\mathcal{D} \to \mathcal{A}$ s.t. $H' \circ Q = H$(4.1.1.58) is also a cohomological functor.
- If $\mathcal{D}'$ is a triangulated category and $F : \mathcal{D} \to \mathcal{D}'$ is an exact functor that $F(s)$ are isomorphisms for all $s \in S$, then the unique factorization $F' : S^{-1}\mathcal{D} \to \mathcal{A}$ s.t. $F' \circ Q = F$(4.1.1.58) is also an exact functor.

⌟

Proof: Cf.[Sta]05R6. □

Cor. (4.8.4.21) [Kernel of Localizing Functor]. An object $Z \in \mathcal{D}$ is in the kernel of the localizing functor $Q : \mathcal{D} \to S^{-1}\mathcal{D}$ iff it satisfies the following equivalent conditions:

- There exists Z' s.t. $0 : Z \to Z' \in S$.
- There exists Z' s.t. $0 :' \to Z \in S$.
- There exists Z' and a distinguished triangle $(X, Y, Z \oplus Z', f, g, h)$ that $f \in S$.

⌟

Proof: Cf.[Sta]05R8. □

Prop. (4.8.4.22) [Triangulated Subcategories of Localized Triangulated Categories]. Let $\mathcal{D}$ be a triangulated category and S is a localizing system compatible with the triangulated structure. Let $\mathcal{D}'$ be a full triangulated subcategory of $\mathcal{D}$ and S' is a localizing system of $\mathcal{D}'$. If either of the following holds:

- For any $s : X \to Y \in S$ and $X \in \mathcal{D}'$, there is a morphism $t : Y \to Z$ that $Z \in \mathcal{D}'$ and $t \circ s \in S'$.
- The same as in item1 but with arrows reversed.

Then the natural functor $(S')^{-1}\mathcal{D}' \to S^{-1}\mathcal{D}$ is fully faithful. ⌟

Proof: This is immediate from(4.1.1.61). □

Quotients of Triangulated Categories

Def. (4.8.4.23) [Saturated Triangulated Subcategories]. Let $\mathcal{D}$ be a triangulated category, then a full triangulated subcategory $\mathcal{D}'$ is called a **saturated triangulated subcategory** if whenever $X \oplus Y$ is isomorphic to an object of $\mathcal{D}'$, X, Y are all isomorphic to an object of $\mathcal{D}'$. ⌟

Prop. (4.8.4.24) [Full Triangulated Subcategories and Localizing Systems]. Let $\mathcal{D}$ be a triangulated category.

- If $\mathcal{D}'$ is a full triangulated subcategory, then
$$S = \{f : X \to Y \in \mathcal{D}' | \text{there exists a distinguished triangle } (X, Y, Z, f, g, h), Z \in \mathcal{D}'\}$$
is a localizing system compatible with the triangulated structure of $\mathcal{D}$. And S is saturated iff $\mathcal{D}'$ is saturated.
- If S is a localizing system of $\mathcal{D}$, then $\mathcal{D}' = \ker(\mathcal{D} \to S^{-1}\mathcal{D})$(4.8.4.20)(4.8.4.16) is a saturated full triangulated subcategory of $\mathcal{D}$.

⌟

Proof: 1: Cf.[Sta]05RH. □

Def. (4.8.4.25) [Quotient Triangulated Categories]. Let $\mathcal{D}$ be a triangulated subcategory and $\mathcal{B}$ a full triangulated subcategory, define the **quotient triangulated category** $\mathcal{D}/\mathcal{B}$ as the localized triangulated category $S^{-1}\mathcal{D}$, where S is the localizing system associated to $\mathcal{B}$(4.8.4.24).

Moreover, $\mathcal{D}/\mathcal{B}$ satisfies the following universal properties:

- If $\mathcal{A}$ is an Abelian category and $H : \mathcal{D} \to \mathcal{A}$ is a cohomological functor that $\mathcal{B} \subset \ker(H)$, then H factors uniquely through $\mathcal{D}/\mathcal{B}$ by a functor H', and H' is also a cohomological functor.
- If $\mathcal{D}'$ is a triangulated category and $F : \mathcal{D} \to \mathcal{D}'$ is a cohomological functor that $\mathcal{B} \subset \ker(F)$, then F factors uniquely through $\mathcal{D}/\mathcal{B}$ by a functor F', and F' is also an exact functor.

⌟

Proof: The universal properties follow from the universal properties of localized triangulated categories(4.8.4.20) and the definition of S(4.8.4.24), using the long exact sequence or(4.8.4.14). □

Prop. (4.8.4.26) [Saturation]. Let $\mathcal{D}$ be a triangulated category and $\mathcal{D}'$ be a full triangulated subcategory, then the kernel of the quotient map $\mathcal{D} \to \mathcal{D}/\mathcal{D}'$(4.8.4.25) is a strictly full saturated subcategory consisting of objects $Z \in \mathcal{D}$ that $Z \oplus Z'$ is an object of $\mathcal{D}'$ for some object $Z' \in \mathcal{D}$. In particular, it is the smallest saturated triangulated subcategory containing $\mathcal{D}'$, called the **saturation of** $\mathcal{D}'$. ⌟

Proof: the kernel is a strictly full saturated subcategory by(4.8.4.16). The description of the objects of kernel follows from the definition(4.8.4.25)(4.8.4.24) amd(4.8.4.21). □

Prop. (4.8.4.27) [Kernel of Cohomological Functor is Saturated]. Let $\mathcal{D} \in \mathcal{T}\mathrm{ri}\,\mathcal{C}\mathrm{at}, \mathcal{A} \in \mathcal{A}\mathrm{b}\,\mathcal{C}\mathrm{at}$ and $H : \mathcal{D} \to \mathcal{A}$ a cohomological functor, then $\ker(H)$ is a saturated full triangulated subcategory(4.8.4.16) whose corresponding saturated localizing system(4.8.4.19) is the set

$$S = \{f | H^i(f) \text{ is an isomorphism in } \mathcal{A}\},$$

and H factors through the quotient $\mathcal{D} \to \mathcal{D}/\ker(H)$. ⌟

Proof: The description of S is clear from the definitions(4.8.4.16)(4.8.4.24) and a use of long exact sequences. The factorization follows from(4.8.4.25). □

Brown Representability

References are [Triangulated Categories, Neeman] and [Brown Representation, Krause].

Def. (4.8.4.28) [Generators]. Let $\mathcal{D}$ be a triangulated category, a **generator of** $\mathcal{D}$ is an object of $\mathcal{D}$ s.t. for any object K of $\mathcal{D}$, there exists some integer n and a non-zero map $E[n] \to K$. ⌟

Prop. (4.8.4.29). For $\mathcal{T} \in \mathcal{T}\mathrm{ri}\,\mathcal{C}\mathrm{at}$, the compact objects of $\mathcal{D}$ form a Karoubian, saturated, strictly full triangulated category of $\mathcal{T}$. ⌟

Proof: Cf.[Sta]09QH. □

Def. (4.8.4.30) [Compactly Generated]. Let $\mathcal{D}$ be a triangulated category with arbitrary small direct sums, then $\mathcal{D}$ is said to be a **compactly generated triangulated category** if there exists a set of compact objects $\{E_i\}$ that $\oplus E_i$ is a generator of $\mathcal{D}$(4.8.4.28). ⌟

Thm. (4.8.4.31) [Brown Representability, Neeman/Krause]. Suppose $\mathcal{T} \in \mathcal{T}\mathrm{ri}\,\mathcal{C}\mathrm{at}$ has arbitrary small direct sums and is generated by a set of perfect objects, then a functor $F : \mathcal{T} \to \mathcal{A}\mathrm{b}^{\mathrm{op}}$ is cohomological and transforms direct sums into products, then H is representable.

In particular, the hypothesis is satisfied when $\mathscr{T}$ is compactly generated. ⌟

Proof: Cf.[Sta]018F or [Krause, A Brown representability theorem]. □

Cor. (4.8.4.32) [Adjointness Lemma]. Let $\mathcal{D} \in \mathcal{T}\mathrm{ri}\,\mathcal{C}\mathrm{at}$ with arbitrary small coproducts that is compactly generated and $F : \mathcal{D} \to \mathcal{D}'$ an exact functor of triangulated categories that transforms direct limits to direct limits, then F has an exact right adjoint. ⌟

Proof: By Brown representability, for any $Y \in \mathcal{D}'$, there is an object $G(Y) \in \mathcal{D}$ that represents the contravariant cohomological functor $\mathcal{D} \to \mathcal{A}\mathrm{b} : X \mapsto \mathrm{Hom}_{\mathcal{D}'}(F(X), Y)$(4.8.4.12). Then G is a functor by Yoneda lemma. It is exact by(4.8.4.9). □

5 T-Structures

Def. (4.8.5.1) [T-Structures]. A **T-structure** on a triangulated category $\mathcal{D}$(4.8.4.1) is a pair of strictly full subcategories $\mathcal{D}^{\leq 0}$ and $\mathcal{D}^{\geq 0}$ s.t. if we denote $\mathcal{D}^{\leq n} = \mathcal{D}^{\leq 0}[-n]$ and $\mathcal{D}^{\geq n} = \mathcal{D}^{\geq 0}[-n]$, then

1. If $A \in \mathcal{D}^{\leq 0}$ and $B \in \mathcal{D}^{\geq 1}$, then $\mathrm{Hom}(A, B) = 0$.
2. $\mathcal{D}^{\leq 0} \subset \mathcal{D}^{\leq 1}$, $\mathcal{D}^{\geq 1} \subset \mathcal{D}^{\geq 0}$.
3. For any $E \in \mathcal{D}$, there is a distinguished triangle (A, E, B) with $A \in \mathcal{D}^{\leq 0}$ and $B \in \mathcal{D}^{\geq 1}$.

And $\mathcal{D}$ is said to be **bounded** w.r.t. this T-structure iff each object in $\mathcal{D}$ is contained in $\mathcal{D}^{\geq a} \cap \mathcal{D}^{\leq b}$ for some $a, b \in \mathbb{Z}$.

We use the symbol $(\mathcal{D}, \mathcal{D}^{\leq 0}, \mathcal{D}^{\geq 0}) \in$ t-$\mathcal{T}$ri $\mathcal{C}$at or $\mathcal{D} \in$ t-$\mathcal{T}$ri $\mathcal{C}$at to denote that $(\mathcal{D}, \mathcal{D}^{\leq 0}, \mathcal{D}^{\geq 0})$ is a triangulated category with the T-structure $(\mathcal{D}^{\leq 0}, \mathcal{D}^{\geq 0})$. ⌟

Def. (4.8.5.2) [Truncations]. For $\mathcal{D} \in$ t-$\mathcal{T}$ri $\mathcal{C}$at and $E \in \mathcal{D}$, by item3 of(4.8.5.1) there exists a distinguished triangle (A, E, B) with $A \in \mathcal{D}^{\leq 0}$ and $B \in \mathcal{D}^{\geq 1}$. Then it follows from the long exact sequence(4.8.4.12) that for any $X \in \mathcal{D}^{\leq 0}$,

$$\mathrm{Hom}(X, A) \cong \mathrm{Hom}(X, E).$$

In other words, A initial w.r.t. morphisms from $\mathcal{D}^{\leq 0}$ to E. Thus by using the axiom of choice, we can define a **truncation functor**

$$\tau_{\leq 0} : \mathcal{D} \to \mathcal{D}^{\leq 0}$$

right adjoint to the inclusion functor $\mathcal{D}^{\leq 0} \subset \mathcal{D}$.

Similarly, we can define the truncation functor

$$\tau_{\geq 0} : \mathcal{D} \to \mathcal{D}^{\geq 0}$$

left adjoint to the inclusion functor $\mathcal{D}^{\geq 0} \subset \mathcal{D}$. And by shifting, we can define all $\tau_{\leq n}$ and $\tau_{\geq n}$ for $n \in \mathbb{Z}$.

In particular, there are canonical **truncation distinguished triangles**

$$(\tau_{\leq n} E, E, \tau_{\geq n+1} E).$$

⌟

Prop. (4.8.5.3) [Orthogonality]. For $\mathcal{D} \in t\,\mathcal{C}$at and $E \in \mathcal{D}, n \in \mathbb{Z}_+$, the following are equivalent:

- $E \in \mathcal{D}^{\geq n+1}$.
- $\mathrm{Hom}(A, E) = 0$ for any $A \in \mathcal{D}^{\leq n}$.

⌟

Proof: We may assume $n = 0$. And $1 \to 2$ follows from the definition. For $2 \to 1$, it suffices to show that $\tau_{\leq n} E = 0$. For this, use the adjunction

$$\mathrm{Hom}(\tau_{\leq 0} E, \tau_{\leq 0} E) = \mathrm{Hom}(\tau_{\leq 0} E, E) = 0.$$

□

Cor. (4.8.5.4) [Extension Property]. Suppose (X, Y, Z) is a distinguished triangle and $n \in \mathbb{Z}$.

- If $X, Z \in \mathcal{D}^{\leq n}$, then $Y \in \mathcal{D}^{\leq n}$.
- If $X \in \mathcal{D}^{\leq n}$ and $Y \in \mathcal{D}^{\leq n+1}$, then $Z \in \mathcal{D}^{\leq n}$.

⌟

Proof: These follow from the orthogonality property above. □

Cor. (4.8.5.5). Let $\mathcal{D} \in \mathcal{T}$ri $\mathcal{C}$at and α, β are two T-structures s.t. ${}^{\alpha}\mathcal{D}^{\leq 0} \subset {}^{\beta}\mathcal{D}^{\leq 0}$ and ${}^{\alpha}\mathcal{D}^{\geq 0} \subset {}^{\beta}\mathcal{D}^{\geq 0}$, then the two T-structures are the same. ⌟

Prop. (4.8.5.6)[Compatibility]. Let $\mathcal{D}$ be a triangulated category with a T-structure, then for $m, n \in \mathbb{Z}$,

$$\tau_{\geq m}(\mathcal{D}^{\leq n}) \subset \mathcal{D}^{\leq n}, \quad \tau_{\leq m}(\mathcal{D}^{\geq n}) \subset \mathcal{D}^{\geq n}.$$

And if $m > n$,

$$\tau_{\geq m}(\mathcal{D}^{\leq n}) = \tau_{\leq n}(\mathcal{D}^{\geq m}) = 0.$$

⌟

Proof: If $m > n$ and $X \in \mathcal{D}^{\leq n}$, then $\mathrm{Hom}(X, \tau_{\geq m}(X)) = 0$, and then by adjunction $\mathrm{Hom}(\tau_{\geq m}(X), \tau_{\geq m}(X)) = 0$, so $\tau_{\geq m}(X) = 0$.

If $m \leq n$ and $X \in \mathcal{D}^{\leq n}$, then there is a truncation distinguished triangle $(\tau_{\leq m-1}X, X, \tau_{\geq m}X)$, so it follows from the extension property 2 that $\tau_{\geq m}X \in \mathcal{D}^{\leq n}$. □

Def. (4.8.5.7) [Cores]. For $\mathcal{D} \in$ t-$\mathcal{T}$ri $\mathcal{C}$at, the **core of** $\mathcal{D}$ is defined to be the full subcategory

$$\mathcal{D}^{\heartsuit} = \mathcal{D}^{\geq 0} \cap \mathcal{D}^{\leq 0}.$$

⌟

Prop. (4.8.5.8) [Cores are Abelian Categories]. If $\mathcal{D} \in$ t-$\mathcal{T}$ri $\mathcal{C}$at, then $\mathcal{D}^{\heartsuit}$ is an Abelian category, and a sequence

$$0 \to X \xrightarrow{u} Y \xrightarrow{v} Z \to 0$$

in $\mathcal{D}^{\heartsuit}$ is exact iff there exists some distinguished triangle (X, Y, Z, u, v, w) in $\mathcal{D}$. ⌟

Proof:

□

Prop. (4.8.5.9). For $\mathcal{D} \in$ t-$\mathcal{T}$ri $\mathcal{C}$at and $X, Z \in \mathcal{D}^{\heartsuit}$,

$$\mathrm{Ext}^1_{\mathcal{D}^{\heartsuit}}(Z, X) = \mathrm{Hom}(Z, X[1]).$$

⌟

Proof:

□

Def. (4.8.5.10) [Thick Triangulated Subcategories]. For $\mathcal{D} \in \mathcal{T}$ri $\mathcal{C}$at, a full triangulated subcategory $\mathcal{C} \subset \mathcal{D}$ is called a **thick triangulated subcategory** if objects $X, Y \in \mathcal{D}$ must lie in $\mathcal{C}$, provided there exists a morphism $f : X \to Y$ s.t.

- f factors through an object in $\mathcal{C}$, and
- f has a mapping cone $C(f) \in \mathcal{C}$.

⌟

Def. (4.8.5.11) [Cohomology Functors]. For $\mathcal{D} \in$ t-$\mathcal{T}$ri $\mathcal{C}$at and $n \in \mathbb{Z}$, the **n-th cohomology functor** is defined to be

$$H^n : \mathcal{D} \to \mathcal{D}^{\heartsuit} : X \mapsto \tau_{\leq 0}\tau_{\geq 0}(X[n]) = (\tau_{\leq n}\tau_{\geq n}X)[n].$$

⌟

6 Chain Complexes

Def. (4.8.6.1) [Chain Complexes]. A **chain complex** over an additive category $\mathcal{A}$ is**?**. The category of complexes over $\mathcal{A}$ is denoted by $\mathrm{Ch}^{\mathbb{Z}}(\mathcal{A})$. ⌟

Prop. (4.8.6.2). For any Abelian category $\mathcal{A}$, $\mathrm{Ch}^{\mathbb{Z}}(\mathcal{A})$ is an Abelian category. ⌟

Prop. (4.8.6.3). The natural inclusion $\mathcal{A} \subset \mathrm{Ch}^{\mathbb{Z}}(A)$ embeds $\mathcal{A}$ as a full subcategory of $\mathrm{Ch}^{\mathbb{Z}}(A)$, and H^0 is just the left adjoint.

An object $K \in \mathrm{Ch}^{\mathbb{Z}}(A)$ is called **discrete** if it is in the essential image of this embedding. ⌟

Def. (4.8.6.4) [Shifting of Complexes]. For $\mathcal{A} \in \mathcal{A}\mathrm{dd}\,\mathfrak{C}\mathrm{at}$, there is a **shifting of complex functor** $[1] : \mathrm{Ch}^{\mathbb{Z}}(\mathcal{A}) \to \mathrm{Ch}^{\mathbb{Z}}(\mathcal{A})$ s.t. for $K^\bullet \in \mathrm{Ch}^{\mathbb{Z}}(\mathcal{A})$,

$$K^\bullet[1]_n = K^\bullet_{n+1}, \quad d^n_{K^\bullet[1]} = -d^{n=1}_{K^\bullet}.$$

⌟

Def. (4.8.6.5) [Truncation of Complexes]. Let $\mathcal{A}$ be an Abelian category and $A^\bullet \subset \mathrm{Ch}^{\mathbb{Z}}(\mathcal{A})$, there are several ways to truncate $A^\bullet$:

- The **stupid truncation** $\sigma_{\leq n} A = \ldots \to A_{n-1} \to A_n \to 0 \to \ldots$. There is a morphism $A \to \sigma_{\leq n} A$.
- The stupid truncation $\sigma_{\geq n} A = \ldots \to 0 \to A_n \to A_{n+1} \to \ldots$. There is a morphism $\sigma_{\geq n} A \to A$.
- The **canonical truncation** $\tau_{\leq n} A = \ldots \to A_{n-1} \to \ker(d_n) \to 0 \to \ldots$. There is a natural morphism $\tau_{\leq n} A \to A$ that induces isomorphism on cohomology groups on degree$\leq n$.
- The canonical truncation $\tau_{\geq n} A = \ldots \to 0 \to \mathrm{Coker}(d_{n-1}) \to A_{n+1} \to \ldots$. There is a natural morphism $A \to \tau_{\geq n} A$ that induces isomorphism on cohomology groups on degree$\geq n$.

⌟

Cor. (4.8.6.6). There are exact sequences of complexes

$$0 \to \tau_{\leq n} A^\bullet \to A^\bullet \to \tau_{\geq n+1} A^\bullet \to 0$$

$$0 \to \sigma_{\geq n+1} A^\bullet \to A^\bullet \to \sigma_{\leq n} A^\bullet \to 0$$

⌟

Def. (4.8.6.7) [Cone & Cylinder]. The **mapping cone** of $f : K^\bullet \to L^\bullet$ is the complex $C(f)^\bullet$ that:

$$C(f) = K[1]^\bullet \oplus L^\bullet, \quad d(k^{i+1}, l^i) = (-d_K k^{i+1}, f(k^{i+1}) + d_L l^i)$$

The **mapping cylinder** of $f : K^\bullet \to L^\bullet$ is the complex $\mathrm{Cyl}(f)$ that:

$$\mathrm{Cyl}(f) = K^\bullet \oplus K[1]^\bullet \oplus L^\bullet, \quad d(k^i, k^{i+1}, l^i) = (d_K k^i - k^{i+1}, -d_K k^{i+1}, f(k^{i+1}) + d_L l^i)$$

It is a shame I haven't see clearly the similarity of this with the topological cone and cylinder, should study it further. ⌟

Def. (4.8.6.8) [Double Complexes]. A **double complex** over an Abelian category is a complex over $Comp(\mathcal{A})$(4.8.6.2). ⌟

Def. (4.8.6.9)[Totalization]. Given a double complex $K^{\bullet,\bullet}$ over an Abelian category $\mathcal{A}$, the associated **total complexes** is defined to be

$$(\mathrm{Tot}^{\Pi}(K))^n = \prod_{n=p+q} K^{p,q}, \quad d^n = \prod_{n=p+q} (d_1^{p,q} + (-1)^p d_2^{p,q})$$

$$(\mathrm{Tot}^{\oplus}(K))^n = \bigoplus_{n=p+q} K^{p,q}, \quad d^n = \sum_{n=p+q} (d_1^{p,q} + (-1)^p d_2^{p,q})$$

⌟

Def. (4.8.6.10) [Hom Complexes]. Let $\mathcal{A}$ be an Abelian category and $P^\bullet, Q^\bullet \in K(\mathcal{A})$, we define **Hom complex** $\mathrm{Hom}^\bullet(P^\bullet, Q^\bullet)$ to be

$$\mathrm{Hom}^n(P^\bullet, Q^\bullet) = \prod \mathrm{Hom}_i(P^i, Q^{n+i}),$$

with the differential giving by $d(\{f_k\})_i = \{df_i - (-1)^i f_{i+1} d\}$ and suitable signatures.

It is clear that $H^n(\mathrm{Hom}^\bullet(P^\bullet, Q^\bullet)) = \mathrm{Hom}_{K(\mathcal{A})}(P^\bullet, Q^\bullet[n])$. ⌟

Homotopy Category $K(\mathcal{A})$

Def. (4.8.6.11)[Homotopies of Complexes]. ⌟

Def. (4.8.6.12)[$K(\mathcal{A})$]. Let $\mathcal{A}$ be an additive category, the **homotopy category of complexes** $K(\mathcal{A})$ is the category whose objects are complexes in $\mathcal{A}$ and whose morphisms are homotopy classes of morphism between complexes. ⌟

Prop. (4.8.6.13) [Distinguished Triangle of $K^*(\mathcal{A})$]. For any morphism $K^\bullet \to L^\bullet$, there exists a termwise-spliting exact sequence of Complexes commuting in $K(\mathcal{A})$.

$$\begin{array}{ccccccccc}
 & & K^\bullet & \longrightarrow & L^\bullet & & & & \\
 & & \| & & \downarrow{\scriptstyle\alpha} & & & & \\
0 & \longrightarrow & K^\bullet & \longrightarrow & \mathrm{Cyl}(f) & \longrightarrow & C(f) & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle\beta} & & \| & & \\
 & & 0 & \longrightarrow & L^\bullet & \longrightarrow & C(f) & \longrightarrow & K^\bullet[1] \longrightarrow 0
\end{array}$$

where $\beta\alpha = \mathrm{id}$ and $\alpha\beta \sim \mathrm{id}$. And $K^\bullet \to L^\bullet \to C(f) \to K^\bullet[1]$ is called a distinguished triangle. Any exact triple of complexes in $\mathrm{Kom}(\mathcal{A})$ is quasi-isomorphic to a distinguished triangle. In fact, we can define the distinguished triangle in $K(\mathcal{A})$ as that induced by a split exact sequence, Cf.[Sta]014L.

Notice all this can imitate the similar parallel construction in the category of topological spaces. ⌟

Proof: Cf.[Gelfand P157] □

Cor. (4.8.6.14)[Long Exact Sequences]. A distinguished triangle will induce a long exact sequence of cohomology groups, for this, just need to verify that the δ-homomorphism and the morphism $C(f) \to K^\bullet[1]$ induce the same map of cohomology groups. ⌟

Cor. (4.8.6.15). A morphism of complexes $f : K^\bullet \to L^\bullet$ is quasi-iso iff $C(f)$ is acyclic. It is homotopic to 0 iff f can be extended to a morphism $C(f) \to L$. ⌟

Prop. (4.8.6.16) [$K(\mathcal{A})$ is Triangulated]. If $\mathcal{A}$ is an additive category, then $K^*(\mathcal{A})$ are triangulated categories, with shifting functors defined in(4.8.6.4) and distinguished triangles defined in(4.8.6.13).

And an additive functor will induce exact functor between K^* because distinguished is split. ⌟

Proof: Cf.[Sta]014S. or [Gelfand P246]. □

Prop. (4.8.6.17). An additive functor $F : \mathcal{A} \to \mathcal{B}$ between additive categories induces an exact functor $K(\mathcal{A}) \to K(\mathcal{B})$. Moreover, this functor maps quasi-isomorphisms to quasi-isomorphisms(4.8.7.1). ⌟

Proof: Cf.[Sta]014X. □

Def. (4.8.6.18) [Bounded Subcategories]. ⌟

Prop. (4.8.6.19). Let $\mathcal{A}$ be an Abelian category,

- If $A^\bullet \subset K^+(\mathcal{A})$, then $\tau_{\leq n}(A^\bullet) \to A^\bullet$ is a quasi-isomorphism for n sufficiently large.
- If $A^\bullet \subset K^-(\mathcal{A})$, then $A^\bullet \to \tau_{\geq n}A^\bullet$ is a quasi-isomorphism for n sufficiently small.

⌟

<u>**Unbounded Complexes**</u>

Lemma (4.8.6.20) [Left Resolutions of Unbounded Complexes]. Let $\mathcal{A}$ be an Abelian category and $\mathcal{P}$ be a subset of objects of $\mathcal{A}$. Assume that every object of $\mathcal{A}$ is a quotient of an object of $\mathcal{P}$, then for any complex $\mathcal{K}^\bullet$, there exists a commutative diagram

$$\begin{array}{ccccc} P_1^\bullet & \longrightarrow & P_2^\bullet & \longrightarrow & \cdots \\ \downarrow & & \downarrow & & \\ \tau_{\leq 1}K^\bullet & \longrightarrow & \tau_{\leq 2}K^\bullet & \longrightarrow & \cdots \end{array}.$$

where the vertical arrows are quasi-isomorphisms, and each $P_n^\bullet$ is a bounded above complex with terms in $\mathcal{P}$, and each $P_n^\bullet \to P_{n+1}^\bullet$ are termwise-split injections and the cokernel is also a complex with terms in $\mathcal{P}$. ⌟

Proof: Cf.[Sta]06XX. □

7 Cohomology of Complexes

Def. (4.8.7.1) [Quasi-irosmoepwhiss]. ⌟

Prop. (4.8.7.2) [Five lemma]. In an Abelian category, if there is a diagram

$$\begin{array}{ccccccccc} * & \longrightarrow & * & \longrightarrow & * & \longrightarrow & * & \longrightarrow & * \\ \downarrow s & & \downarrow g & & \downarrow f & & \downarrow h & & \downarrow i \\ * & \longrightarrow & * & \longrightarrow & * & \longrightarrow & * & \longrightarrow & * \end{array}$$

Where the rows are exact and g, h are isomorphisms. If i is injective, then f is surjective; if s is surjective, then f is injective. ⌟

Proof: Rotate the diagram counterclockwise $90°$. Then use the two different filtration both converge(4.10.7.8). □

Prop. (4.8.7.3) [Snake lemma]. In an Abelian category, if there is a diagram

$$\begin{CD} @. * @>i>> * @>>> * @>>> 0\\ @. @VfVV @VgVV @VhVV \\ 0 @>>> * @>>> * @>s>> * \end{CD}$$

where the rows are exact, then there is a long exact sequence

$$\ker f \to \ker g \to \ker h \to \operatorname{Coker} f \to \operatorname{Coker} g \to \operatorname{Coker} h$$

And if i is injective, then the first one is injective; if s is surjective, then the last one is surjective. ⌟

Proof: Rotate the diagram counterclockwise 90°. Then use the two different filtration both converge(4.10.7.8). □

Cor. (4.8.7.4). In an Abelian category, if $f: A \to B, g: B \to C$, then there is a long exact sequence:

$$0 \to \ker f \to \ker gf \to \ker g \to \operatorname{Coker} f \to \operatorname{Coker} gf \to \operatorname{Coker} g \to 0.$$

⌟

Proof: Use snake lemma(as modules), there is a diagrams:

$$\begin{CD} @. A @>f>> B @>>> \operatorname{Coker} f @>>> 0\\ @. @VgfVV @VgVV @VVV \\ 0 @>>> C @= C @>>> 0 \end{CD}$$

So by Snake lemma,

$$\ker gf \to \ker g \to \operatorname{Coker} f \to \operatorname{Coker} gf \to \operatorname{Coker} g \to 0.$$

As Abelian category is dual, we can do this dually to get:

$$0 \to \ker f \to \ker gf \to \ker g \to \operatorname{Coker} f \to \operatorname{Coker} gf.$$

They splint together to get the desired long exact sequence. □

Prop. (4.8.7.5). For a 3×3 diagram of complexes, the connection homomorphism satisfies an anti-commutative diagram:

$$\begin{CD} H^{q-1}(Z'') @>\delta>> H^q(X'') \\ @V\delta VV @V-\delta VV \\ H^q(Z) @>\delta>> H^{q+1}(X) \end{CD}$$

by(4.8.4.15) as the category $K(\mathcal{A})$ is triangulated. ⌟

Prop. (4.8.7.6) [Universal Coefficient Theorem]. Should be somewhere in [Weibel]. ⌟

Def. (4.8.7.7) [Herbrand Quotient]. For a complex of R-modules cyclic of order 2, we define the **additive Herbrand quotient** as $\operatorname{length}_R(H^0) - \operatorname{length}_R(H^1)$, when both are definable and the **multiplicative Herbrand quotient** as $|H^0|/|H^1|$ when they are both finite. ⌟

Prop. (4.8.7.8). For an exact sequence $0 \to M \to N \to K \to$ of complexes of cyclic order 2, we have $h(N) = h(M) + h(K)$ and $h^*(N) = h^*(M)h^*(K)$ in the sense that if two of them are definable, then so is the third. This is an easy consequence of long exact sequence. ⌟

Prop. (4.8.7.9). If each term of this complex has finite length, then $h(M) = 0$. If each term is finite, then $h^*(M) = 0$. This is an consequence of isomorphism theorem. So we have, if a morphism of complexes has kernel and cokernel finite, then it induce an isomorphism on h or h^*. ⌟

Proof: □

8 Injectives & Projectives

Remark (4.8.8.1). The use of injection resolutions can be replaced by the use of ∞-categories.?? ⌟

Def. (4.8.8.2) [Injective Objects]. An **injective object** in a Abelian category is a I s.t. $\mathrm{Hom}(-, I)$ is an exact functor, equivalently, maps to I can be extended along injections.

A **projective object** in a Abelian category is a I s.t. $\mathrm{Hom}(I, -)$ is an exact functor, equivalently, maps to I can be pulled back along surjections. ⌟

Prop. (4.8.8.3). Product of injective elements are injective, sums of projective elements are projective. ⌟

Prop. (4.8.8.4). In an Abelian category, the direct summand of a projective object is projective. (The summand has definition in an Abelian category). ⌟

Prop. (4.8.8.5). If a functor f between Abelian categories is left adjoint to an exact functor, then it preserves injectives. Dually for projectives. ⌟

Prop. (4.8.8.6). If A is an Abelian category, the chain complex category $Ch(A)$ is abelian by(4.8.3.8). A chain complex P is projective iff it is a split exact complex of projective objects. The same is true by dual argument for injectives. ⌟

Proof: If K is projective, use the surjection $C(\mathrm{id}_K) \to K[1]$, there is a homotopy between id_K and 0. Thus we have $x = dhx + hdx$. And if $dhx = hdy$, then $dhdy = 0$, thus $dy = 0$, so $K = dhK \oplus hdK$ and thus $K[n] = B_n \oplus B_{n+1}$. Thus K is a direct product of $0 \to B \to B \to 0$. And this one is projective if B is projective. □

Prop. (4.8.8.7) [Check Injectives]. In a Grothendieck Abelian category with generator U, an object is injective iff it is extendable over subobjects of U. (AB5 assures we can extend by Zorn's lemma. Then use GEN, Cf.[Sta]079G?). If it is a family of objects, it suffice to extend over each one of them. ⌟

Proof:

□

Injective Resolutions

Prop. (4.8.8.8) [Horseshoe Lemma]. For a exact sequence $0 \to X_1 \to X \to X_2 \to 0$ and a injective resolution of X_1 and X_2, there is a injective resolution of X commuting with them. (Choose them one-by-one, in fact, $I_n = I_n^1 \oplus I_n^2$ using the injectivity of I_n^1. Snake lemma told us that the cokernel is an exact sequence, use that to define the next one. ⌟

Prop. (4.8.8.9). For two lifting of morphisms $X_1 \to Y_1$ and $X_2 \to Y_2$, there is a lifting of the morphism $X \to Y$ compatible with that. Cf.[Weibel P2.4.6]. ⌟

Prop. (4.8.8.10)[Cartan-Eilenberg Resolution]. For a complex $K \in K^+(\mathcal{A})$, a **Cartan-Eilenberg resolution** of K consists of a 2-complex $I^{\bullet,\bullet}$ and a map of complexes $K \to I^{\bullet,0}$ that the induced complexes:

$$0 \to K^i \to I^{i,0} \to I^{i,2} \to \dots$$

$$0 \to B^i(K) \to B^i_x(I^{\bullet,0}) \to B^i_x(I^{\bullet,1}) \to \dots$$

$$0 \to Z^i(K) \to Z^i_x(I^{\bullet,0}) \to Z^i_x(I^{\bullet,1}) \to \dots$$

$$0 \to H^i(K) \to B^i_x(I^{\bullet,0}) \to H^i_x(I^{\bullet,1}) \to \dots$$

are all injective resolutions, and the exact sequences

$$0 \to B^i_x(I^{\bullet,j}) \to Z^i_x(I^{\bullet,j}) \to H^i_x(I^{\bullet,j}) \to 0$$

$$0 \to Z^i_x(I^{\bullet,j}) \to I^{\bullet,j} \to Z^i_x(I^{\bullet,j}) \to 0$$

split.

Then if $\mathcal{I}_\mathcal{B}$ is sufficiently large, for any K in $K(\mathcal{B})$ there is a Cartan-Eilenberg resolution. ⌟

Proof: Cf.[Gelfand P210],[Weibel P146].? □

Cor. (4.8.8.11). For a CE resolution of a complex $K \in K^+(\mathcal{B})$, the spectral sequence can be applied and shows $K \to \mathrm{Tot}(L)$ is a quasi-isomorphism, i.e. Tot(L) is a injective resolution of K. ⌟

Cor. (4.8.8.12)[Functoriality of Cartan-Eilenberg Resolution]. If $f : A \to B$ is a chain map and $A \to P, B \to Q$ are Cartan-Eilenberg resolutions, then there is a double complex map $\widetilde{f} : P \to Q$ extending f. And if f is homotopic to g, then $\widetilde{f}$ is homotopic to $\widetilde{g}$. In other words, we have a functor $K(\mathcal{A}) \to K(\mathcal{I}_\mathcal{A}^{\bullet\bullet})$

In particular, for any two Cartan-Eilenberg resolutions P, Q of A and an additive functor F, the chain complex $\mathrm{Tot}^\Pi(F(P))$ and $\mathrm{Tot}^\Pi(F(Q))$ are chain homotopy equivalent. ⌟

Def. (4.8.8.13)[Injective Amplitude]. Let $\mathcal{A}$ be an Abelian category with sufficiently injectives, then $K \in D(A)$ is said to have **finite injective dimension** if $K \subset D^b(\mathcal{I}_A)$. It is saied to have **injective amplitude** in $[a, b]$ iff $K \subset D^{[a,b]}(\mathcal{I}_A)$. ⌟

Prop. (4.8.8.14). Suppose $\mathcal{A}^\bullet \to \mathcal{I}^\bullet$ is an injective resolution of sheaves on $(\mathcal{C}, \mathcal{O})$, then the induced map of presheaves with values in $D_\infty(\mathbb{Z})$:

$$|\mathcal{A}^\bullet| \to |\mathcal{I}^\bullet|$$

identifies $|\mathcal{I}^\bullet|$ with the shifification of $|\mathcal{A}^\bullet|$. ⌟

Proof: ? □

9 Tensor Category Case

In this subsection we consider complexes over a tensor category(4.2.1.2) $\mathcal{A}$.

Lemma (4.8.9.1) [Koszul Sign Rule]. There is an isomorphism of complexes

$$\sigma : C^\bullet \otimes D^\bullet \to D^\bullet \otimes C^\bullet : \sigma(x \otimes y) = (-1)^{mn} y \otimes x$$

where $x \in C^m$ and $y \in D^n$. ⌟

Proof:

$$\partial(\sigma(x\otimes y)) = \partial((-1)^{mn}y\otimes x) = (-1)^{mn}(\partial y\otimes x)+(-1)^{mn+n}(y\otimes\partial x) = (-1)^n\sigma(x\otimes\partial y)+\sigma(\partial x\otimes y) = \sigma(\partial(x\otimes y))$$

□

Prop. (4.8.9.2) [Commutative Monoidal Structure on $\mathrm{Ch}^{\mathbb{Z}}(\mathcal{A})$]. The functor

$$\mathrm{Ch}^{\mathbb{Z}}(\mathcal{A}) \times \mathrm{Ch}^{\mathbb{Z}}(\mathcal{A}) \to \mathrm{Ch}^{\mathbb{Z}}(\mathcal{A}) : \quad (C^\bullet, D^\bullet) \mapsto \mathrm{Tot}^{\oplus}(C^\bullet \otimes D^\bullet)$$

endows $\mathrm{Ch}^{\mathbb{Z}}(\mathcal{A})$ with a (non-strict) commutative monoidal structure. ⌟

Proof: Commutativity follows from(4.8.9.1). Associality follows from the definition of totalization(4.8.6.9). □

Prop. (4.8.9.3) [Commutative Monoidal Structure on $K^*(\mathcal{A})$]. This monoidal functor descends to a strict monoidal structure on $K^*(\mathcal{A})$. ⌟

Proof: □

Prop. (4.8.9.4) [Tensoring is Exact]. Let $L^\bullet \in K(\mathcal{A})$, then tensoring functor $\mathrm{Tot}^{\oplus}(- \oplus L^\bullet)$ is an exact functor between triangulated categories. ⌟

Proof: □

Prop. (4.8.9.5). An R-module I is injective iff for any injective homomorphism from I to any R-module splits. ⌟

Proof: The critical point is that we can always embed I to an injective hull J by(4.8.3.23), then $J = I \oplus J'$, so I is clearly injective. □

Prop. (4.8.9.6) [K-Injective under Change of Rings]. If $R \to S$ is a ring map, then

1. If $R \to S$ is flat and $I^\bullet$ is a K-injective complex of S-modules, then $I^\bullet$ is K-injective as a complex of R-modules.
2. If $R \to S$ is surjective and $I^\bullet$ is a complex of S-modules that is K-injective as a complex of R-modules, then it is K-injective as a complex of S-modules.
3. If $I^\bullet$ is a K-injective complex of R-modules, then $\mathrm{Hom}_R(S, I^\bullet)$ is K-injective as a complex of S-modules.

⌟

Proof: 1: This is because $\mathrm{Hom}_{K(R)}(M^\bullet, I^\bullet) = \mathrm{Hom}_{K(S)}(M^\bullet \otimes_R S, I^\bullet)$ and(4.10.2.1), as tensoring S is exact.

2: This is because $\mathrm{Hom}_{K(R)}(N^\bullet, I^\bullet) = \mathrm{Hom}_{K(S)}(N^\bullet, I^\bullet)$ for a complex of S-modules $N^\bullet$ and(4.10.2.1).

3: This is because $\mathrm{Hom}_{K(S)}(N^\bullet, \mathrm{Hom}_R(S, I^\bullet)) = \mathrm{Hom}_{K(R)}(N^\bullet, I^\bullet)$, and(4.10.2.1). □

4.9 Stable ∞-Categories

References are [nLab], [Lur11]

Notation (4.9.0.1).

- Use notations defined in ∞-Categories.

⌟

1 Stable ∞-Categories

Def. (4.9.1.1) [Zero Objects]. A **zero object** in an ∞-category is an object that is both initial and final. A **pointed ∞-category** is an ∞-category with a zero object.

In a pointed ∞-category $\mathcal{C}$, the subcategory of zero objects is a trivial Kan complex. And for any $x, y \in \mathcal{C}$, $\mathrm{Map}(x, y)$(4.7.1.20) is a trivial Kan complex, by(4.5.8.3) and(4.7.1.21). So there is a **zero morphism** $0 : x \to y$ that is unique up to contractible choice. ⌟

Def. (4.9.1.2) [∞-Category of Pointed Objects]. For $\mathcal{C} \in \mathcal{C}\mathrm{at}_\infty$ with a final object $*$, denote $\mathcal{C}^{\mathrm{pt}} = \mathcal{C}_{*/}$, called the **∞-category of pointed objects** in $\mathcal{C}$. Then $\mathcal{C}_*$ is pointed, and there is a map $(-)_- : \mathcal{C}_* \to \mathcal{C}$, and there is also a map $(-)_+ : \mathcal{C} \to \mathcal{C}_*$ given by adding a final object. Then we have an adjunction between ∞-categories:

$$(-)_+ : \mathcal{C} \rightleftharpoons \mathcal{C}^{\mathrm{pt}} : (-)_-.$$

⌟

Proof:

□

Prop. (4.9.1.3). Let $\mathcal{C}$ be a pointed presentable ∞-category, then evaluation at $S^0 \in \mathcal{G}\mathrm{rpd}_\infty^{\mathrm{pt}}$ induces an equivalence of ∞-categories

$$\mathrm{Func}^L(\mathcal{G}\mathrm{rpd}_\infty^{\mathrm{pt}}, \mathcal{C}) \cong \mathcal{C}.$$

⌟

Proof:

□

Def. (4.9.1.4) [Triangles in ∞-Categories]. A **triangle** is a pointed ∞-category $\mathcal{C}$ is a diagram

$$\tau : \Delta^1 \times \Delta^1 \to \mathcal{C} : \begin{array}{ccc} x & \longrightarrow & y \\ \downarrow & \searrow & \downarrow \\ 0 & \longrightarrow & z \end{array}$$

where 0 is a zero object. It is called a **fiber sequence** if this diagram is a pullback diagram, and called a **cofiber sequence** if this diagram is a pushout diagram. Denote $\mathrm{Tri}(\mathcal{C}) \subset \mathrm{Func}(\Delta^1 \times \Delta^1, \mathcal{C})$ the full sub-∞-category of triangles. ⌟

Def. (4.9.1.5) [Cofiber Maps and Fiber Maps]. If $\mathcal{C}$ is a pointed ∞-category which admits cofibers, then by(4.7.3.16) and(4.7.3.17), there is a **fiber sequence map**

$$\mathrm{Cof} : \mathrm{Func}(\Delta^1, \mathcal{C}) \to \mathrm{Func}(\Delta^1 \times \Delta^1, \mathcal{C}).$$

unique up to contractible choice. And its composition with $\mathrm{ev}_{(1,1)}$ is also denoted by $\Sigma : \mathrm{Func}(\Delta^1, \mathcal{C}) \to \mathcal{C}$. The dual is true for fibrations. ⌟

Prop. (4.9.1.6) [Cofiber Map Preserves Colimits]. If $\mathcal{C}$ is a pointed ∞-category which admits cofibers, choose a zero object 0, then any $\mathrm{Cof}:\mathrm{Func}(\Delta^1,\mathcal{C})\to\mathcal{C}$ is left adjoint to a functor $\mathcal{C}\to\mathcal{C}_{0/}\to\mathrm{Func}(\Delta^1,\mathcal{C})$ which maps each $C\in\mathcal{C}$ to a morphism $0\to C$. In particular, Cof preserves small colimits by(4.7.4.5). Dually, Fib preserves small limits. ⌟

Proof: □

Def. (4.9.1.7) [Suspension and Loop Diagrams]. For $\mathcal{C}\in\mathcal{C}\mathrm{at}_\infty$, denote $\mathcal{C}^\Sigma\subset\mathrm{Func}(\Delta^1\times\Delta^1,\mathcal{C})$ the full ∞-subcategory of cofiber sequences of the form

$$\tau:\Delta^1\times\Delta^1\to\mathcal{C}:\quad \begin{array}{ccc} x & \longrightarrow & 0' \\ \downarrow & \searrow & \downarrow \\ 0 & \longrightarrow & z \end{array}$$

where $0,0'$ are zero objects.

Dually, define $\mathcal{C}^\Omega\subset\mathrm{Func}(\Delta^1\times\Delta^1,\mathcal{C})$ the full ∞-subcategory of exact triangles of the form

$$\tau:\Delta^1\times\Delta^1\to\mathcal{C}:\quad \begin{array}{ccc} x & \longrightarrow & 0' \\ \downarrow & \searrow & \downarrow \\ 0 & \longrightarrow & z \end{array}$$

where $0,0'$ are zero objects. ⌟

Def. (4.9.1.8) [Suspension Functors and Loop Functors]. If $\mathcal{C}\in\mathcal{C}\mathrm{at}_\infty$ is a pointed ∞-category with admits cofibers, then same argument as in(4.9.1.5) shows that $\mathcal{C}^\Sigma\to\mathcal{C}$ is a trivial Kan fibration, so there is a section $\Sigma:\mathcal{C}\to\mathcal{C}^\Sigma$, called a **suspension functor**. And its composition with $\mathrm{ev}_{(1,1)}$ is also denoted by $\Sigma:\mathcal{C}\to\mathcal{C}$.

Dually, if $\mathcal{C}$ is a pointed ∞-category which admits fibers, we can define **loop functors**. If $\mathcal{C}$ admits both fibers and cofibers, for $C\in\mathcal{C}$ and $n\in\mathbb{N}$, denote $X[n]=\Sigma^n(X),X[-n]=\Omega^n(X)$. ⌟

Def. (4.9.1.9) [Stable ∞-Category]. A **stable ∞-category** is a pointed ∞-category $(\mathcal{C},0)$ s.t.

- $\mathcal{C}$ admits cofibers and fibers.
- A triangle in $\mathcal{C}$ is a fiber sequence iff it is a cofiber sequence.

Notice that $\mathcal{C}$ is stable iff $\mathcal{C}^{\mathrm{op}}$ is stable. ⌟

Prop. (4.9.1.10). If $\mathcal{C}$ is a pointed category which admits both cofibers and fibers, then there is an adjunction

$$\Sigma:\mathrm{Ho}(\mathcal{C})\rightleftarrows\mathrm{Ho}(\mathcal{C}):\Omega.$$

And if $\mathcal{C}$ is stable, they are mutually inverse to each other. ⌟

Proof: □

Prop. (4.9.1.11) [HA.1.1.3.4]. A stable ∞-category is complete and cocomplete. And pullback squares and pushout squares coincide. ⌟

Prop. (4.9.1.12). Let $\mathcal{C}$ be a pointed ∞-category, then the following are equivalent:

- $\mathcal{C}$ is stable.
- $\mathcal{C}$ admits finite colimits, and the suspension functor $\Sigma:\mathcal{C}\to\mathcal{C}$ is an equivalence.
- $\mathcal{C}$ admits finite limits, and the loop functor $\Omega:\mathcal{C}\to\mathcal{C}$ is an equivalence.

⌟

Proof: Cf.[HA, 1.4.2.27]. □

Homological Algebra

Prop. (4.9.1.13) [Homotopy Groups]. Let $\mathcal{C}$ be a pointed ∞-category that admits cofibers, then for any $X, Y \in \mathcal{C}$, there is a bijection

$$\mathrm{Hom}_{\mathrm{Ho}(\mathcal{C})}(\Sigma^n(X), Y) \cong \pi_n \mathrm{Map}_{\mathcal{C}}(X, Y).$$

⌟

Proof: ? □

Def. (4.9.1.14) [Ext Groups]. For a pointed ∞-category $\mathcal{C}$ and $X, Y \in \mathcal{C}$, denote $\mathrm{Ext}^n(X, Y) = \mathrm{Hom}_{\mathrm{Ho}(\mathcal{C})}(X[-n], Y)$, called the **Ext groups**. ⌟

Prop. (4.9.1.15). Let $\mathcal{C}$ be a pointed ∞-category that admits cofibers, then any diagram

$$\begin{array}{ccc} X & \xrightarrow{f} & 0 \\ \downarrow & & \downarrow f' \\ 0' & \longrightarrow & Y \end{array}$$

in $\mathcal{C}$ corresponds to a homotopy class of morphisms $\theta \in \mathrm{Hom}_{\mathrm{Ho}(\mathcal{C})}(X[1], Y)$. Then in this way, the diagram diagram

$$\begin{array}{ccc} X & \xrightarrow{f'} & 0' \\ \downarrow & & \downarrow f' \\ 0 & \longrightarrow & Y \end{array}$$

corresponds to $-\theta \in \mathrm{Hom}_{\mathrm{Ho}(\mathcal{C})}(X[1], Y)$, where the group structure is given by(4.9.1.13). ⌟

Proof: Cf.[Lur11]P25. □

Lemma (4.9.1.16). Let $\mathcal{C}$ be a pointed ∞-category that admits cofibers, and the suspension functor Σ is an equivalence, then $\mathrm{Ho}(\mathcal{C})$ is an additive category(4.8.1.10). ⌟

Proof: It follows from(4.9.1.13) and the compatibility of group structures on π_n that $\mathcal{C}$ is preadditive. To show it is additive, Cf.[Lur11]P24.? □

Def. (4.9.1.17) [Distinguished Triangles]. Let $\mathcal{C}$ be a pointed ∞-category which admits cofibers, then a diagram $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} X[1]$ in $\mathrm{Ho}(\mathcal{C})$ is called a **distinguished triangle** if there exists a diagram $\Delta^1 \times \Delta^2 \to \mathcal{C}$ as shown:

$$\begin{array}{ccccc} X & \xrightarrow{\widetilde{f}} & Y & \longrightarrow & 0 \\ \downarrow & & \downarrow \widetilde{g} & & \downarrow \\ 0' & \longrightarrow & Z & \xrightarrow{\widetilde{h}} & W \end{array}$$

s.t.

- Both $0, 0'$ are zeros.
- both square are pushout squares.
- $\widetilde{f}$ lifts f, $\widetilde{g}$ lifts g.
- $h : Z \to X[1]$ equals $\widetilde{h}$ composed with an equivalence $W \cong X[1]$ determined by the outer rectangle.

⌟

Prop. (4.9.1.18) [Stable ∞-Categories and Triangulated Categories]. Let $\mathcal{C}$ be a stable ∞-category, then the translation functor defined(4.9.1.8) and distinguished triangles defined in(4.9.1.17) endow $\mathrm{Ho}(\mathcal{C})$ with the structure of a triangulated category(4.8.4.1). ⌟

Proof: Cf.[Lur11]P27. □

Def. (4.9.1.19) [Exact Functors]. An **exact functor** between stable ∞-categories is a functor $F : \mathcal{C} \to \mathcal{D}$ that is left and right exact and preserves fiber sequences. ⌟

Prop. (4.9.1.20). Let $\mathcal{C}\mathrm{at}_\infty^{\mathrm{Ex}} \subset \mathcal{C}\mathrm{at}_\infty$ be the subcategory of all stable ∞-categories and exact functors, then it admits all small limits and small filtered colimits, and they are preserved by the inclusion. ⌟

Proof: Cf.[HA1.1.4.4., 1.1.4.6.] □

Def. (4.9.1.21) [T-Structure]. A T-structure on a stable ∞-category $\mathcal{C}$ is a pair of full subcategories $\mathcal{C}_{\geq 0}.\mathcal{C}_{\leq 0}$ that ⌟

Prop. (4.9.1.22). For any $n \in \mathbb{Z}$, $\mathcal{C}_{\leq n} \subset \mathcal{C}$ is a localization, thus admits a left adjoint $\tau_{\leq n}$, called the **truncation functor**. Dually for $\tau_{\geq n}$. ⌟

Proof: Cf.[HA, P1.2.1.5]. □

Def. (4.9.1.23) [Heart]. The **heart** $\mathcal{C}^\heartsuit \subset \mathcal{C}$ is defined to be the full subcategory of $\mathcal{C}_{\leq 0} \cap \mathcal{C}_{\geq 0} \subset \mathcal{C}$. ⌟

Spectra Objects and Stabilization

Def. (4.9.1.24) [Spectra]. A **spectrum** is an object in the universal $(\infty, 1)$-category $\mathrm{Sp} = \mathrm{Sp}(\mathcal{T}\mathrm{op}) \cong \mathrm{Sp}(\mathcal{G}\mathrm{rpd}_\infty)$ ⌟

Def. (4.9.1.25) [Homology Groups of Spectra]. ⌟

Def. (4.9.1.26) [Connective Spectra]. A **connective spectrum** is a spectrum(4.9.1.24) that the negative homotopy groups vanish. ⌟

Prop. (4.9.1.27). There are equivalences between the following categories**?**:

- connected spectra.
- infinite loop spaces.
- group-like $\mathbb{E}_\infty$-spaces.

⌟

Proof: □

Def. (4.9.1.28) [$\mathbb{E}_\infty$-Rings]. An $\mathbb{E}_\infty$**-ring** is an object in $\mathcal{C}\mathcal{M}\mathrm{on}_\infty(\mathrm{Sp}(\mathcal{G}\mathrm{rpd}_\infty))$(4.9.1.24). ⌟

Cor. (4.9.1.29). For $(\mathcal{C}, 0) \in \mathcal{C}\mathrm{at}_\infty^{\mathrm{pt}}$, the following are equivalent:

- $\mathcal{C}$ is stable.
- $\mathcal{C}$ admits finite finite colimits and the suspension functor $\Sigma : \mathcal{C} \to \mathcal{C}$ is an equivalence.
- $\mathcal{C}$ admits finite finite limits and the loop functor $\Sigma : \mathcal{C} \to \mathcal{C}$ is an equivalence.

⌟

Proof: Cf.[Lur11]P149. □

Presentable Stable ∞-Categories

2 Monoidal ∞-Categories

Def. (4.9.2.1) [Monoidal ∞-Categories]. A **monoidal** $(\infty, 1)$**-category** is a tuple $(\mathcal{C}, \otimes)$ where

- $\mathcal{C}$ is a simplicial set.
- $\otimes : \mathcal{C} \to N(\Delta)^{\mathrm{op}}$ is a coCartesian fibration.
- For $n \in \mathbb{N}$ and $0 \leq i \leq n-1$, the induced $(\infty, 1)$-functor $\mathcal{C}_{[n]} \to \mathcal{C}_{\{i,i+1\}}$ determines an equivalence of $(\infty, 1)$-categories

$$\mathcal{C}_{[n]} \to \mathcal{C}_{\{0,1\}} \times \ldots \times \mathcal{C}_{\{n-1,n\}} \cong (\mathcal{C}_{[1]})^n$$

⌟

Def. (4.9.2.2) [$\mathbb{A}_\infty$-Rings]. Let $\mathcal{C}$ be a stable monoidal $(\infty, 1)$-category(4.9.2.1) with the $(\infty, 1)$-functor

$$p_\infty : \mathcal{C} \to N(\Delta)^{\mathrm{op}},$$

an $\mathbb{A}_\infty$**-Ring** is a lax monoidal section of $p_\otimes$. ⌟

Monoidal $(\infty, 1)$-Categories

Def. (4.9.2.3) [Symmetric Monoidal $(\infty, 1)$-Categories]. A symmetric monoidal $(\infty, 1)$-category is an $(\infty, 1)$-category which is ∞-tuply monoidal. Equivalently, it is a commutative algebra in the $(\infty, 1)$-category of $(\infty, 1)$-categories.

Or equivalently, it is a coCartesian fibration of simplicial sets

$$\pi : \mathcal{C}^\otimes \to N(\mathrm{fin}\,\mathcal{S}\mathrm{et}_*)$$

s.t. for any $n \in \mathbb{N}$, the associated functor $\mathcal{C}^\otimes_{[n]} \to \mathcal{C}^\otimes_{[1]}$ determines an equivalence of $(\infty, 1)$-categories. ⌟

Proof: ? □

Def. (4.9.2.4) [$\mathbb{E}_\infty$-Algebras(Commutative Monoids)]. Let $\mathcal{C}$ be a symmetric monoidal $(\infty, 1)$-category, then an $\mathbb{E}_\infty$**-algebra** of a **commutative monoid** in $\mathcal{C}$ is a lax monoidal $(\infty, 1)$-functor $* \to \mathcal{C}$?. The $(\infty, 1)$-category of commutative monoids in $\mathcal{C}$ is denoted by $\mathcal{CM}\mathrm{on}_\infty(\mathcal{C})$. ⌟

Def. (4.9.2.5) [$\mathbb{E}_\infty$-Space]. An $\mathbb{E}_\infty$**-space** is a commutative ∞-monoid in $\mathcal{G}\mathrm{rpd}_\infty$(4.7.2.5), i.e.

$$\mathbb{E}_\infty\text{-Spa} = \mathcal{CM}\mathrm{on}_\infty(\mathcal{G}\mathrm{rpd}_\infty).$$

It is also denoted by $\mathcal{CM}\mathrm{on}_\infty$. ⌟

Def. (4.9.2.6) [Commutative Ring Spectra($\mathbb{E}_\infty$-Rings)]. An $\mathbb{E}_\infty$**-ring** or a **commutative ring spectra** is a commutative monoid in the stable $(\infty, 1)$-category of spectra?. ⌟

Prop. (4.9.2.7) [∞-Abelianization]. There is an $(\infty, 1)$-functor

$$\mathcal{A}\mathrm{b}_\infty : \mathcal{G}\mathrm{rpd}_\infty \to \mathcal{CM}\mathrm{on}_\infty \text{(4.9.2.5)}$$

that is left adjoint to the ⌟

4.10 Derived Categories

Main references are [G-M03] and [Sta]. Need to be refreshed by the language of ∞-categories **?**

1 Derived Categories

Def. (4.10.1.1)[Derived Categories]. For $\mathcal{A} \in \mathcal{A}b\,\mathcal{C}at$, the full subcategory $Ac(\mathcal{A})$ of $K(\mathcal{A})$ consisting of acyclic complexes is a strictly full saturated triangulated subcategory, and its associated saturated localizing system is the class $\mathrm{QIso}(\mathcal{A})$ of quasi-isomorphisms.

Thus the kernel of the localizing functor $Q_{\mathcal{A}} : K(\mathcal{A}) \to \mathrm{QIso}(\mathcal{A})^{-1}K(\mathcal{A})$ is $Ac(\mathcal{A})$, and H^0 factors through $Q_{\mathcal{A}}$. Then the quotient triangulated category(4.8.4.25)

$$D(\mathcal{A}) = K(\mathcal{A})/Ac(\mathcal{A}) = \mathrm{QIso}(\mathcal{A})^{-1}K(\mathcal{A})$$

is called the **derived category** of $\mathcal{A}$. ⌟

Proof: As H^0 is a cohomological functor on $K(\mathcal{A})$(4.8.6.14), these follow from(4.8.4.27) and(4.8.4.26). □

Cor. (4.10.1.2) [Universal Properties of Derived Categories]. For $\mathcal{A} \in \mathcal{A}b\,\mathcal{C}at$,

- By(4.8.4.20), the derived category $D(\mathcal{A})$ of an Abelian category $\mathcal{A}$ has the universal property that any exact functor between Distinguished categories $F : K(\mathcal{A}) \to \mathcal{D}$ s.t. quasi-isomorphisms is mapped to isomorphisms uniquely factors through $D(\mathcal{A})$.
- Let $F : \mathcal{A} \to \mathcal{B}$ be an exact functor between Abelian categories, then F induces an exact functor $F : K(\mathcal{A}) \to K(\mathcal{B})$ of triangulated categories(4.8.6.17), and it maps quasi-isomorphisms to quasi-isomorphisms, so by item1 induces a morphism of categories $\mathcal{D}(\mathcal{A}) \to \mathcal{D}(\mathcal{B})$.

⌟

Prop. (4.10.1.3) [Universal δ-Functors]. The functor $\mathrm{Ch}^{\mathbb{Z}}(\mathcal{A}) \to D(A)$ is a δ-functor. ⌟

Proof: Cf.[Sta]014Z.**?** □

Prop. (4.10.1.4) [T-structures]. Let $\mathcal{A} \in \mathcal{A}b\,\mathcal{C}at$ and $K^\bullet \in K(\mathcal{A})$, then for any $a \in \mathbb{Z}$, truncations induces a distinguished triangle

$$\tau_{\leq a}K^\bullet \to K^\bullet \to \tau_{\geq a+1}K^\bullet \to \tau_{\leq a}K^\bullet[1].$$

In particular, $K(\mathcal{A})$ and $D(\mathcal{A})$ are triangulated categories with T-structures(4.8.5.1). ⌟

Proof: This distinguished triangle comes from the exact sequence $0 \to \tau_{\leq a}K^\bullet \to K^\bullet \to K^\bullet/\tau_{\leq a}K^\bullet$ via the δ-functor(4.10.1.3) and the fact $K^\bullet/\tau_{\leq a} \to K^\bullet \to \tau_{\geq a+1}K^\bullet$ is a quasi-isomorphism thus an isomorphism in $D(\mathcal{A})$. □

Triangulated Subcategories of $D(\mathcal{A})$

Prop. (4.10.1.5). Let $A \in \mathcal{A}b\,\mathcal{C}at$ and $\mathcal{L}$ a full triangulated subcategory of $K(\mathcal{A})$, let $S = \mathcal{L} \cap \mathrm{QIso}(\mathcal{A})$, then S is the saturated localizing system compatible with the triangulated structure associated to the cohomological functor H^0 restricted to L(4.8.4.19), the we can form the localizing triangulated category $S^{-1}\mathcal{L}$(4.8.4.20) and there is a natural exact functor of triangulated categories $S^{-1}\mathcal{L} \to D(\mathcal{A})$ by the universal property(4.8.4.20). ⌟

Prop. (4.10.1.6) [Full Subcategories of $D(\mathcal{A})$]. Let $\mathcal{L} \subset \widetilde{\mathcal{L}}$ be full triangulated subcategories of $K(\mathcal{A})$, and $S = \mathcal{L} \cap \mathrm{QIso}(\mathcal{A})$, $\widetilde{S} = \widetilde{\mathcal{L}} \cap \mathrm{QIso}(\mathcal{A})$. If either of the following holds:

- For any $s : L_1 \to \widetilde{L}_1 \in \widetilde{S}$ and $L_1 \in \mathcal{L}$, there is a morphism $t : \widetilde{L}_1 \to L_2$ that $L_2 \in \mathcal{L}$ and $t \circ s \in \widetilde{S}$.
- The same as in item1 but with arrows reversed.

then the natural functor $S^{-1}\mathcal{L} \subset \widetilde{S}^{-1}\widetilde{\mathcal{L}}$ is fully faithful. ⌟

Proof: This follows immediately from(4.10.1.5) and(4.8.4.22). □

Cor. (4.10.1.7) [Bounded Derived Categories]. For $* = -, +, b$, the triangulated categories $D^*(\mathcal{A})$ are the localized category of $K^*(\mathcal{A})$ at the classes of isomorphism in $K^*(\mathcal{A})$(4.10.1.5). Then they are naturally full subcategories of $D(\mathcal{A})$, by(4.10.1.6), as the condition is satisfied by(4.8.6.19). ⌟

Def. (4.10.1.8) [Derived Category of Serre Subcategories]. If $\mathcal{B}$ is a Serre subcategory of an Abelian category $\mathcal{A}$, let $D^*_{\mathcal{B}}(\mathcal{A})$ be the full subcategory of $D^*(\mathcal{A})$ consisting of objects X that $H^n(X) \in \mathcal{B}$ for all n, then $D^*_{\mathcal{B}}(\mathcal{A})$ is a strictly full saturated triangulated subcategory of $D^*(\mathcal{A})$, as it is just the kernel of the cohomological functor $H^0 : D^*(\mathcal{A}) \to \mathcal{A} \to \mathcal{A}/\mathcal{B}$(4.8.3.14)(4.8.4.16).

Also there are natural exact functors $D^*(\mathcal{B}) \to D^*_{\mathcal{B}}(\mathcal{A})$, and $D^*(\mathcal{A})/D^*_{\mathcal{B}}(\mathcal{A}) \to D^*(\mathcal{A}/\mathcal{B})$(4.8.4.25). ⌟

Prop. (4.10.1.9). The map $D^*(\mathcal{A}) \to D^*(\mathcal{A}/\mathcal{B})$ is essentially surjective. ⌟

Proof: Cf.[Sta]06XL. □

Prop. (4.10.1.10). Let $\mathcal{B} \subset \mathcal{A}$ be a Serre subcategory and suppose that for any surjection $X \to Y \in \mathcal{A}$ with $Y \in \mathcal{B}$, there is a subobject $X' \subset X$ that $X' \to Y$ is surjective, then the exact functor $D^*(\mathcal{B}) \to D^*_{\mathcal{B}}(\mathcal{A})$ is an equivalence for $* = -$ or b. ⌟

Proof: Cf.[Sta]0FCL. □

Prop. (4.10.1.11). If $(\mathcal{C}, \mathcal{O})$ is a ringed site and $\mathcal{A} \subset \mathfrak{Mod}_{\mathcal{O}}$ is the Serre subcategory of torsion modules, then the functor $D(\mathcal{A}) \to D_{\mathcal{A}}(\mathcal{O})$ is an equivalence. ⌟

Proof: Cf.[Sta]0DD7. □

Prop. (4.10.1.12) [Embedding of $\mathcal{A}$ in $D(\mathcal{A})$]. For $A \in \mathcal{A}\mathrm{b}\,\mathfrak{Cat}$, the natural inclusion $i : \mathcal{A} \subset D(A)$ induces an equivalence of $\mathcal{A}$ with the subcategory of $D(\mathcal{A})$ consisting of complexes with cohomology concentrated at degree 0.

An object $K \in D(A)$ is called **discrete** if it is in the essential image of this inclusion. ⌟

Proof: The natural map $H^0 : D(\mathcal{A}) \to \mathcal{A}$ is inverse to i, so i is faithful. To show it is full, let (L, f, s^{-1}) be a morphism from $i(M)$ to $i(N)$, then we get a morphism $(H^0(L), H^0(f), H^0(s)^{-1})$, and these two morphisms are both dominated by the morphism $(\sigma^{\geq n}L, \sigma^{\leq n} \circ f, (\sigma^{\leq n} \circ s)^{-1})$, so they are equal morphisms in $D(\mathcal{A})$. But $(H^0(L), H^0(f), H^0(s)^{-1}) = i(s^{-1}f)$ is in the image of i, so i is full.

The assertion that any complex with cohomology groups concentrated at degree 0 is true by using truncation functors(4.8.6.19). □

Prop. (4.10.1.13) [K-Groups]. For $A \in \mathcal{A}\mathrm{b}\,\mathfrak{Cat}$, the embedding(4.10.1.12) induces an isomorphism of K-groups $K_0(\mathcal{A}) \cong K_0(D^b(\mathcal{A}))$(10.1.2.1). ⌟

Proof: The map $\mathcal{A} \to D^b(\mathcal{A})$ is a δ-functor by(4.10.1.3), thus by(10.1.2.2) induces a map $K_0(\mathcal{A}) \cong K_0(D^b(\mathcal{A}))$. There is a reverse map $K_0(D^b(\mathcal{A})) \to K_0(\mathcal{A}) : X \mapsto \sum_i (-1)^i H^i(X)$, which is inverse the the map above: one direction is clear, for the other, use induction and the truncation triangles(4.10.1.4). □

Def. (4.10.1.14) [Perfect Complex]. Let $\mathcal{A}$ be an Abelian category, a **perfect complex** in $D(\mathcal{A})$ is a complex that is equivalent to a bounded complex. ⌟

Operations on the Derived Category

Lemma (4.10.1.15) [Direct Sum]. If $\mathcal{A} \in \mathcal{A}b\,\mathcal{C}at$ has exact countable direct sums, then $D(\mathcal{A})$ has countable direct sums given by term-wise direct sums. ⌟

Proof: A system of morphisms $K_i^\bullet \to L^\bullet$ is a system of quasiisos $M_i^\bullet \to K_i^\bullet$ and $M_i \to L^\bullet$. Then by hypothesis $\oplus M_i^\bullet \to \oplus K_i^\bullet$ is a quasi-iso, thus defines a morphism $\oplus K_i^\bullet \to L^\bullet$. It can be verified that this morphism is unique**?**. □

Lemma (4.10.1.16) [Termwise Colimit as Hocolim]. Let $\mathcal{A} \in \mathcal{A}b\,\mathcal{C}at$ and $L_n^\bullet$ be a system of complexes of $\mathcal{A}$. Assume colimits over $\mathbb{N}$ exists and are exact over $\mathcal{A}$, then the termwise colimit $L^\bullet$ is a derived colimit in $D(\mathcal{A})$. ⌟

Proof: We have an exact sequence

$$0 \to \oplus L_n^\bullet \to \oplus L_n^\bullet \to L^\bullet \to 0$$

and the termwise direct sum is the direct sum in $D(\mathcal{A})$ by(4.10.1.15), and then $L^\bullet$ is a derived colimit, by(4.8.6.13). □

Bounded (Co)Homological Dimensions

Def. (4.10.1.17)[Bounded Cohomological Dimensions]. An exact functor between two derived categories $F : D(\mathcal{A}) \to D(\mathcal{B})$ is called has **cohomological dimension bounded by** N if $F(D^{\leq m}(\mathcal{A})) \subset D^{\leq m+N}(\mathcal{B})$. Dually, it has **homological dimension bounded by** N if $F(D^{\geq m}(\mathcal{A})) \subset D^{\geq m-N}(\mathcal{B})$. ⌟

Prop. (4.10.1.18). If $(F, G) : D(\mathcal{A}) \to D(\mathfrak{B})$ is an adjunction pair of exact functors, then F has cohomological dimension bounded by N iff G has homological dimension bounded by N. ⌟

Proof: If F has cohomological dimension bounded by N, let $K \in D^{\geq m}(\mathcal{B})$, then

$$\mathrm{Hom}_{D(\mathcal{A})}(\tau_{\leq m-N-1} GK, GK) = \mathrm{Hom}_{D(\mathcal{B})}(F\tau_{\leq m-N-1} GK, K) = 0.$$

The dual case is similar. □

2 K-injectives and K-Adapted Classes

Prop. (4.10.2.1) [K-injectives]. For an Abelian category $\mathcal{A}$, a complex $I^\bullet$ in $K(\mathcal{A})$ is called a **K-injective** object iff it satisfies the following equivalent conditions:

- $\mathrm{Hom}_{K(\mathcal{A})}(S^\bullet, I^\bullet) = 0$ for any acyclic $S^\bullet$ in $K(\mathcal{A})$.
- $\mathrm{Hom}_{K(\mathcal{A})}(N^\bullet, I^\bullet) \cong \mathrm{Hom}_{K(\mathcal{A})}(M^\bullet, I^\bullet)$ for quasi-iso $M^\bullet \to N^\bullet$.

- $\mathrm{Hom}_{K(\mathcal{A})}(X^\bullet, I^\bullet) \cong \mathrm{Hom}_{D(\mathcal{A})}(X^\bullet, I^\bullet)$ for every $X^\bullet$. In particular, a quasi-iso between two K-injective objects is an isomorphism in $K(\mathcal{A})$.
  Dually, we can define **K-projective** objects.

⌟

Proof: $1 \to 2$ is by(4.8.6.14); $2 \to 3$ use(4.10.1.7), for $3 \to 1$, notice any acyclic complex is quasi-iso to 0. □

Cor. (4.10.2.2). K-Injectives form a full triangulated subcategory of $K(\mathcal{A})$. ⌟

Cor. (4.10.2.3). If $I^\bullet$ is K-injective and quasi-isomorphic to an object in $K^+(\mathcal{A})$, then $I^\bullet \in K^+(\mathcal{A})$. ⌟

Cor. (4.10.2.4) [K-Injective Resolutions are Unique]. by item3 of the definition(4.10.2.1), K-injective resolutions are unique in $K(\mathcal{A})$. ⌟

Prop. (4.10.2.5) [Injectives and K-Injective]. Objects $K^+(\mathcal{I}_\mathcal{A})$ are all K-injectives. thus the injective resolution is unique in K^+. Dually $K^-(\mathcal{P})$ are all K-projectives. ⌟

Proof: Use the first definition of K-injectives(4.10.2.1), we prove any morphism $f : S^\bullet \to I^\bullet$ from an acyclic complex to a K-injective $I^\bullet$ is homotopic to 0 by a homotopy h. Let $I_k = 0$ for $k < n$, choose $h_k = 0$ for $k \le n$, then $f_k = dh_k + h_{k+1}d$ for $k < n$. We use induction on n to find $h_k, k \le n$ that $f_k = dh_k + h_{k+1}d$ for $k < n$ Suppose h_k are constructed for $k \le n$, for $n+1$, $(f_n - dh_n)d = f_nd - df_{n-1} = 0$, thus $f_n - dh_n = h_{n+1}d$ for some h_{n+1} as I_n is injective. Then we are done. □

Prop. (4.10.2.6). If a functor f between Abelian categories is left adjoint to an exact functor, then it preserves K-injectives (use definition1). ⌟

Prop. (4.10.2.7) [Products of K-Injectives]. Let $\mathcal{A}$ be an Abelian category, I_t be K-injective complexes. If the termwise product of I_t exists, then it is also K-injective, and is the products of I_t in $D(\mathcal{A})$. ⌟

Proof: It is clearly K-injective by(4.10.2.1) item1 as it is the product in the category $K(\mathcal{A})$. Thus we can easily use the (4.10.2.1) item3 to see that $I^\bullet$ is also the product in the category $D(\mathcal{A})$. □

Lemma (4.10.2.8). [Sta]070M ⌟

Prop. (4.10.2.9) [Functorial K-injective Resolution]. If $\mathcal{A}$ is an Abelian category having enough injectives and exact countable products, then every complex is quasi-isomorphic to a K-injective complex that each term is injective.

Moreover, if $\mathcal{A}$ is a Grothendieck category, then the K-injective resolution can be chosen to be functorial. ⌟

Remark (4.10.2.10). Maybe this can be extended to any large enough class of elements, at least for $K^+(\mathcal{A})$. ⌟

Proof: By(4.10.2.8), it suffices to show that $K \to R\lim \tau_{\ge -n}K$ is a quasi-isomorphism for all complex K. But this is clear from the distinguished triangle

$$R\lim \tau_{\ge -n}K \to \prod \tau_{\ge -n}K \to \prod \tau_{\ge -n}K \to R\lim \tau_{\ge -n}K[1]$$

and the fact $H^p(\prod \tau_{\ge -n}K) = \prod_{p \ge -n} H^p(K)$.

For the second assertion, Cf.[Sta]079P.? □

K-Adapted Classes

Def. (4.10.2.11) [K-Adapted Classes]. Let $\mathcal{A}$ be an Abelian category, $\mathcal{D}$ a triangularized category and $F : K(\mathcal{A}) \to \mathcal{D}$ a triangularized functor, a **K-adapted class** for F is a full triangulated subcategory $\mathcal{R} \subset K(\mathcal{A})$ that

- If $I \to I'$ is a quasi-isomorphism in $\mathcal{R}$, then $F(I) \to F(I')$ is an isomorphism in $\mathcal{D}$.
- Every $A^\bullet \in K(\mathcal{A})$ admits some quasi-isomorphism $A^\bullet \to I^\bullet$ where $I^\bullet \in \mathcal{R}$.

$\lrcorner$

Cor. (4.10.2.12) [K-Injective is K-Adapted]. If $\mathcal{A}$ has sufficiently many K-injectives, then the class of K-injectives is K-adapted to any left exact functor F, by(4.10.2.2) and(4.10.2.1). $\lrcorner$

3 Derived Functors

Def. (4.10.3.1)[Right Derived Functors]. Let $\mathcal{A}$ be an Abelian category, E a triangularized category and $F : K(\mathcal{A}) \to \mathcal{D}$ an exact functor between triangulated categories. Then a **right derived functor** of F is an exact functor $RF : D(\mathcal{A}) \to \mathcal{D}$ together with a natural transformation $\eta : F \to RF \circ Q_{\mathcal{A}}$ that satisfies the following universal property: For any exact functor $G : D(\mathcal{A}) \to \mathcal{D}$ and a natural transformation $\eta' : F \to G \circ Q_{\mathcal{A}}$, there is a natural transformation $\theta : RF \to G$ that $\eta' = (\theta \star Q_{\mathcal{A}}) \circ \eta$.

In particular, if RF exists, then it is unique up to unique isomorphism of exact functors. $\lrcorner$

Prop. (4.10.3.2) [Derived Functors via K-Adapted Classes]. Let $\mathcal{A}$ be an Abelian category, $\mathcal{D}$ a triangularized category and $F : K(\mathcal{A}) \to E$ an exact functor, if there exists a K-adapted class $\mathcal{R}$ for F, then RF exists. Moreover, for $I \in \mathcal{R}$, the morphism $\eta_I : F(I) \to RF \circ Q_{\mathcal{A}}(I)$ is an isomorphism in $\mathcal{D}$. $\lrcorner$

Proof: Let $S = \mathcal{R} \cap \mathrm{QIso}(\mathcal{A})$, then $\mathcal{R}, K(\mathcal{A})$ and the localizing systems $S, \mathrm{QIso}(\mathcal{A})$ satisfy the conditions in(4.10.1.6), so $\iota : S^{-1}\mathcal{R} \subset D(\mathcal{A})$ is a full triangulated subcategory, and it is also essentially surjective, thus it is an equivalence of categories. Let I be a right adjoint of the inclusion, then I is also an exact functor(4.8.4.9), and there is a natural isomorphism $\zeta : \mathrm{id}_{D(\mathcal{A})} \cong \iota \circ I$.

By the universal property, there is an exact functor $F_{\mathcal{R}} : S^{-1}\mathcal{R} \to \mathcal{D}$ extending $F|_{\mathcal{R}}$. Define

$$RF = F_{\mathcal{R}} \circ I : D(\mathcal{A}) \to \mathcal{D}.$$

To construct $\eta : F \to RF \circ Q_{\mathcal{A}}$, for any $X \in \mathrm{Ob}(K(\mathcal{A})) = \mathrm{Ob}(D(\mathcal{A}))$, the isomorphism ζ gives an isomorphism $X \cong \iota(I(X))$, which is represented by a roof $(R, f, s^{-1}), f, s \in \mathrm{QIso}(\mathcal{A})$, and we can assume $R \in \mathrm{Ob}(\iota(S^{-1}\mathcal{R})) = \mathrm{Ob}(\mathcal{R})$ by hypothesis, thus $s \in S$, and $F(s)$ is an isomorphism in E by hypothesis. Thus we get a morphism $\eta_X : F(s)^{-1} \circ F(f) : F(X) \to F(\iota(I(X))) = RF(Q_{\mathcal{A}}(X))$. This η_X is independent of the representation given, because if there is another dominant roof $(R', t \circ f, (t \circ s)^{-1})$, where $t : R \to R' \in S$, then $F(t \circ s)^{-1} \circ F(t \circ f) = F(s)^{-1} \circ F(f) \in E$.

And for a morphism $f : X \to Y \in K(X)$, ζ gives a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\zeta_X} & \iota(I(X)) \\ \downarrow f & & \downarrow \iota(I(f)) \\ Y & \xrightarrow{\zeta_Y} & \iota(I(Y)) \end{array}$$

in $D(\mathcal{A})$ where ζ_X, ζ_Y are represented by $(R_X, f_X, s_X^{-1}), (R_Y, f_Y, s_Y^{-1})$, and $I(f)$ is represented (R_0, f_0, s_0^{-1}), then we can construct roof to realize this commutative diagram in $K(\mathcal{A})$ and show there is a commutative diagram

$$\begin{array}{ccc} F(X) & \xrightarrow{F(s_X)^{-1}\circ F(f_X)} & RF(Q_{\mathcal{A}}(X)) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle F(s_0)^{-1}\circ F(f_0)=RF\circ Q_{\mathcal{A}}(f)} \\ F(Y) & \xrightarrow{F(s_Y)^{-1}\circ F(f_Y)} & RF(Q_{\mathcal{A}}(Y)) \end{array}$$

in E, which means $\eta : F \to RF \circ Q_{\mathcal{A}}$ is a natural isomorphism.

Notice that η_I is an isomorphism for $I \in \mathcal{R}$, because in this case $F(f_I), F(s_I)$ are both isomorphisms.

It remains to show the universal properties of η: Given any exact functor $G : D(\mathcal{A}) \to E$ and a natural transformation $\eta' : F \to G \circ Q_{\mathcal{A}}$, for any $X \in \mathrm{Ob}(K(\mathcal{A})) = \mathrm{Ob}(D(\mathcal{A}))$, we get a morphism $\eta'_X : F(X) \to G(X)$ in E. Notation as before, because η' is a natural transformation, we get a commutative diagram in $K(\mathcal{A})$

$$\begin{array}{ccc} F(X) & \xrightarrow{\eta'_X} & G(X) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(Q_{\mathcal{A}}(f))} \\ F(R_X) & \xrightarrow{\eta'_{R_X}} & G(R_X) \\ \uparrow{\scriptstyle F(s)} & & \uparrow{\scriptstyle G(Q_{\mathcal{A}}(s))} \\ F(\iota(I(X))) & \xrightarrow{\eta'_{\iota(I(X))}} & G(\iota(I(X))) \end{array}$$

In E. As $\zeta_X = (R_X, f, s^{-1})$ is an isomorphism between X and $\iota(I(X))$, f, s are both quasi-isomorphisms, thus the vertical arrows are both isomorphisms, and we get a commutative diagram

$$\begin{array}{ccc} F(X) & \xrightarrow{\eta'_X} & G(X) \\ \downarrow{\scriptstyle \eta_X} & & \downarrow{\scriptstyle G(\zeta_X)} \\ RF(Q_{\mathcal{A}}(X)) & \xrightarrow{\eta'_{\iota(I(X))}} & G(\iota(I(X))) \end{array}.$$

So we can define

$$\theta_X = (G(\zeta_X))^{-1} \circ \eta'_{\iota(I(X))} : RF(Q_{\mathcal{A}}(X)) \to G(X),$$

then it is is functorial in X as both $\eta'_{\iota(I(X))}$ and $G(\zeta_X)$ are functorial in X, so defines a natural transformation $RF \circ Q_{\mathcal{A}} \to G$ that $(\theta \star Q_{\mathcal{A}}) \circ \eta = \eta'$.

For the uniqueness of η: For any $X \in \mathrm{Ob}(S^{-1}\mathcal{R}) = \mathrm{Ob}(\mathcal{R})$, η_X is an isomorphism, thus η_X is determined, but $\iota : S^{-1}\mathcal{R} \to D(\mathcal{A})$ is essentially surjective, so η_X is determined for any $X \in D(\mathcal{A})$. □

Cor. (4.10.3.3) [Derived Functors via K-Injective Classes]. Let $\mathcal{A}$ be an Abelian category, E a triangularized category and $F : K^*(\mathcal{A}) \to E$ an exact functor, if $K^*(\mathcal{A})$ has enough K-injectives, then the class of K-injectives is K-adapted to F(4.10.2.12), so $RF : D^*(\mathcal{A}) \to E$ exists. Moreover, for any K-injective $I^\bullet$, the morphism $\eta_{I^\bullet} : F(I^\bullet) \to RF \circ Q_{\mathcal{A}}(I^\bullet)$ is an isomorphism in E ⌟

Cor. (4.10.3.4) [Derived Functors via Injectives]. Let $\mathcal{A}, \mathcal{B}$ be Abelian categories s.t $\mathcal{A}$ has enough injective and countable products, and $F : \mathcal{A} \to \mathcal{B}$ an additive functor, then $K^*(F) : K^*(\mathcal{A}) \to D^*(\mathcal{A})$ is an exact functor by**??**, and $K^*(\mathcal{A})$ has enough K-injectives by(4.10.2.9).

However, this is useless unless F is left exact in which case we see $R^0F(A) = F(A)$ for any $A \in \mathcal{A}$ by(4.10.3.3). ⌟

Cor. (4.10.3.5) [Naturality]. If $\eta : F \to F'$ is a natural transformation of left-exact functors, then by universal property(4.10.3.1), there is a natural transformation $R\eta : RF \to RF'$ inducing a long exact sequence about cohomology groups extending η. ⌟

Prop. (4.10.3.6) [Composition of Derived Functors]. $\mathcal{A}, \mathcal{B}$ be Abelian categories and $\mathcal{D}$ a triangulated category. If $F : K^*(\mathcal{A}) \to K^*(\mathcal{B}), G : K^*(\mathcal{B}) \to \mathcal{D}$ are exact functors between triangulated categories, and $\mathcal{R}_{\mathcal{A}}$ is K-adapted to F and $G \circ F$, $\mathcal{R}_{\mathcal{B}}$ is K-adapted to G, then the natural transformation $R(G \circ F) \to RG \circ RF$ is an isomorphism. ⌟

Proof: RF is isomorphic to F on $\mathcal{R}_{\mathcal{A}}$, so for any $A^\bullet \in K^*(\mathcal{A})$, choose some quasi-isomorphism $A^\bullet \to R$, where $R \in \mathcal{R}_{\mathcal{A}}$, then there is a commutative diagram

$$\begin{array}{ccccc} R(G \circ F)(A^\bullet) & \xrightarrow{\cong} & R(G \circ F)(R) & \xrightarrow{\cong} & G \circ F(R) \\ \downarrow & & \downarrow & & \downarrow \text{id} \\ RG \circ RF(A^\bullet) & \xrightarrow{\cong} & RG \circ RF(R) & \xrightarrow{\cong} & G \circ F(R) \end{array}$$

$$G \circ F(R) \cong G(F(R)) \to RG(F(I^\bullet)) \cong RG \circ RF(A^\bullet),$$

and we are done. □

Def. (4.10.3.7) [Universal δ-Functors]. A **universal δ-functor** between Abelian categories is one that any natural transformation from T^0 to another δ-functor will generate a δ-map. A **effaceable δ-functor** is one that for any $n > 0$ and any object A, there is an injection $A \to B$ that $T^n(A) \to T^n(B) = 0$. ⌟

Prop. (4.10.3.8) [Grothendieck]. A δ-functor is universal if it is effaceable. ⌟

Proof: We construct by induction on n. choose a $0 \to A \to B \to C \to 0$ such that $T^{n+1}(A) \to T^{n+1}(B) = 0$ then there is an isomorphism $T^{n+1}(A) \cong \text{Coker}(T^n(B) \to T^n(C))$, and so we can construct the map on T^{n+1} induces by

$$\text{Coker}(T^n(B) \to T^n(C)) \to \text{Coker}(G^n(B) \to G^n(C)) \to G^{n+1}(A).$$

This can be verified to be a δ map. □

Prop. (4.10.3.9). The derived functors form a universal δ-functor (when it exists). ⌟

Proof: It is a δ functor by(4.10.1.1), it is universal by(4.10.3.8). □

Prop. (4.10.3.10). Derived functor commutes with filtered colimits on a Grothendieck Abelian category, this is by $AB5$. ⌟

Prop. (4.10.3.11) [Hypercohomology]. Given an Abelian category $\mathcal{A}$ with enough injectives, $\mathcal{B}$ a complete Abelian category, $F : \mathcal{A} \to \mathcal{B}$ a left exact functor, and $K \in \mathcal{K}(\mathcal{A})$, we can define the **right**

hyper-derived functor of F at K as $\mathbb{R}F(K) = \mathrm{Tot}^{\Pi}F(P) \in K(\mathcal{B})$ where $K \to P$ is a Cartan-Eilenberg resolution of K. and the **hypercohomologies** of F at K as $R^nF(K) = H^n(\mathrm{Tot}^{\Pi}F(P))$. Dually we can define the left hyper-derived functor and hyperhomologies.

For complexes in $K^+(\mathcal{A})$, there is no restriction and the right derived-hyper functor descends to a functor from $D^+(\mathcal{A}) \to D^+(\mathcal{B})$.

When the Abelian category $\mathcal{A}$ satisfies AB3* and AB4*, i.e. the direct product is exact, then Tot^{Π} of the Cartan-Eilenberg resolution of any complex is a quasi-isomorphism to it by the dual of(4.8.8.11). (Take horizontal filtration, AB4* assures it collapse). ⌟

Derived Bifunctors

Def. (4.10.3.12) [Right Derived Functors of Bi-Exact Bi-Functors]. Let $\mathcal{A}, \mathcal{B}$ be Abelian categories and $F : K(\mathcal{A}) \times K(\mathcal{B}) \to \mathcal{D}$ be bi-exact bifunctor between triangulated categories, a **right derived functor** of F is a bi-exact bifunctor $RF : D(\mathcal{A}) \times D(\mathcal{B}) \to \mathcal{D}$ together with a natural transformation $\eta : F \to RF \circ (Q_{\mathcal{A}} \times Q_{\mathcal{B}})$ that satisfies the following universal property: For any bi-exact bifunctor $G : \mathcal{D}(\mathcal{A}) \times \mathcal{D}(\mathcal{B}) \to \mathcal{D}$ and a natural transformation $\eta' : F \to G \circ (Q_{\mathcal{A}} \times Q_{\mathcal{B}})$, there is a natural transformation $\theta : RF \to G$ that $\eta' = (\theta \star (Q_{\mathcal{A}} \times Q_{\mathcal{B}})) \circ \eta$.

In particular, if RF exists, then it is unique up to unique isomorphisms of bi-exact bi-functors. ⌟

Prop. (4.10.3.13)[Deriving Bi-Exact Functors]. Let $\mathcal{A}_1, \mathcal{A}_2$ be Abelian categories and $F : K(\mathcal{A}_1) \times K(\mathcal{A}_2) \to \mathcal{D}$ be bi-exact bifunctor between triangulated categories, if $\mathcal{R}_i$ are full subcategories of $\mathcal{A}_i$ s.t.

- If $R_i \to R_i'$ are quasi-isomorphisms in $\mathcal{R}_i$, the induced map $F(R_1, R_2) \to F(R_1', R_2')$ is an isomorphism in $\mathcal{D}$.
- Any $A_i^\bullet \in K(\mathcal{A}_i)$ admits some quasi-isomorphism $A_i^\bullet \to \mathcal{I}_i^\bullet$ where $I_i^\bullet \in \mathcal{R}_i$.

Then the right derived functor(4.10.3.12) RF exists. Moreover, for any $R_i \in \mathcal{R}_i$, $\eta_{R_1,R_2} : F(R_1, R_2) \to RF \circ (Q_{\mathcal{A}_1} \times Q_{\mathcal{A}_2})(R_1, R_2)$ is an isomorphism. ⌟

Proof: Let $S_i = \mathcal{R}_i \cap \mathrm{QIso}(\mathcal{A}_i)$, then $\mathcal{R}_i, K(\mathcal{A}_i)$ and the localizing systems $S_i, \mathrm{QIso}(\mathcal{A}_i)$ satisfy the conditions in(4.10.1.6), so $\iota : S_i^{-1}\mathcal{R}_i \subset D(\mathcal{A}_i)$ is a full triangulated subcategory, and it is also essentially surjective, thus it is an equivalence of categories. Let I_i be a right adjoint of the inclusion, then I_i is also an exact functor(4.8.4.9), and there is a natural isomorphism $\zeta_i : \mathrm{id}_{D(\mathcal{A}_i)} \cong \iota_i \circ I_i$.

By hypothesis of universal properties, the functor F extends to an exact functor $F_{\mathcal{R}} : \prod_i S_i^{-1}\mathcal{R}_i \to \mathcal{D}$. Define

$$RF = F_{\mathcal{R}} \circ \prod_i \mathcal{I}_i : \prod_i D(\mathcal{A}_i) \to \mathcal{D}.$$

The rest of the proof is verbatim as that of(4.10.3.2). □

Remark (4.10.3.14). This proposition can be naturally extended to any multi-exact multi-functors. In fact, I suppose this can be deduced from the usual derived functors by considering the tensor product category $\mathcal{A} \otimes \mathcal{B}$, Cf.[Basic Concepts of Enriched Category Theory, Kelly]. ⌟

Prop. (4.10.3.15)[Derived Functors of Adjunctions]. Let $\mathcal{A}_1, \mathcal{A}_2$ be Abelian categories and (F, G) be an adjunction between $K(\mathcal{A}_1)$ and $K(\mathcal{A}_2)$, and $\mathcal{R}_i$ are full subcategories of $\mathcal{A}_i$ s.t.

- If $R_i \to R_i'$ are quasi-isomorphisms in $\mathcal{R}_i$, the induced map $F(R_1', R_2) \to \mathrm{Hom}^\bullet_{\mathcal{B}}(R_1, R_2')$ is an isomorphism in $D(\mathcal{A}b)$.
- Any $A_1^\bullet \in K(\mathcal{A}_1)$ admits some quasi-isomorphism $A_1^\bullet \to I_1^\bullet$ where $I_1^\bullet \in \mathcal{R}_1$.

- Any $A_2^\bullet \in K(\mathcal{A}_2)$ admits some quasi-isomorphism $I_1^\bullet \to A_2^\bullet$ where $I_2^\bullet \in \mathcal{R}_2$.

then there is a functorial isomorphism

$$R\operatorname{Hom}(LF(A^\bullet), B^\bullet) \cong R\operatorname{Hom}(A^\bullet, RG(B^\bullet)) \in D(\mathcal{A}\mathrm{b})$$

for $A^\bullet \in K(\mathcal{A}), B^\bullet \in K(\mathcal{B})$. In particular,

$$\operatorname{Hom}(LF(A^\bullet), B^\bullet) \cong \operatorname{Hom}(A^\bullet, RG(B^\bullet)) \in \mathcal{A}\mathrm{b}$$

⌟

Proof: Regard both side as a right derived functor of the isomorphic bi-exact bi-functors

$$K(\mathcal{A})^{op} \times K(\mathcal{B}) \to D(\mathcal{A}\mathrm{b}) : (A^\bullet, B^\bullet) \mapsto \operatorname{Hom}^\bullet_{\mathcal{B}}(F(A^\bullet), B^\bullet) \cong \operatorname{Hom}_{\mathcal{A}}{}^\bullet(A^\bullet, G(B^\bullet)) \in D(\mathcal{A}\mathrm{b}).$$

Then the functorial isomorphism follows from universal properties. □

Prop. (4.10.3.16). Situation as in(4.10.3.15), for any $K^\bullet \in K(\mathcal{A}_2)$, there is a commutative diagram of adjunction maps

$$\begin{array}{ccc} LF \circ G(K^\bullet) & \longrightarrow & F \circ G(K^\bullet) \\ \downarrow & & \downarrow \\ LF \circ RG(K^\bullet) & \longrightarrow & K^\bullet \end{array}$$

⌟

Proof: Cf.[Sta]0FPI. □

<u>**Internal Hom**</u>

Def. (4.10.3.17) [Internal Hom]. If $\mathcal{A}$ is an Abelian category and $K(\mathcal{A})$ has enough K-injectives or enough K-projectives, thus by(4.10.3.13), we can define the **internal Hom**

$$R\operatorname{Hom} : D(\mathcal{A})^{op} \times D(\mathcal{A}) \to D(\mathcal{A})$$

as the right derived functor of the bi-exact bifunctor $\operatorname{Hom}^\bullet : K(\mathcal{A})^{op} \times K(\mathcal{A}) \to D(\mathcal{A}\mathrm{b})$. ⌟

Prop. (4.10.3.18) [Ext Groups]. For $X, Y \in D(\mathcal{A})$, define the **ext groups**

$$\operatorname{Ext}^i_{\mathcal{A}}(X, Y) = H^i(R\operatorname{Hom}(X, Y)) = \operatorname{Hom}_{D(\mathcal{A})}(X[0], Y[i]).$$

⌟

Proof: To show $H^i(R\operatorname{Hom}(X, Y)) = \operatorname{Hom}_{D(\mathcal{A})}(X[0], Y[i])$, choose a K-injective resolution $Y \to I^\bullet$ of Y, then

$$H^i(R\operatorname{Hom}(X, Y)) = H^i(\operatorname{Hom}^\bullet(X, I^\bullet)) = \operatorname{Hom}_{K(\mathcal{A})}(X, I^\bullet[n]) = \operatorname{Hom}_{D(\mathcal{A})}(X, I^\bullet[n]) = \operatorname{Hom}_{D(\mathcal{A})}(X, Y[n])$$

by(4.8.6.10) and the definition(4.10.2.1). □

Prop. (4.10.3.19). If $P^\bullet \to X^\bullet$ is a projective resolution, then $\operatorname{Ext}^i(X^\bullet, Y^\bullet) = \operatorname{Hom}_{K(\mathcal{A})}(P^\bullet[-i], Y^\bullet)$. If $Y^\bullet \to I^\bullet$ is an injective resolution, then $\operatorname{Ext}^i(X^\bullet, Y^\bullet) = \operatorname{Hom}_{K(\mathcal{A})}(X^\bullet, I^\bullet)$. ⌟

Prop. (4.10.3.20). If $X \in D^{\leq a}(\mathcal{A})$ and $Y \in D^{\geq b}(\mathcal{A})$, then for $i < b-a$, $\mathrm{Ext}^i(X,Y) = 0$, and $\mathrm{Ext}^{b-a}(X,Y) = \mathrm{Hom}(H^a(X), H^b(Y))$.

In particular, for $A, B \in \mathcal{A}$, $\mathrm{Ext}^i(A,B) = 0$ for $i < 0$ and $\mathrm{Ext}^0(A,B) = \mathrm{Hom}(A,B)$. ⌟

Proof: This is because X can be represented by $K^{\leq a}(\mathcal{P})$ or Y can be represented by $K^{\geq b}(\mathcal{I})$. □

Prop. (4.10.3.21) [Long Exact Sequences]. Let $0 \to A_1 \to A_2 \to A_3 \to 0$ be an exact sequence in $\mathcal{A}$, then it is distinguished in $D(\mathcal{A})$, so by(4.8.4.12), for any $B \in \mathcal{A}$, there is a long exact sequence

$$0 \to \mathrm{Hom}(B, A_1) \to \mathrm{Hom}(B, A_2) \to \mathrm{Hom}(B, A_3) \to \mathrm{Ext}^1(B, A_1) \to \mathrm{Ext}^1(B, A_2) \to \ldots,$$

and similarly a long exact sequence

$$0 \to \mathrm{Hom}(A_3, B) \to \mathrm{Hom}(A_2, B) \to \mathrm{Hom}(A_1, B) \to \mathrm{Ext}^1(A_3, B) \to \mathrm{Ext}^1(A_2, B) \to \ldots.$$

⌟

Def. (4.10.3.22) [Yoneda Extensions]. Let $\mathcal{A}$ be an Abelian category and $A, B \in \mathcal{A}$, a **Yoneda extension** of B by A of degree d is an exact sequence

$$0 \to A \to Z_{d-1} \to \ldots \to Z_0 \to B \to 0.$$

One Yoneda extension is said to **dominate** another if there is a map of extensions s.t. restricts to id_A and id_B. Two Yoneda extensions of degree d is called **equivalent** if they are dominated by a common Yoneda extension.(Notice this is an equivalence relation by(4.10.3.23)). ⌟

Prop. (4.10.3.23) [Ext and Yoneda Extensions]. There is a map from the equivalence classes of Yoneda extensions of degree d of B over A to $\mathrm{Ext}^d(B,A)$, which maps the exact sequence $0 \to A \to Z_{d-1} \to \ldots \to Z_0 \to B \to 0$ to $fs^{-1} \in \mathrm{Hom}_{D(\mathcal{A})}(B[0], A[d])$, where $f : (A \to Z_{d-1} \to \ldots \to Z_0) \to A[d]$, and $s : (A \to Z_{d-1} \to \ldots \to Z_0) \to B[0]$.

and corresponds to the set of i-term extensions of Y by X. There is a natural map

$$\mathrm{Ext}^i_{\mathcal{A}}(X,Y) \times \mathrm{Ext}^i_{\mathcal{A}}(Y,Z) \to \mathrm{Ext}^{i+j}_{\mathcal{A}}(X,Z)$$

by composition or equivalently the conjunction of extensions. ⌟

Proof: Cf.[Sta]06XU. □

Prop. (4.10.3.24)[Explicit Addition as Extensions]. In an Abelian category with enough injectives, the extension $\mathrm{Ext}^1(N,M)$ is equivalent with the Abelian group of extensions with Baer sum as addition. ⌟

Proof: We choose a projective resolution $0 \to K \to P \to N \to 0$, so $\mathrm{Hom}(K,M) \to \mathrm{Ext}^1(N,M)$ is surjective, so choose a lifting and the pushout $0 \to M \to L \to N \to 0$ with be the corresponding extension, Now the Baer sum is easy to define and verify. □

Prop. (4.10.3.25). If $\mathcal{A}$ is an Abelian category and $p \geq 0$ s.t. $\mathrm{Ext}^p(A,B) = 0$ for any $A, B \in \mathcal{A}$, then $\mathrm{Ext}^i(A,B) = 0$ for any $i \geq p$ and $A, B \in \mathcal{A}$. ⌟

Proof: Any Yoneda extension of degree i is a conjunction of extensions of degree p and degree $i-p$. □

Cor. (4.10.3.26). If $\mathcal{A}$ is an Abelian category s.t. $\mathrm{Ext}^2(A,B)=0$ for any $A,B\in\mathcal{A}$, then each object of $D^b(\mathcal{A})$ is isomorphic to a direct sum of cohomologies. ⌟

Proof: Let K be represented by $K^\bullet\in D^{[a,b]}(\mathcal{A})$. We use induction on $b-a$. If $b-a>0$, then there is a distinguished triangle $\tau_{\le b-1}K\to K^\bullet\to H^b(K)[-b]\to\tau_{\le b-1}K^\bullet[1]$(4.10.1.4). If we can prove $H^b(K)[-b]\to\tau_{\le b-1}K^\bullet[1]$ is 0, then we finish by(4.8.4.4). But by induction and the hypothesis,

$$\mathrm{Hom}_{D(\mathcal{A})}(H^b(K)[-b],\tau_{\le b-1}(K^\bullet)[1])=\oplus_{i<b}\mathrm{Ext}_{\mathcal{A}}^{b-i+1}(H^b(K),H^i(K)),$$

which vanishes by hypothesis. □

Acyclic Objects

Prop. (4.10.3.27) [F-Acyclic Objects]. For a left exact functor F, an object X is (right)F-acyclic if RF is defined for X, and the natural map $F(X)\to RF(X)$ is an isomorphism, or equivalently $R^iF(X)=0$ for all $i>0$.

Then there is an adapted class of F iff the class of F-acyclic objects $Acy(F)$ is sufficiently large, and in this case adapted classes of F are exactly sufficiently large subclasses of $Acy(F)$, and $Acy(F)$ contains all injectives(But the class of injectives may not be sufficiently large!). ⌟

Proof: Cf.[Gelfand P195]. □

Prop. (4.10.3.28) [Leray's Acyclicity Lemma]. Let $F:\mathcal{A}\to\mathcal{B}$ be an additive functor and RF is everywhere defined, then for a complex $A^\bullet$ in $K^+(\mathcal{A})$ consisting of F-acyclic objects, the natural map $F(A^\bullet)\to RF(A^\bullet)$ is an isomorphism. ⌟

Proof: Cf.[Sta]015E. This may be equivalent to(4.10.3.27). □

Prop. (4.10.3.29) [Acyclic Criterion]. Let F be a left exact functor from an Abelian category $\mathcal{C}$ of enough injectives to another Abelian category, T is a class of objects of $\mathcal{C}$ that satisfies:

- T is sufficiently large.
- Cokernel of maps between elements of T is in T and $0\to F(A)\to F(A')\to F(\mathrm{Coker})\to 0$ is exact. (To use induction).

Then every object of T is F-acyclic. ⌟

Proof: Cf.[[Sta]05T8]. □

Prop. (4.10.3.30) [Injectives are adapted]. By(4.10.2.5), if $\mathcal{A}$ contains sufficiently many injectives, then injective objects are adapted to any left exact functor F. (Because id on acyclic injective complexes is homotopic to 0 by the lemma). ⌟

4 $D_\infty(R)$

5 (Co)Homological Dimension

Prop. (4.10.5.1). If $\mathcal{A}$ has enough projectives, then the projective dimension of an object X is the length of projective resolutions. (Use resolution and long sequence). ⌟

Prop. (4.10.5.2) [Hilbert Theorem]. For an Abelian category $\mathcal{A}$, the category $\mathcal{A}[T]$ is an Abelian category. If $\mathcal{A}$ has enough projectives and have infinite direct sum, then $\mathrm{dhp}_{\mathcal{A}[T]}(X,t)\le\mathrm{dhp}_{\mathcal{A}}(X)+1$ and equality with $t=0$. ⌟

Cor. (4.10.5.3). The Categories $\mathcal{A}$b and $K[X]$-mod have homological dimension 1. $K[X_i,\dots,X_k]$ has homological dimension k. ⌟

Def. (4.10.5.4) [Injective Amplitude]. Let $\mathcal{A}$ be an Abelian category with enough injectives, $K \in D(A)$ is said to have **finite injective dimension** if $K \in D^b(\mathcal{I})$. It is said to have **injective amplitude in** $[a,b]$ if $K \in D^{[a,b]}(\mathcal{I})$. ⌟

Prop. (4.10.5.5). Let $\mathcal{A}$ be an Abelian category and $K \in D(\mathcal{A})$,

- If $K \in D^b(\mathcal{A})$ and $H^i(K)$ all have finite injective dimensions, then K also has finite injective dimension.
- If K is represented by $K^\bullet \in K^b(\mathcal{A})$, and K^i all have finite injective dimensions, then K also has finite injective dimension.

⌟

Proof: 1 follows from the Grothendieck spectral sequence applied to the functor $\mathrm{Hom}(N,-)$ for any $N \in \mathcal{A}$ and the CE resolution of K(4.8.8.10).

2 follows from 1 as we can use induction to show all $H^i(K)$ has finite injective dimensions. □

6 Derived Limits and Colimits

Def. (4.10.6.1) [Derived (Co)Limits]. Let $\mathcal{D}$ be a triangulated category, and (K_n, f_n) is an inverse system of objects in $\mathcal{D}$, then an object K is called the **derived colimit** of it iff there $\oplus K_n$ exists and there is a distinguished triangle

$$\oplus K_n \to \oplus K_n \to K \to \oplus K_n[1]$$

where the first map is given by $(1-f_n)$. By TR1, the derived colimit exists as long as $\oplus K_n$ exists, and by TR3(4.8.4.12), the colimit is unique if it exists. And by TR3 again a morphism of systems induces a morphism of colimits.

The definition of **derived limit** is dual. ⌟

Prop. (4.10.6.2)[Cofinality of Hocolim]. Let $\mathcal{D}$ be a triangulated category and (K_n, f_n) be a system, if $0 \le n_{i_0} < n_{i_1} < \dots$ be a sequence of integers, then there is an isomorphism $ho\,\mathrm{colim}\, K_{n_i} \to ho\,\mathrm{colim}\, K_n$. ⌟

Proof: Cf.[[Sta]0CRJ]. □

Lemma (4.10.6.3). Let $\mathcal{A}$ be an Abelian category with countable products and enough injectives, then the derived limit $R\lim$ for any inverse system in $D^+(\mathcal{A})$ exists. ⌟

Proof: It suffices to show $\prod K_i^\bullet$ exists in $D(\mathcal{A})$. But every $K_n^\bullet$ has a K-injective resolution $I_n^\bullet$, by(4.8.8.10)(4.10.2.5). And then $\prod K_n^\bullet$ is represented by $\prod I_n^\bullet$, by(4.10.2.7). □

Def. (4.10.6.4) [Rlim]. Rlim on an Abelian category $\mathcal{A}$ with countable products and enough injectives is defined to be the right derived functor of $\lim : \mathcal{A}^{\mathbb{N}} \to \mathcal{A}$. Equivalently, it is just the derived limit(4.10.6.1)(4.10.6.3) in $D(\mathcal{A})$ restricted to the case where each K_n is discrete. ⌟

Prop. (4.10.6.5). Let $R\lim A$ exists on $\mathcal{A}$, if K_n, f_n is a system of objects in $D^+(\mathcal{A})$, then there are exact sequences

$$0 \to R^1\lim(H^m(K_n), f_n) \to R^{m+1}\lim(K_n, f_n) \to \lim(H^m(K_n), f_n) \to 0.$$

Immediately from the definition(4.10.6.1). ⌟

7 Spectral Sequence

Reference for this section is [Weibel Ch5]. All the definition below is dual for homology and cohomology, just rotate the diagram 180 degree.

We work in an Abelian category.

Def. (4.10.7.1). A convergent **Spectral Sequence** is a three-dimensional arrange of entries $E_r^{p,q}$ that:

1. $d_r : E_r^{p,q} \to E_r^{p+r,q-r+1}$ that $d_r d_r = 0$.
2. $H^{p,q}(E_r^{p,q}) \cong E_{r+1}^{p,q}$. And $E_r^{p,q}$ has a direct limit $E_\infty^{p,q}$.
3. There is a complex $E^\bullet$ and a decreasing bounded filtration F^pE^n on each E^n and $E_\infty^{p,q} \cong F^pE^{p+q}/F^{p+1}E^{p+q}$.

⌟

Def. (4.10.7.2) [Notations For Cohomological Spectral Sequence].

- The cohomology filtration is called **bounded below** $F^{n_s}E^n = 0$ for some n_s, it is called **bounded above** $F^{n_s}E_n = E^n$ for some n^s.
- The cohomology filtration is called **exhaustive** iff $\cup F^iE^n = E^n$.
- The spectral sequence is called **regular** iff $d_{pq}^r = 0$ for sufficiently large r.
- A spectral sequence is said to **weakly converges** to $E^\bullet$ if there is a filtration

  $$\ldots \subset F^tH^n \subset F^{t-1}H^n \subset \ldots \subset F^sH^n \subset \ldots \subset H^n$$

  that $E_\infty^{pq} \cong F^pH^{p+q}/F^{p+1}H^{p+q}$.
- A spectral sequence **approaches** $E^\bullet$ if it weakly converges to $E^\bullet$.
- A spectral sequence **converges** to $E^\bullet$ if it approaches $E^\bullet$, it is regular, and $E^n = \varprojlim(E^n/F^pE^n)$.
- If a first quadrant spectral sequence converges to $E^\bullet$, then the morphisms $E_0^{n,0} \to E_\infty^{n,0} \subset E^n$ and $E^n \to E_\infty^{0,n} \to E_0^{0,n}$ are called the **edge morphisms**.

⌟

Prop. (4.10.7.3) [Notation for Filtrations on Homological Complexes]. Let $C_\bullet$ be a complex and $\ldots \subset F_{p-1}C \subset F_pC \subset \ldots \subset C$ be filtrations of complexes. Then it is called **exhaustive** if $C = \cup F_pC$. It is called **Hausdorff** if $\cap F_pC = 0$. It is called **complete** if $C = \varprojlim C/F_pC$. ⌟

Def. (4.10.7.4) [Spectral Sequence of a Filtered Complex]. For a complex $K^\bullet$ and a filtration F^pK^n on K^n, we have a natural spectral sequence

$$E_1^{pq} = H^{p+q}(F^pE^{p+q}/F^{p+1}E^{p+q}), \quad E^n = H^n(K^\bullet), \quad F^pE^n = H^n(F^pK^\bullet).$$

For a morphism of filtered complexes that are isomorphism for some r, induction on the exact sequence $0 \to F^pE^n \to F^{p+1}E^n \to E_\infty^{p,n-p}$ and use five-lemma shows it induces isomorphism on H^*E. ⌟

Prop. (4.10.7.5) [Comparison Theorem]. For a morphism F between two convergent spectral sequences, if it is an isomorphism for some r, then it induce isomorphism on the infinite homologies. ⌟

Proof: Clearly F induces isomorphisms on $E_\infty^{p,q}$. Because there are exact sequence

$$0 \to F^{p+1}H^n \to F^pH^n \to E_\infty^{p,n-p} \to 0$$

we can use five lemma and induction to show that F induces isomorphisms on F^pH^n/F^sH^n. Then because $H^n = \cup F^pH^n$, we can take colimit to show F induces isomorphisms on H^n/F^sH^n, then take inverse limits, we are done. □

Prop. (4.10.7.6) [Classical Convergence]. If the filtration on a complex $C_\bullet$ is bounded below and exhaustive for all C_n, then there is a spectral sequence that is also bounded below and converges to $H_\bullet(C_\bullet)$. ⌟

Proof: Cf[Gelfand P203] for cohomological case and [Weibel P135] for homological case. □

Prop. (4.10.7.7) [Complete convergence]. If the filtration is complete, exhaustive and the spectral sequence is regular, then the spectral sequence weakly converges to $H_\bullet(C_\bullet)$. And if it is also bounded above, then it converges to $H_\bullet(C_\bullet)$. ⌟

Proof: Cf.[Weibel, P139]. □

There are two examples, the stupid filtration and the canonical filtration, the canonical filtration is natural and factors through $D(\mathcal{A})$.

Prop. (4.10.7.8) [Spectral Sequence of a Double Complex]. A double complex has two natural filtration of the total complex, they defines two spectral sequence, one has

$$E_{2,x}^{p,q} = H_x^p(H_y^{\bullet,q}(L^{\bullet,\bullet}))$$

and the other has

$$E_{2,y}^{p,q} = H_y^p(H_x^{q,\bullet}(L^{\bullet\bullet})).$$

Cf.[Gelfand P209]. In fact under reflection, there is only one spectral sequence. For the horizontal filtration, the differential goes vertical first, for the vertical filtration, the differential goes horizontal first. The differential goes one way, the convergence goes reversely.

If both the filtration is finite and bounded, in particular if E is in the first quadrant, then they both converges to $H^n(E)$, this will generate important consequences. ⌟

Cor. (4.10.7.9). If a double complex in the first quadrant has its all column acyclic (3rd-quadrant pointing), then the total complex is acyclic. Thus a morphism of double complex inducing quasi-isomorphism on each column induces a quasi-isomorphism on the total complex.

If a double complex has $H_p(C_{*,q}) = 0, \forall p > 0, q$, then

$$H_n(\mathrm{Tot}C_{*,*}) = H_n(\mathrm{Coker}(C_{1,*} \to C_{0,*})$$

⌟

Prop. (4.10.7.10)[Horizontal Filtration]. For a second-quadrant-free homology double complex, the filtration is bounded below and exhaustive for $\mathrm{Tot}^\oplus$, so the classical convergence(4.10.7.6) applies and there is a convergence

$$E_{p,q}^2 = H_p^hH_q^v(C) \Rightarrow H_{p+q}\mathrm{Tot}^\oplus(C).$$

For a fourth-quadrant free homology double complex, the filtration is complete and exhaustive for Tot^Π, so the complete convergence(4.10.7.7) applies and there is a weak convergence

$$E_{p,q}^2 = H_p^hH_q^v(C) \Rightarrow H_{p+q}\mathrm{Tot}^\Pi(C).$$

⌟

Cor. (4.10.7.11) [Grothendieck Spectral Sequence]. If $\mathcal{A},\mathcal{B},\mathcal{C}$ be Abelian categories, $\mathcal{B}$ have enough injectives and $F : K^+(\mathcal{A}) \to K^+(\mathcal{B}), G : K^+(\mathcal{B}) \to K^+(\mathcal{C})$ are exact functors between triangulated categories. If $\mathcal{R}_\mathcal{A}$ is adapted to $F, G\circ F$, then for any $X^\bullet \in K^+(\mathcal{A})$, there is a spectral sequence convergence(to upper left)

$$E_2^{p,q} = R^pG(R^qF(X)) \Longrightarrow E^n = R^n(G\circ F)(X).$$

And if $\mathcal{R}_\mathcal{A} = \mathcal{I}_\mathcal{A}$, this spectral sequence is functorial in $X^\bullet$.

In particular, this applies to the case that F is right adjoint to an exact functor and both $\mathcal{A},\mathcal{B}$ have enough injectives. ⌟

Proof: Choose a functorial injective resolution $X \mapsto I_X^\bullet$(4.10.2.9), let $K^\bullet = F(I_X^\bullet) = RF(X)$, and choose a functorial CE resolution of $K^\bullet$(4.8.8.10), because the resolutions for $B^i \to Z^i \to H^i$ and $Z^i \to K^i \to B^{i+1}$ split and G is additive, we have

$$H_x^{q,\bullet}(G(L^{\bullet,\bullet})) = G(H_x^{q,\bullet}(L^{\bullet,\bullet})) = RG(H^q(K))$$

So

$$E_{2,y}^{p,q} = H_y^p(H_x^{q,\bullet}(L^{\bullet\bullet})) = R^pG(H^q(K)) = R^pG(R^qF(X))$$

and

$$E^\bullet = RG(\mathrm{Tot}(L)) = G(\mathrm{Tot}(L)) = RG(K) = RG\circ RF(X) \cong R(G\circ F)(X)\text{(4.10.3.6)}.$$

□

Cor. (4.10.7.12). The low degree parts read:

$$0 \to R^1G(F(A)) \to R^1(G\circ F)(A) \to G(R^1F(A)) \to R^2(G)(F(A)) \to R^2(G\circ F)(A).$$

(Check definition). More generally, if $R^pG(R^qF(A)) = 0, 0 < q < n$, then

$$R^mG(F(A)) \cong R^m(G\circ F)(A) \quad m < n$$

And

$$0 \to R^nG(F(A)) \to R^n(G\circ F)(A) \to G(R^nF(A)) \to R^{n+1}G(F(A)) \to R^{n+1}(G\circ F)(A).$$

⌟

Remark (4.10.7.13). The Grothendieck spectral sequence is very important. ⌟

Cor. (4.10.7.14) [Spectral Sequence for Hypercohomologies]. For chain complex K in $K^+(\mathcal{A})$ and a left exact functor F, the CE resolution will generate two spectral sequences by(4.10.7.10):

$$E_{2,x}^{p,q} = H_x^p(R^qF(A)) \Rightarrow \mathbb{R}^{p+q}(A), \text{when } A \text{ is bounded below}$$

$$E_{2,y}^{p,q} = (R^pF)(H^q(A)) \Rightarrow \mathbb{R}^{p+q}(A).\text{weakly convergent}$$

where the RHS is the hypercohomologies(4.10.3.11). ⌟

4.11 Differential Graded Algebras

Main references are [Ker] and [Sta].

Def. (4.11.0.1)[Differential Graded Algebras]. A **differential graded algebra** or *DGA* is a chain complex $A^\bullet$ of R-modules with R-linear maps $A^m \times A^n \to A^{m+n}$ that

$$d(ab) = d(a)b + (-1)^n ad(b).$$

that makes $\oplus A^n$ into an associative and unital R-algebra.

Notice the first condition is equivalent to giving a map $\mathrm{Tor}(A^\bullet \times_R A^\bullet) \to A$.

For a differential algebra $A^\bullet$, a right **differential module** is defined naturally. The tensor operation gives a closed symmetric monoidal structure $\mathcal{M}_A$.

Notice a usual R-algebra A can be seen as a differential graded algebra as $A^0 = A$ and $A^n = 0$ for $n > 0$.

And as in the case of chain complexes, the category of differential modules over A can be given a derived category. ⌟

Def. (4.11.0.2). A differential graded algebra $A^\bullet$ is called **commutative** if $ab = (-1)^{\deg(a)\deg(b)}ba$. It is called **strictly commutative** if moreover $a^2 = 0$ for $\deg(a)$ odd. ⌟

Def. (4.11.0.3). For two differential graded algebras A, B, the tensor graded algebra $A^\bullet \otimes B^\bullet$ is given by the $\mathrm{Tor}(A^\bullet \otimes_R B^\bullet)$. ⌟

1 dg-Categories

Def. (4.11.1.1) [dg-Categories]. Given a DGA A, a **dg-category** over A is a category enriched over the monoidal category $\mathcal{M}_A$(4.11.0.1). Let $dgCat_A$ denote the category of small dg-categories over A where morphisms are given by monoidal functors. ⌟

Def. (4.11.1.2) [Homotopy Categories]. Because H^0 and Z^0 are right-lax monoidal functors from $\mathrm{Ch}(R)$ to $\mathrm{Mod}(R)$, given a dg-category $\mathcal{C}$, by transferring, we can get categories $H^0(\mathcal{C})$ and $Z^0(C)$ enriched over $\mathcal{M}\mathrm{od}_{A^0}$. ⌟

Def. (4.11.1.3) [Equivalences]. A morphism between dg-categories are called an **equivalence** if induces quasi-isomorphisms on all hom-complexes. ⌟

Prop. (4.11.1.4) [Model Category of dg-Categories]. There is a cofibrantly generated model category on $dgCat_A$, where weak equivalences are quasi-equivalences and the fibrations are morphisms $F : \mathcal{A} \to \mathcal{B}$ that:

- induces component-wise surjections on hom-complexes.
- given an isomorphism $g : F(X) \to Y \in H^0(\mathcal{B})$, there is an isomorphism in $H^0(\mathcal{A})$ lifting g.

This monoidal structure is induced from that of the case $A = R$ and the right-lax monoidal functor $Ch(R) \to \mathcal{M}(A)$ given by $M^\bullet \mapsto A \otimes M$. ⌟

Proof: Cf.[Tabuada, Gon calo. Une structure de catgorie de modles de Quillen sur la catgorie des dg- catgories. C. R. Acad. Sci. Paris Sr. I Math. 340 (1) (2005), 15-19. (2005), 3309?3339.] □

2 Sheaves of DGAs

4.12 Topology II

1 Topological Groups

Def. (4.12.1.1). A **topological group** is a group object in the category of groups(4.1.1.66). ⌟

Prop. (4.12.1.2). If U is a nbhd of 1 in a topological group, then there is a nbhd V of 1 that $VV \subset U$. ⌟

Proof: Consider the map $G \times G \to G$ continuous, and it maps $(1, 1)$ to $1 \in U$, so the preimage of U contains a nbhd of $(1, 1)$, thus some $V_1 \times V_2$, then choose $V = V_1 \cap V_2$. □

Prop. (4.12.1.3). Let G be a connected topological group, then for any nbhd U of e, $G = \bigcup_{n=1}^{\infty} (U \cup U^{-1})^n$. In particular, any open subgroup of G equals G. ⌟

Proof: This is because the RHS is an open subgroup of G, so all its cosets in G are also open, so it equals G as G is connected. □

Prop. (4.12.1.4) [Separating Axioms]. For a topological group G, the following are equivalent:

- e is a closed pt.
- G is T_1.
- G is Hausdorff(T_2).
- G is regular.
- G is completely regular

⌟

Proof: □

Prop. (4.12.1.5). Hausdorff topological group is completely regular. ⌟

Proof: Use a sequence of neighbourhood of identity to construct a uniform metric on G. Then set $\phi(x) = \min\{1, 2\sigma(a, x)\}$. Cf.[Abstract Harmonic Analysis Ross §8.4] □

Prop. (4.12.1.6). For a compact subset K and a nbhd U of e in a topological group, there exists a nbhd V of e that $xVx^{-1} \subset U$ for any $x \in K$. ⌟

Proof: For any x, there exists a nbhd W_x of x and a nbhd V_x of e that $txt^{-1} \in U$ for any $t \in W_x$ and $y \in V_x$. Let f.m. W_{x_i} cover K, then $V = \cap V_{x_i}$ satisfies the condition. □

Prop. (4.12.1.7). A compact open nbhd of e in a Hausdorff topological group contains an open subgroup of G. ⌟

Proof: Cf.[Etale Cohomology Fulei P147] □

Prop. (4.12.1.8)[Homogenous Space]. Let G be a topological group and H a closed subgroup. G/H is the quotient space in the quotient topology(4.4.1.9), then it is Hausdorff. ⌟

Proof: If $\overline{x} \neq y$, then consider a preimage $xy^{-1} \in G \backslash H$, then we can find some open subset V that $VV \subset G \backslash H$ by(4.12.1.2), thus $\overline{x} + \overline{V} \cap \overline{y} + \overline{V} = \varnothing$. Hence G/H is Hausdorff. □

Group Actions

Prop. (4.12.1.9) [Quotient by Group Action is Open]. Let $G \times X \to X$ be a group action, then the quotient map $\pi : X \to X/G$ is open. ⌟

Proof: This is because the $\pi^{-1}(\pi(U)) = \bigcup_{g\in G} gU$. □

Def. (4.12.1.10) [Regular Action]. An **regular action** is an action $\gamma : G \times X \to X$ that satisfies the following equivalent conditions:

- the graph of γ in $X \times X$ is closed.
- The diagonal $\Delta_{X/G} \subset X/G \times X/G$ is closed.
- X/G is Hausdorff.

⌟

Proof: $2 \iff 3$ is clear, for $1, 2$, notice $X/G \times X/G \cong (X \times X)/(G \times G)$, and the inverse image of Δ in $X \times X$ is just the graph of γ. □

Def. (4.12.1.11) [Proper Action]. A **proper action** is an action $\gamma : G \times X \to X$ that the graph map $\Gamma : G \times X \to X \times X$ is a proper map. ⌟

Prop. (4.12.1.12) [Proper Action is Regular]. A proper action of a group G on a locally compact Hausdorff space X is a regular action. ⌟

Proof: This follows from(4.4.2.12). □

Def. (4.12.1.13) [Proper Discontinuous Actions]. A group action is called **proper discontinuous** iff any elements $x, y \in H$ there are nbhds U_x, U_y that $\{g \in G | g(U_x) \cap U_y \neq \varnothing\}$ is finite. ⌟

Def. (4.12.1.14) [Covering Space Action]. A **covering space action** is action of a topological group G on a topological space Y is called if for any $y \in Y$, there is a nbhd U that $g(U) \cap U = \varnothing$ if $g \neq 1$. ⌟

Prop. (4.12.1.15) [Characterization of Proper Actions]. Let $\gamma : G\times X \to X$ be a group action that X is Hausdorff, then γ is a proper action iff any $K \subset X$ compact, the set $G_K = \{g \in G | g(K) \cap K \neq \varnothing\}$ is compact. ⌟

Proof: Let $\Gamma : G \times X \to X \times X$ be the graph.

$1 \to 2$: $G_K = \pi_1(\Gamma^{-1}(K \times K))$, thus it is compact.

$2 \to 1$: Let $L \subset M \times M$ be compact, then $L \subset \pi_1(L) \times \pi_2(L)$, and L is closed. Let $K = \pi_1(L) \cup \pi_2(L)$, then $\Gamma^{-1}(L) \subset \Gamma^{-1}(\pi_1(L) \times \pi_2(L)) \subset G_K \times K$, which is a closed subset of a compact set, so $\Gamma^{-1}(L)$ is compact, and Γ is a proper map. □

Prop. (4.12.1.16). If G is a compact topological group, then any group action $\gamma : G \times X \to X$ on a Hausdorff space X is proper. ⌟

Prop. (4.12.1.17) [Orbit of Proper Maps]. Let θ be a proper action of G on a Hausdorff space X, then each orbit map $\theta^{(p)}$ is proper. In particular, if X is locally compact, then the orbits are all closed(4.4.2.12). ⌟

Proof: For any compact subset $K \subset X$, $(\theta^{(p)})^{-1}(K)$ is closed by continuity and is contained in $G_{K\cup\{p\}}$, thus is compact. □

Prop. (4.12.1.18) [Properly Discontinuous Map is Proper]. If G acts proper discontinuously on a topological space H, then for any compact subsets $K_1, K_2 \in H$, $\{g \in G | K_2 \cap g(K_1) \neq \varnothing\}$ is finite. In particular, if H is Hausdorff, then it is a proper action. ⌟

Proof: Notice for any two points we can find nbhds that f.m. g intersects these two nbhds, so we can use the compactness to find f.m. pair of nbhds to cover K_2, and then use these nbhds to cover K_1 and finite the proof. □

Prop. (4.12.1.19) [Proper Free Action is a Covering Space Action]. Let $G \times X \to X$ be a proper free action on a locally compact Hausdorff space, then it is a covering space action. ⌟

Proof: For any $p \in X$, choose a precompact nbhd U of x, then $G_{\overline{U}}$ is finite, then shrink U. □

Prop. (4.12.1.20) [Continuity]. Let a topological group G acts freely and properly on a space X. If G and X/G are both connected, then X is connected. ⌟

Proof: If U, V are open subsets of X that $U \cap V = \varnothing, U \cup V = X$, then $\pi(U), \pi(V)$ are open by(4.12.1.9). Now $\pi(U) \cap \pi(V) = \varnothing$, because otherwise there is a G-orbit of X intersecting both U and V, contradiction the fact G is connected. Then $\pi_1(U) = \varnothing$ of $\pi(V) = \varnothing$, thus $U = \varnothing$ or $V = \varnothing$, and X is connected. □

Def. (4.12.1.21) [Constructible Action]. An action of a topological group G on a topological space X is called **constructible** if its graph is constructible in $X \times X$(4.12.3.10). ⌟

Prop. (4.12.1.22). Let $\gamma : G \times X \to X$ be an action

- γ is constructible iff the diagonal $\Delta_{X/G} \subset X/G \times X/G$ is constructible.
- If γ is constructible and X is non-empty, then there is a G-invariant open subset $U \subset X$ that G acts regularly.
- For a constructible action, each G-orbit is locally closed.

⌟

Proof: Cf.[Bernstein-Zelevinsky, P54]. □

Totally Disconnectedness

Prop. (4.12.1.23). A compact topological group is totally disconnected iff the intersection of all compact open nbhds of e equals $\{e\}$. ⌟

Proof: If it is totally disconnected, then $\{1\}$ is closed, so G is Hausdorff(4.12.1.4), so by(4.4.1.25), the assertion is true. Conversely, if the intersection of all compact open nbhds of e equals $\{e\}$, then $\{1\}$ is closed because G is a group. □

Prop. (4.12.1.24). A precompact nbhd of a e in a totally disconnected topological group contains a compact open subgroup. ⌟

Proof: Cf.[Etale Cohomology Fulei P147]. □

2 Hausdorff Geometry

Def. (4.12.2.1). The **Hausdorff distance** for two subset $Y_1, Y_2 \in X$ is the

$$d_X^H(Y_1, Y_2) = \inf\{\varepsilon | Y_2 \subset B(Y_1, \varepsilon), Y_1 \subset B(Y_2, \varepsilon)\}.$$

The **Gromov-Hausdorff metric** for two metric space is

$$d^{GH}(X_1, X_2) = \inf\{d_Z^H(i_1(X_1), i_2(X_2))\}$$

where i_1, i_2 are isometry of X_1, X_2 into a metric space Z.

This metric makes the set of all compact metric space into a complete Hausdorff space $\mathcal{MET}$. ⌟

Def. (4.12.2.2). A map from X to Y is called a ε **approximation** iff $B(f(X), \varepsilon) = Y$ and $|d(x, y) - d(f(x), f(y))| \leq \varepsilon$.

We have: if there is a ε approximation, then $d^{GH}(X, Y) \leq 3\varepsilon$, and if $d^{GH}(X, Y) \leq \varepsilon$, there is a 3ε approximation. ⌟

Prop. (4.12.2.3). The set of isometries of ⌟

3 Spaces from Algebraic Geometry

Noetherian Space

Def. (4.12.3.1) [Noetherian Spaces]. A **Noetherian space** is a space $X \in \mathfrak{Top}$ that any descending chain of closed subsets stabilizes. A **locally Noetherian space** is a space $X \in \mathfrak{Top}$ that every point has a nbhd U s.t. U is a Noetherian space. ⌟

Prop. (4.12.3.2). A Noetherian space is quasi-compact and all subsets of it in the induced topology is Noetherian hence quasi-compact. ⌟

Proof: Let $T \subset X$, for a chain of closed subsets $Z_i \cap T$ of T, $Z_1, Z_1 \cap Z_2, \ldots$ stabilize in X, hence the chain stabilize in T. □

Prop. (4.12.3.3). If X can be covered by f.m. Noetherian subspaces, then X is Noetherian. ⌟

Proof: □

Prop. (4.12.3.4) [Noetherian Space F.M. Irreducible Components]. A Noetherian space has only f.m. irreducible component, hence it has only f.m. connected components. ⌟

Proof: Let $\mathcal{C}$ be the family of closed subset that has infinitely many component, then there is a minimal object, but it is not irreducible, one of the component has infinitely many components and be smaller. □

Quasi-Separated

Def. (4.12.3.5) [Quasi-Separated]. A space X is called **quasi-separated** if the diagonal morphism is quasi-compact(4.4.2.2). If X has a basis consisting of quasi-compact open subsets, then this is equivalent to any intersection of two quasi-compact open subsets is quasi-separated open. ⌟

Specialization & Generalization

Def. (4.12.3.6) [Specializations and Generalizations]. Let $X \in \mathcal{T}\mathrm{op}$ then x is said to be a **specialization of** y if $x \in \overline{\{y\}}$. And in this case y is said to be a **generalization of** x.

And they are called **immediate specializations/generalizations** if there are no other points $z \in X$ s.t. $y \to z \to x$. ⌟

Def. (4.12.3.7) [Going Up and Down]. A map f of spaces is said to satisfy the **going-up property** iff specialization lifts along f. It is said to satisfy the **going-down property** iff generalization lifts along f. ⌟

Prop. (4.12.3.8). A closed map satisfies going-up. ⌟

Proof: If $y \to y'$, $f(x) = y$, consider $f(\overline{\{x\}})$, it is closed and contains y, so it contains y', thus the result. □

Constructible Set

Def. (4.12.3.9) [Retrocompact Subset]. A subset of X is called **retrocompact** if the inclusion map is quasi-compact(4.4.2.2). ⌟

Def. (4.12.3.10) [Constructible Subset]. A subset of X is called **constructible** if it is a finite union of sets of the form $U \cap V^c$ where U, V are open and retrocompact in X. In the case when X is Noetherian, by(4.12.3.2), all subsets are retrocompact hence constructible sets are just union of locally closed subsets of X.

A set of X is called **locally constructible** if locally it is constructible. If X is quasi-compact, then a locally constructible set is just a constructible set. ⌟

Prop. (4.12.3.11). Constructible subsets of X forms a Boolean algebra. ⌟

Proof: Cf.[Sta]005H. □

Prop. (4.12.3.12) [Constructible and Subsets].

- If U is open in X, then for any E constructible in X, $E \cap U$ is constructible in U.
- If U is retrocompact open and E is constructible in U, then E is constructible in X.

⌟

Proof: Easy. □

Prop. (4.12.3.13). Any constructible subsets of X is retrocompact. ⌟

Proof: It suffices to prove $U_i \cap V_i^c \cap W$ is quasi-compact for W quasi-compact, but this is because it is a closed subspace of the quasi-compact subspace $U_i \cap W$. □

Cor. (4.12.3.14). An open subset of X is constructible iff it is retrocompact, a closed subset of X is constructible iff its complement is retrocompact.((4.12.3.11) used). ⌟

Def. (4.12.3.15) [Constructible topology]. The **constructible topology** X_{cons} on a quasi-compact space X is generated by the open subsets U, U^c, where U is a quasi-compact open.

Notice that the space is quasi-compact, so the constructible topology is the coarsest topology that every constructible subset of X is both open and closed. ⌟

Prop. (4.12.3.16). Let X be quasi-compact and quasi-separated, then any constructible subset of X is quasi-compact. In particular, if Y is closed in X, then Y is constructible iff it is quasi-compact. ⌟

Proof: For $Y = \cup_{i=1}^n (U_i - V_i)$, with U_i, V_j quasi-compact open in X, then $U_i - V_i$ is closed in U_i thus quasi-compact, and then Y is quasi-compact. □

Prop. (4.12.3.17). Let E be a constructible subset of a space X, if E is dense in then E contains some open dense subset of its closure. ⌟

Proof: Let $Y = \cup_{i=1}^k Y_i$ where Y_i are locally closed. Denote $Z_i = \overline{Y}_i \backslash Y_i, Z = \cup Z_i$, $W = \overline{Y} \backslash Z$. Then $W \subset Y$, and we show that W is open dense in $\overline{Y}$: As Y_i are locally closed, Y_i is open in $\overline{Y}_i$, thus Z_i is closed, and Z is closed, so W is open in $\overline{Y}$. To show W is dense in $\overline{Y}$: If some open subset U of $\overline{Y}$ satisfies $U \cup Z_i$, then U cannot be contained in any Z_i, so we can inductively show $U \backslash Z_1, U \backslash (Z_1 \cup Z_2), \ldots$ are non-empty, which is a contradiction. □

Irreducible

Def. (4.12.3.18) [Irreducible Space]. A space is called **irreducible** iff there are no two nonempty nonintersecting open subsets. Thus an open subset of an irreducible set is dense and irreducible. ⌟

Prop. (4.12.3.19). If Y is irreducible in X, then $\overline{Y}$ is also irreducible. ⌟

Proof: Any two nonempty open sets of $\overline{Y}$ must intersect Y thus must intersect. □

Prop. (4.12.3.20). If $X \in \mathcal{T}\mathrm{op}$ and $U \subset X$ is open, then $Y \mapsto \overline{Y}$ is a order preserving bijection between irreducible closed subspaces of U and irreducible closed subspaces of X meeting U. ⌟

Jacobson Space

Def. (4.12.3.21). Let X be a space and X_0 the set of closed pts of X, then X is called **Jacobson** iff $\overline{Z \cap X_0} = Z$ for every closed subset Z of X. This is equivalent to every non-empty locally closed subset of X contains a closed pt.

Thus there is a correspondence between closed subsets of X_0 and closed subsets of X, so they have the same Krull dimension. ⌟

Prop. (4.12.3.22). Being Jacobson is local. And for an open covering U_i of X, $X_0 = \cup U_{i,0}$. ⌟

Proof: Firstly, if $X = \cup U_i$ where U_i are Jacobson, $X_0 \cap U_i = U_{i,0}$. One direction is trivial, for the other, let x be closed in U_i, then consider $\overline{\{x\}} \cap U_j$. If $x \notin U_j$, this is empty, if $x \in U_j$, consider $T = \{x\} \cup (U_j - U_i \cap U_j)$, then T is closed in U_j, so by hypothesis, closed pts of U_j are dense in T, so x must be closed in U_j, so x is closed in X. Now clearly X is Jacobson.

Conversely, if X is Jacobson, for a closed subset Z of U_i, $X_0 \cap \overline{Z}$ is dense in $\overline{Z}$, so $X_0 \cap Z$ is dense in Z, then clearly U_i is Jacobson. □

Cor. (4.12.3.23). If X is Jacobson, then any locally constructible sets of X is Jacobson. And its closed pts are closed in X. ⌟

Proof: By the proposition, we only have to prove for constructible sets. For $T = \cup T_i$ where T_i is locally closed, then a locally closed set in T has a non-empty intersection $T \cap T_i$ which is also locally closed for some i.

Hence is has a closed pt in X hence in T, so T is Jacobson. The second assertion is implicit in the proof. □

Prop. (4.12.3.24). If X is Jacobson, then an open set U of X is compact iff $U \cap X_0$ is compact, hence an open set U is retrocompact iff $U \cap X_0$ is retrocompact.

Hence the constructible sets of X correspond to the constructible sets of X_0.

And Irreducible closed subsets correspond to irreducible subsets of X_0. ⌟

Krull Dimension

Def. (4.12.3.25). The **Krull dimension** of a topological space is the length of the longest chain of closed irreducible subsets.

The **local dimension** $\dim_x(X) = \min\{\dim U | x \in U \subset X \text{ open in X}\}$. ⌟

Prop. (4.12.3.26). If $Y \subset X$, then $\dim Y \leq \dim X$, because the closure of any chain of Y is a chain of X by(4.12.3.19).

For an open covering $\{U_i\}$ of X, $\dim X = \sup \dim U_i$, because for any chain of closed irreducible subsets, if U_i intersects the minimal one, then $\dim U_i$ = length of this chain. ⌟

Prop. (4.12.3.27). $\dim X = \sup \dim_x(X)$. ⌟

Proof: The right is smaller than the left by(4.12.3.26), and for any chain $Z_0 \subset Z_1 \subset \ldots \subset Z_n$ of irreducible closed subset of X, if I choose a point $x \in Z_0$, then $\dim_x(X) \geq n$. □

Prop. (4.12.3.28). In case $X = \operatorname{Spec} A$ for a Noetherian ring A, $\dim X = \sup \dim A_p$, because A is of finite**?** ⌟

Def. (4.12.3.29) [Codimensions]. Let $X \in \mathcal{T}\mathrm{op}$ and $Y \subset X$ be an irreducible closed subspace, then the **codimension** of Y in X is defined to be the supremum of lengths e of chains $Y = Y_0 \subset Y_1 \subset \ldots \subset Y_e = X$, denoted by $\operatorname{codim}(Y, X)$. ⌟

Sober Spaces

Def. (4.12.3.30) [Sober Spaces]. A space X is called **sober** if every irreducible closed subset has a unique generic point. ⌟

Prop. (4.12.3.31). A sober space is T_1. Conversely, a finite T_0 space is sober. ⌟

Proof: The first assertion is because if $x \in \overline{\{y\}}$ and $y \in \overline{\{x\}}$, then $\overline{\{x\}} = \overline{\{y\}}$, and this irreducible closed subset has two generic point, contradiction.

If the space is finite, then for a closed irreducible subset $T = \{x_1, \ldots, x_n\}$, $T = \cup\overline{\{x_i\}}$, as it is irreducible, $T = \overline{\{x_i\}}$ for some x_i, and i is unique as it is T_1, so X is sober. □

Prop. (4.12.3.32) [Soberization]. There is a left adjoint t to the forgetful functor from the Sober spaces. $t(X)$ consists of irreducible closed subsets of X, and use $t(Y)$ for Y closed as closed subsets. for a map $f : X \to Z$ to a sober space Z, the extension maps the generic point of an irreducible Y to the generic point of the closure of $f(Y)$. ⌟

Def. (4.12.3.33) [Zariski Space]. A Noetherian Sober space is called a **Zariski space**. ⌟

Catenary spaces and Dimension Functions

Def. (4.12.3.34) [Catenary Space]. A space X is called **catenary** iff for any inclusion of irreducible closed subsets of X, their codimension is finite and every maximal chain of irreducible closed subsets has the same dimension. This is equivalent to $\mathrm{codim}(X,Y)+\mathrm{codim}(Y,Z)=\mathrm{codim}(X,Z)$. ⌟

Prop. (4.12.3.35). Catenary is a local property, by(4.12.3.20). ⌟

Def. (4.12.3.36) [Dimension Function]. For $X\in\mathcal{T}\mathrm{op}$, consider the specialization relation(4.12.3.6), a **dimension function** is a function $\delta:|X|\to\mathbb{Z}$ that

- if y is a specialization of x in X, then $\delta(y)<\delta(x)$.
- if it is a direct specialization, then $\delta(y)=\delta(x)-1$.

The dimension function is usually considered only when the space is sober. ⌟

Prop. (4.12.3.37). Let $X\in\mathcal{T}\mathrm{op}$ be sober and catenary with a catenary function, then X is catenary, and if x is a specialization of x in X, then

$$\delta(x)-\delta(y)=\mathrm{codim}(\overline{\{y\}},\overline{\{x\}}).$$

⌟

Proof: This is clear from the definitions(4.12.3.29). □

Prop. (4.12.3.38). If $X\in\mathcal{T}\mathrm{op}$ be locally Noetherian and sober, and δ,δ' are two dimension functions on X, then $\delta-\delta'$ is locally constant on X. ⌟

Proof: We may assume X is Noetherian, so it has only f.m. irreducible components by(4.12.3.4), then $\delta-\delta'$ is locally constant on the X minus the irreducible components not passing through x by(4.12.3.37). □

Prop. (4.12.3.39) [Catenary and Sober]. Let $X\in\mathcal{T}\mathrm{op}$ be locally Noetherian, sober, then X is catenary iff any point $x\in X$ has a nbhd U which has a dimension function. ⌟

Proof: Cf.[Sta]02IC.
The other direction follows from(4.12.3.37) and(4.12.3.35). □

Sober Spaces

Def. (4.12.3.40) [Sober Spaces]. A space X is called **sober** if every irreducible closed subset has a unique generic point. ⌟

Prop. (4.12.3.41). A sober space is T_1. Conversely, a finite T_0 space is sober. ⌟

Proof: The first assertion is because if $x\in\overline{\{y\}}$ and $y\in\overline{\{x\}}$, then $\overline{\{x\}}=\overline{\{y\}}$, and this irreducible closed subset has two generic point, contradiction.
. □

Prop. (4.12.3.42) [Catenary and Sober]. Let $X\in\mathcal{T}\mathrm{op}$ be locally Noetherian, sober and catenary, then any point $x\in X$ has a nbhd U which has a dimension function. ⌟

Proof: Cf.[Sta]02IC. □

4 Spectral Spaces

References are [Sta]5.23 and [Adic Spaces].

Def. (4.12.4.1) [Spectral Space]. A space is called **spectral** iff it is quasi-compact, quasi-separated(4.12.3.5), sober and the quasi-compact opens form a basis for the topology.

A space is called **locally spectral** iff it has an open covering by spectral spaces.

A morphism $f : X \to Y$ between locally spectral spaces is called **spectral** if for any open spectral spaces $U \subset f^{-1}(V)$, $f : U \to V$ is quasi-compact. ⌟

Prop. (4.12.4.2) [Connected Components]. Let X be a spectral space, then any connected subset of X is an intersection of clopen subsets. ⌟

Proof: Let $x \in X$ and S be the intersection of all clopen subsets of X containing x, then it suffices to show S is connected. Suppose $S = B \coprod C$ with B, C closed, then B, C are compact, thus there exist quasi-compact opens $U, V \subset X$ that $B = U \cap S, C = V \cap S$. Then $U \cap V \cap S = \varnothing$. Now $U \cap V$ is quasi-compact also, so there exists some clopen Z_α containing x that $Z_\alpha \cap U \cap V = \varnothing$. Similarly, there exists some clopen Z_β containing x that $Z_\beta \subset U \cup V$. Then $Z_\gamma = Z_\alpha \cap Z_\beta$ is clopen and contained in $U \Delta V$, Then Both $Z_\gamma \cap U$ and $Z_\gamma \cap V$ is clopen, so $U = \varnothing$ or $V = \varnothing$. □

Cor. (4.12.4.3). Let X be a spectral space, then for a subset T of X, T is an intersection of clopen subsets of X iff T is closed in X and is a union of connected components of X. ⌟

Proof: If T is an intersection of clopen subsets, then T is clearly a union of connected components of X. Conversely, if T is a union of connected components of X, if $x \notin T$, let C be a connected components containing x. Then C is an intersection of clopen subsets, by(4.12.4.2). These subsets are closed under finite intersections, so by the compactness of T, there is a clopen subset containing T but not x, so we are done. □

<u>**Constructible Topology**</u>

Lemma (4.12.4.4). If X is a finite T_0 space, then it is spectral and every subset of X is constructible. ⌟

Proof: Cf.[Adic Space Morel, P26]. □

Prop. (4.12.4.5). If X is a spectral space, then the constructible topology(4.12.3.15) is Hausdorff, totally disconnected and quasi-compact. ⌟

Proof: The space is sober hence T_0(4.12.3.41), and then the constructible topology is Hausdorff and totally disconnected.

To show quasi-compactness, it suffices to show that the family $\mathcal{C}$ of quasi-compact open and complement quasi-compact open subsets has the finite intersection property(4.4.2.3). Notice elements in $\mathcal{C}$ are all quasi-compact. Now if there is a family that has the finite intersection property by has intersection 0, by Zorn's lemma, there is a maximal one of them, $\mathcal{B}$. Now let Z be the intersection of all the closed subsets in $\mathcal{B}$, then it is non-empty as X is quasi-compact. And we claim Z is irreducible: otherwise $Z = Z_1 \cup Z_2$, thus there are quasi-compact open sets U_1, U_2 that $U_1 \cap Z_1 \neq \varnothing, U_1 \cap Z_2 = \varnothing, U_2 \cap Z_2 \neq \varnothing, U_2 \cap Z_1 = \varnothing$. then let $B_i = X - U_i$, then B_1, B_2 cannot by added to $\mathcal{B}$ by maximality, so there is a finite intersection T_1, T_2 that $B_i \cap T_i = 0$. But then $Z \cap T_1 \cap T_2 = 0$, but Z is an intersection of closed subsets, thus some finite intersection of closed subsets in $\mathcal{B}$ will $\cap T_1 \cap T_2 = 0$, contradiction.

So now Z is irreducible, but then for every element $B \in \mathcal{B}$, $Z \cap B$ contains the generic point of Z, thus the intersection of B is not empty, contradiction. □

Cor. (4.12.4.6). Let X be a spectral space, then

- The constructible topology is finer than the original topology.
- A subset X is constructible iff it is clopen in the constructible topology of X.
- If U is open in X, then the constructible topology induces the constructible topology on U.

⌟

Proof:
1: Every open subset of X is a union of its quasi-compact open subsets, so it is open in the constructible topology.
2: Clearly constructible subset is clopen in the constructible topology. Conversely, if Y is clopen, then Y is a union of constructible subsets, but also it is quasi-compact, so it is a finite union of constructible subsets, thus constructible.
3: Cf.[Mor19] P28. □

Prop. (4.12.4.7). If $E \subset X$ is closed in the constructible topology, then it is a spectral space with the induced topology, and the inclusion map is spectral. ⌟

Proof: Cf. [Mor19]P34. □

Prop. (4.12.4.8). For a set E closed in the constructible topology in a spectral space,

- every point of $\overline{E}$ is a specialization of elements in E. Thus if E is stable under specialization, then it is closed.
- If E is open in the constructible topology and stable under generalization, then it is open.

⌟

Proof: Cf. [Sta]0903**?**. □

Prop. (4.12.4.9). For a map between spectral spaces $f : X \to Y$, the following are equivalent:

- f is spectral.
- f is quasi-compact.
- $f : X_{cons} \to Y_{cons}$ is continuous.

And if this is true, then $f : X_{cons} \to Y_{cons}$ is proper. ⌟

Proof: $1 \to 2 \to 3$ is trivial, an open subset of X is quasi-compact iff it is clopen in the constructible topology(4.12.4.6), so $3 \to 2$. For $2 \to 1$, notice that if $U \subset f^{-1}(V)$ are open spectrals, and $W \subset U$ is quasi-compact open, then $f^{-1}W \cap U$ is quasi-compact open, because X is quasi-separated.
Finally, f is proper because X_{cons}, Y_{cons} is compact Hausdorff(4.12.4.5), then use(4.4.2.10). □

<u>**Criterion of Spectralness**</u>

Lemma (4.12.4.10). Let X be a quasi-compact T_0 space that is has a subbasis consisting of quasi-compact open subsets that is stable under finite intersections. Let X' be the topology generated by the quasi-compact open subsets and their complements, then the following are equivalent:

- X is spectral.
- X' is compact Hausdorff, and its topology has a basis consisting of open and closed subsets.

- X' is quasi-compact.

⌟

Proof: Cf.[Adic Space Morel P30]. □

Prop. (4.12.4.11) [Hochster's Criterion of Spectrality]. Let $X' = (X_0, \mathcal{T}')$ be a quasi-compact topological space, and let $\mathcal{U}$ be the family of clopen subsets of $\mathcal{T}'$, let $\mathcal{T}$ be the topology generated by $\mathcal{U}$, let $X = (X_0, \mathcal{T})$.

Then if X is T_0, then it is spectral, and every element of $\mathcal{U}$ is quasi-compact open in X, and $X' = X_{cons}$. ⌟

Proof: Cf.[Adic Space Morel, P29]. □

Prop. (4.12.4.12) [Spectral and Inverse Limit]. A space is spectral iff it is a direct limit of finite sober(finite $T1$(4.12.3.41)) spaces. ⌟

Proof: Cf.[Sta]09XX. □

Prop. (4.12.4.13) [Spec and Spectral Space]. A spectral space is exactly the underlying space of spectrum of some ring. ⌟

Proof: The spectrum of a ring is qc: if $\cup D(f_i) = \operatorname{Spec} A$, then $(f_i) = (1)$, so f.m. of them generate (1). And similarly it is quasi-separable and $D(f) = \operatorname{Spec} A_f$ is quasi-compact. For the other direction, Cf.[M. Hochster. Prime ideal structure in commutative rings, Thm6]**?**. □

Cor. (4.12.4.14). Every quasi-compact irreducible scheme is homeomorphic to an affine scheme. ⌟

Cor. (4.12.4.15) [Characterization of Spectral Spaces]. The following are equivalent for a topological space T:

1. $T \cong \operatorname{Spec} R$ for some ring R.
2. $T \cong \varprojlim T_i$ where $\{T_i\}$ is an inverse system of finite T_0 spaces.
3. T is spectral.

⌟

Proof: This follows from(4.12.4.13) and(4.12.4.12). □

w-localness

Def. (4.12.4.16)[pro-Zariski Localization]. A map of spectral spaces $f: W \to V$ is called a **Zariski localization** if $W = \coprod_i U_i$ where $U_i \to V$ is a quasi-compact open immersion. A **pro-Zariski localization** is a cofiltered limit of Zariski localizations of V. ⌟

Def. (4.12.4.17)[w-Local]. A spectral space is called **w-local** if the set of closed pts of X is closed and any point of X specializes to a unique closed pt. A morphism of w-local spaces are called **w-local** if it is spectral and maps closed pts to closed pts. ⌟

Prop. (4.12.4.18). If X is w-local and $Y \subset X$ is a closed subset, then Y is also w-local. ⌟

Proof: Y is spectral by(4.12.4.7). Y_0 is closed because $Y_0 = Y \cap X_0$. And the second assertion is also trivial. □

Prop. (4.12.4.19). Let X be a spectral space and T profinite, then $Y = X \times_{\pi_0(X)} T$ is also spectral and $T = \pi_0(Y)$. If moreover X is w-local, then Y is also w-local and $Y \to X$ is w-local. ⌟

Proof: Cf.[Sta]096C. □

Def. (4.12.4.20) [Localization Along a Closed Set]. Given a closed set Z of a spectral set X, the pro-open subset of X consisting of all points that specializes to a point of Z is called the **localization of X along Z**. And X is called **local along** Z if $X_0 \subset Z$. ⌟

Prop. (4.12.4.21). A spectral space that is local along a closed w-local subset $Z \subset X$ with $\pi_0(Z) \cong \pi_0(X)$, is also w-local. ⌟

Proof: $X_0 = Z_0$ is clearly closed, and if a pt x of X specializes to two closed pts of Z, then the π_0 map is not injective, contradiction. □

4.13 Algebraic Topology I: Homotopies

Main references are [Hat02], [AGP02], [同调论, 姜伯驹], [May99], [https://ncatlab.org/nlab/show/Introduction+to+Homotopy+Theory#HomotopyGroupsOftopologicalSpaces].

Notation (4.13.0.1).

- Use notations defined in Topology I.
- All spaces are assumed to be compactly generated, and products and mapping spaces are assumed to be compact generated versions.

⌟

1 Homotopy Types

Def. (4.13.1.1) [Retraction]. A **retraction** of a space X to a subspace A is a map $r : X \to A$ that $r|_A = \mathrm{id}_A$. ⌟

Def. (4.13.1.2) [Homotopy]. A **homotopy** $f_t : X \to Y$ is a family of maps f_t for every $t \in I$ that $f : X \times I \to Y$ is continuous. For two homotopies $F : X \times I \to Y$ and $F' : X \times I \to Y$ s.t. $F_1 = F'_0$, we can define the **composite homotopy** $F' \cdot F : X \times I \to Y$.

Tow maps $f_0, f_1 : X \to Y$ are called **homotopic** is there is a homotopy $f_t : X \to Y$ connecting them. Homotopy relations are denoted by $f_0 \cong f_1$.

Let A be a subspace of X, then a **homotopy relative to** A is a homotopy $f_t : X \to Y$ whose restriction to A is fixed.

Let E_1, E_2 be spaces over B, then maps $f_0, f_1 : E_1 \to E_2$ over B are called **fiber homotopic** if there is a homotopy $f_t : E_1 \to Y$ connecting them that each f_t are maps over B. Homotopy relations over B are denoted by $f_0 \cong_B f_1$. ⌟

Def. (4.13.1.3) [Homotopy Equivalences]. A map $f : X \to Y$ is called a **homotopy equivalence** if there is a map $g : Y \to X$ that $f \circ g \cong \mathrm{id}$ and $g \circ f \cong \mathrm{id}$.

A space having the homotopy type of a point is called **contractible**.

A map $f : X \to Y$ over B is called a **fiber homotopy equivalence** if there is a map $g : Y \to X$ over B that $f \circ g \cong_B \mathrm{id}$ and $g \circ f \cong_B \mathrm{id}$. ⌟

Def. (4.13.1.4)[Deformation Retraction]. A **deformation retraction** of a space X onto a subspace A is a homotopy $f_t : X \to X, t \in I$ that $f_0 = \mathrm{id}, f_1(X) = A$ and $f_t|_A = \mathrm{id}_A$ for all t. ⌟

Prop. (4.13.1.5). A map $X \to Y$ is a homotopy equivalence iff the mapping cylinder deformation retracts onto X. ⌟

Proof: ? □

Def. (4.13.1.6) [Excisive Triads]. A **triad of spaces** is a triple $(X; A, B)$ s.t. $A \subset X, B \subset X$. An **excisive triad** is a triad $(X; A, B)$ s.t. $A^o \cup B^o = X$. ⌟

Relative Spaces

Def. (4.13.1.7) [Relative Spaces]. The category $\mathcal{CG}^{\mathrm{rel}}$ is the category of pairs (X, A) where $A \subset X \in \mathcal{CG}$, and morphisms in $\mathcal{CG}^{\mathrm{rel}}$ are equivariant maps. ⌟

Def. (4.13.1.8) [Smash Products]. **smash products** in $\mathcal{CG}^{\text{rel}}$ are defined to be $(X, A) \wedge (Y, B) = (X \times Y, (X, A) \vee (Y, B))$, where $(X, A) \vee (Y, B) = X \times B \cup A \times Y \subset X \times Y$. ⌟

Def. (4.13.1.9) [Cones and Suspensions]. For $(X, A) \in \mathcal{T}\text{op}^{\text{rel}}$, the **cone** over (X, A) is defined to be $C(X, A) = (X, A) \wedge (\mathbb{I}, \{1\})$. The **suspension** of (X, A) is defined to be $\Sigma(X, A) = (X, A) \wedge \mathbb{S}^1$. ⌟

Prop. (4.13.1.10) [$\mathcal{CG}^{\text{rel}}$ is Closed]. For $(X, A), (Y, B), (Z, C) \in \mathcal{CG}^{\text{rel}}$, by(4.4.3.15) there is a homeomorphism

$$\text{Map}((X, A) \wedge (Y, B), (Z, C)) \cong \text{Map}((X, A), \text{Map}((Y, B), (Z, C))).$$

In particular, $\mathcal{CG}^{\text{rel}}$ is a closed symmetric monoidal category. ⌟

Def. (4.13.1.11) [Pointed Spaces]. The category $\mathcal{CG}^{\text{pt}}$ is the subcategory of $\mathcal{CG}^{\text{rel}}$ consisting of pairs (X, A) s.t. $A \cong \text{pt}$. It is stable under finite products.

We can define similarly homotopies of maps between pointed spaces, and denote $\langle X, Y \rangle$ the homotopy classes of maps from X to Y. ⌟

Def. (4.13.1.12) [Smash Products]. For $X, Y \in \mathcal{CG}^{\text{pt}}$, the **smash product** $X \wedge Y$ is defined to be $X \wedge Y = X \times Y / X \wedge Y$, where $X \vee Y = X \coprod_* Y$, called the **wedge sum** of X and Y. Similar to(4.13.1.9), we can define cones and suspensions of pointed spaces.

Then the smash product and wedge sums are commutative and associative, and they satisfy

$$(X \vee Y) \wedge Z = X \wedge Z \vee Z \wedge Z.$$

Because of(4.13.1.14), the smash product and wedge sums are also denoted by $X \otimes Y$ and $X \oplus Y$. ⌟

Proof: For the identities, use the fact product commutes with colimits(4.4.3.16). □

Prop. (4.13.1.13) [Smash Products, and Homotopy]. Suspensions preserves homotopy, as $\Sigma(X \wedge I) = X \wedge I \wedge \mathbb{S}^1 \cong (X \wedge \mathbb{S}^1) \wedge I$. ⌟

Prop. (4.13.1.14) [$\mathcal{CG}^{\text{pt}}$ is Closed]. For $X, Y, Z \in \mathcal{CG}^{\text{pt}}$, by(4.13.1.10), there is a bijection

$$\text{Map}(X \wedge Y, Z) \cong \text{Map}(X, \text{Map}(Y, Z)).$$

In particular, $\mathcal{CG}^{\text{pt}}$ is a closed symmetric monoidal category. ⌟

Def. (4.13.1.15) [Well-Pointed Spaces]. A pointed space $(X, *) \in \mathcal{CG}^{\text{pt}}$ is called a **well-pointed space** if $* \to X$ is a cofibration. The category of well-pointed spaces is denoted by $\mathcal{CG}^{\text{well-pt}}$. ⌟

Def. (4.13.1.16) [Augmentation]. There is a functor $\mathcal{CG} \to \mathcal{CG}^{\text{well-pt}} : X \mapsto X_+ = (X \coprod \text{pt}, \text{pt})$. ⌟

Prop. (4.13.1.17). The cone construction

$$\mathcal{T}\text{op}^{\text{rel}} \to \mathcal{T}\text{op} : (X, A) \mapsto C(A \to X)$$

preserves homotopy equivalence. ⌟

Prop. (4.13.1.18) [Path Spaces and Loop Spaces]. For $X \in \mathcal{CG}^{\text{pt}}$, define the **path space** $P(X) = \text{Map}((\mathbb{I}, \{0\}), X)$, and define the **loop space** $\Omega(X) = \text{Map}(\mathbb{S}^1, X)$.

Then by(4.13.1.14), there are homeomorphism of spaces

$$\text{Map}(\Sigma(X), Y) \cong \text{Map}(X, \Omega(Y)).$$

Thus also

$$\langle \Sigma(X), Y \rangle \cong \langle X, \Omega(Y) \rangle.$$

⌟

Def. (4.13.1.19) [Weak Products]. For $\{X_\alpha\}_\Sigma \in \mathcal{CG}^{\mathrm{pt}}$, define the **weak product** $\prod' X_\alpha$ as

$$\prod{}' X_\alpha = \varinjlim_{S\subset\Sigma, \#S<\infty} \bigvee_{i\in S} X_i$$

with base point $\prod *$. ⌟

2 Isotopies

Def. (4.13.2.1) [Isotopies]. For $V, M \in \mathcal{M}\mathrm{ani}$, an **isotopy** from V to M is a map $V\times I \to M$ s.t. for any $t \in I$, the map $F_t : V \to M$ is an embedding. ⌟

Prop. (4.13.2.2) [Alexander's Trick]. If $f, g : \mathbb{D}^n \to \mathbb{D}^n$ be two self-homeomorphisms that there is an isotopy $F : \mathbb{D}^n \times I \to \mathbb{D}^n$ between $f|_{\partial\mathbb{D}^n}$ and $g|_{\partial\mathbb{D}^n}$, then there exists an isotopy between f and g extending F. ⌟

Proof: Firstly, if $g = \mathrm{id}_{\mathbb{D}^n}$ and f fixes every points on the boundary, then an isotopy connecting f to the identity is given by

$$J(x,t) = \begin{cases} tf(x/t) & ,0\le ||x|| < t \\ x & ,t \le ||x|| \le 1 \end{cases}.$$

In general, isotopy $g^{-1}F : \mathbb{D}^n \times I \to \mathbb{D}^n$ between $g^{-1}f|_{\partial\mathbb{D}^n}$ and $\mathrm{id}_{\partial\mathbb{D}^n}$ can be extended to an isotopy from $F' : \mathrm{Cone}(g^{-1}f|_{\partial\mathbb{D}^n})$ to $\mathrm{id}_{\mathbb{D}^n}$. Then $\mathrm{Cone}(g^{-1}f|_{\partial\mathbb{D}^n})$ and $g^{-1}f$ are identical on $\partial\mathbb{D}^n$, so by the argument above, they are isotopic. Then $g^{-1}f \cong \mathrm{id}_{\mathbb{D}^n}$, which gives an isotopy between f and g. □

Prop. (4.13.2.3). Any orientation-preserving self-homeomorphism f of $\mathbb{S}^d$ is isotopic to $\mathrm{id}_{\mathbb{S}^d}$. ⌟

Proof: By the decomposition of $\mathbb{S}^d$ into two hemispheres and using the annulus theorem(4.4.11.2), we see we can isotopy f to a map that fixes the equator. Then we can use Alexander's trick(4.13.2.2). □

3 CW Complexes

Def. (4.13.3.1) [CW Complexes]. A **CW complex** is a space X that $\varnothing \to X$ is cofibrantly generated by $\mathbb{S}^n \to \mathbb{D}^n$.

For a CW complex X, a **representation of** X is given as follows:

- $\mathrm{sk}_0 X$ is a discrete set, whose elements are regarded as 0-cells.
- Inductively, form the n-**skeleton** $\mathrm{sk}_n X$ from $\mathrm{sk}_{n-1} X$ by adding n-**cells** e^n_α via maps $\varphi_\alpha : \mathbb{S}^{n-1} \to \mathrm{sk}_{n-1} X$.
- Let $X = \cup\, \mathrm{sk}_n X$ be given the quotient topology from $\coprod_n \mathrm{sk}_n X$.

We will also call the image of e^n_α as an n-cell. The category of CW complexes is denoted by $\mathcal{CW}$. Any CW complex is compactly generated, by definition. ⌟

Def. (4.13.3.2) [Sub-CW Complexes]. For a CW complex X, a **subcomplex** $Y \subset X$ is a subspace $Y \subset X$ s.t. the cells with images in Y makes Y a CW complex. ⌟

Def. (4.13.3.3) [Finite CW Complexes].

- A **CW complex of finite dimension** is a CW complex X s.t. $X = \mathrm{sk}_n X$ for some $n \in \mathbb{N}$.

- A **CW complex of finite type** is a CW complex X that has only finitely many n-cells for each n.
- A **finite CW complex** is a CW complex that is both of finite dimensional and of finite type.
- A **locally finite CW complex** is a CW complex that each cell intersect only f.m. other cells.

⌟

Prop. (4.13.3.4) [Dimension of CW Complexes]. Given a representation of a CW complex of finite dimension X, $\dim X$ is defined to be the minimal n s.t. $X = \mathrm{sk}_n X$. Then this dimension is independent of the presentation given. ⌟

Proof: □

Prop. (4.13.3.5). Any compact subspace K of a CW complex X is contained in a finite subcomplex. In particular, a CW complex is compact iff it is finite. ⌟

Proof: Firstly K intersects with only f.m. interiors of cells of X(where we assume the interior of a point in $\mathrm{sk}_0 X$ is the point itself): otherwise take $S = \{x_1, x_2, \ldots\}$ be an infinite sequence of points lying in different cells, then $S \cap e_\alpha$ is closed for any cell e_α of X, so S is closed. But the same argument show any single point of S is also closed, so S is discrete, so S is finite, contradiction.

Then it suffices to show that any cell meets only f.m. cells: for this we can use induction on $\dim X$, and notice that for any cell e_α, the image of its attaching map is compact. □

Prop. (4.13.3.6) [Miyazaki]. Any CW complex is paracompact Hausdorff, thus also normal by(4.4.7.6). ⌟

Proof: To show it is Hausdorff, for any two points x, y, it is not hard to find disjoint precompact nbhds of x, y by induction on cells.

To show it is paracompact, Cf.[Rudolph Fritsch and Renzo Piccinini, Cellular Structures in Topology]Thm1.3.5.? □

Prop. (4.13.3.7). A CW complex is locally compact iff it is locally finite. A connected CW complex is metrizable iff it is locally finite. ⌟

Proof: Cf.[Rudolph Fritsch and Renzo Piccinini, Cellular Structures in Topology, Cambridge University Press, 1990.]Prop1.5.7. □

Prop. (4.13.3.8) [Product of CW Complexes]. For $X, Y \in \mathcal{CW}$, then the compactly generated product space $X \times_c Y$ admits a CW complex structure with

$$\mathrm{sk}_n X = \cup_{i+j=n} \mathrm{sk}_i X \times \mathrm{sk}_j Y.$$

And if either X or Y is locally compact or both X, Y have countably many cells, then $X \times_c Y = X \times Y$. ⌟

Proof: Given presentations of CW complexes of X, Y, we can define the CW complex structure on $X \times Y$ by choosing homeomorphisms of pairs

$$(\mathbb{D}^n, \mathbb{S}^n) \cong (\mathbb{D}^p \times \mathbb{D}^q, \mathbb{D}^p \times \mathbb{S}^{q-1} \cup \mathbb{S}^{p-1} \times \mathbb{D}^q),$$

where $p + q = n$. Then it is a CW structure on $X \times_c Y$ by(4.4.3.16).

For the last assertion, the case X is locally compact follows from(4.4.2.33). The case that X, Y both have countably many cells follow from [Hatcher, P524].? □

Prop. (4.13.3.9) [Cellular Maps]. Given $X, Y \in \mathcal{CW}$, a **cellular map** $f : X \to Y \in \mathcal{CW}$ is a map s.t. $f(\mathrm{sk}_n X) \subset \mathrm{sk}_n Y$ for any $n \in \mathbb{N}$. And a **cellular homotopy** between two cellular maps $f, g : X \to Y$ is a homotopy $F : X \times I \to Y$ between f and g s.t. F is a cellular map. ⌟

Prop. (4.13.3.10) [CW Structure on Compact Manifolds]. $\mathcal{M}\mathrm{ani}_{\mathrm{cpct}} \in \mathcal{CW}^{\mathrm{fin}}$. ⌟

Proof:

□

Def. (4.13.3.11) [Relative CW complexes]. A **relative CW complex** is a pair (A, X) s.t. $A \to X$ is cofibrantly generated by $\mathbb{S}^n \to \mathbb{D}^n$. The category of relative CW complexes is denoted by $\mathcal{CW}^{\mathrm{rel}}$. A **pointed CW complex** is a pointed space $(X, *) \in \mathcal{T}\mathrm{op}^{\mathrm{pt}}$ s.t. X has a presentation as a CW complex with $* \in X^0$. The category of pointed CW complexes is denoted by $\mathcal{CW}^{\mathrm{pt}}$.

Cellular maps in $\mathcal{CW}^{\mathrm{rel}}$ is defined similarly as that of(4.13.3.9). ⌟

Prop. (4.13.3.12) [Pathspace is CW Complex]. The homotopy fibers(4.4.3.18) of any map $f : A \to B$ between CW complexes are homotopic to a CW complex. ⌟

Proof: [Milnor, 1959]. or [Rudolph Fritsch and Renzo Piccinini, Cellular Structures in Topology]. □

Cor. (4.13.3.13) [Loop Space]. For $X \in \mathcal{CW}^{\mathrm{pt}}$, the loop space(4.4.3.19) ΩX is homotopic to a pointed CW complex. In particular, if X is of f.t., then so does ΩX. ⌟

Proof: This is a special case of(4.13.3.12) applied to $A = \{*\}$, by(4.4.3.20). □

Common CW complexes

Def. (4.13.3.14) [Infinite Vector Spaces]. Let $\mathbb{K} = \mathbb{R}, \mathbb{C}$ or $\mathbb{H}$, then the **infinite vector space** $\mathbb{K}^\infty$ is the CW complex $\varinjlim_n \mathbb{K}^n$.

There can be given a norm map on $\mathbb{K}^\infty$, as the canonical embedding is norm preserving. ⌟

Prop. (4.13.3.15) [Grassmannian]. Let $\mathbb{K} = \mathbb{R}, \mathbb{C}$ or $\mathbb{H}$, then the **Grassmannian** $\mathrm{Gra}(k, \mathbb{K}^n)$ admits a CW complex structure. ⌟

Proof: Cf.[Algebraic Topology Miller, P46] or [Characteristic Classes, Milnor].? □

Def. (4.13.3.16) [Infinite Grassmannian]. Let $\mathbb{K} = \mathbb{R}, \mathbb{C}$ or $\mathbb{H}$, then the **infinite Grassmannian** $\mathrm{Gra}(k, \mathbb{K}^\infty)$ is the CW complex $\varinjlim_n \mathrm{Gra}(k, \mathbb{K}^n)$(12.11.2.12).

In particular, $\mathrm{Gra}(1, \mathbb{K}^\infty) \cong \varinjlim_n \mathbb{KP}^n$ is defined to be the **infinite projective space** $\mathbb{KP}^\infty$. ⌟

Def. (4.13.3.17) [Infinite Stiefel Manifold]. Let $\mathbb{K} = \mathbb{R}, \mathbb{C}$ or $\mathbb{H}$, then the **infinite Stiefel Manifold** $V_k(\mathbb{K}^\infty)$ is the CW complex $\varinjlim_n V_k(\mathbb{K}^n)$ where $V_k(\mathbb{K}^n)$ is the set of orthonormal k-frames(12.11.2.12).

$V_1(\mathbb{K}^\infty) = \varinjlim_n S^n$ is called the **infinite sphere**. It is isomorphic to

$$\mathbb{S}^\infty = \varinjlim_k S^{2k+1} = \varinjlim_k \mathbb{C}^{2k+1} \backslash \{0\}/\mathbb{R}^+ = (\mathbb{C}^\infty \backslash \{0\})/\mathbb{R}_+^\times.$$

⌟

Prop. (4.13.3.18). $V_k(\mathbb{K}^\infty)$ is contractible. ⌟

Proof: We prove for $\mathbb{S}^\infty$, the proof for $V_k(\mathbb{K}^\infty)$ is verbatim, using Smith orthogonalization.

There is a map $H : \mathbb{S}^\infty \times I \to \mathbb{S}^\infty$ defined by

$$H((x_1, x_2, \ldots), t) = ((1-t)x_1, tx_2 + (1-t)x_1, tx_3 + (1-t)x_2, \ldots)/N$$

where N is the norm of the non-zero element $((1-t)x_1, tx_2 + (1-t)x_1, tx_3 + (1-t)x_2, \ldots)$. The image of H_1 is in the subspace $\mathbb{S}^\infty_1$ of elements $(x_1, x_2, \ldots)$ with $x_1 = 0$. Notice there is another map $H' : \mathbb{S}^\infty_1 \times I \to \mathbb{S}^\infty$ defined by

$$H'((0, x_2, \ldots), t) = (t, (1-t)x_2, (1-t)x_3, \ldots)/N'$$

where N' is the norm of the non-zero element $(t, (1-t)x_2, (1-t)x_3, \ldots)$. Then the composition homotopy $(H' \circ H_1) \cdot H$ gives the desired homotopy from $\mathrm{id}_{\mathbb{S}^\infty}$ to a constant map. □

Prop. (4.13.3.19). $\mathbb{RP}^\infty = \mathbb{S}^\infty/\{\pm 1\} = (\mathbb{C}^\infty \backslash \{0\})/\mathbb{R}^\times$. ⌟

Def. (4.13.3.20) [James Reduced Product]. Let X be a space with a basepoint e, let the **James reduced product** space $J(X)$ be the quotient of $\coprod_n X^n$ under the identification $(x_1, \ldots, x_j, \ldots, x_n) \sim (x_1, \ldots, \widehat{x}_j, \ldots, x_n)$ if $x_j = e$.

$J(X)$ is a union of subspaces $J_m(X)$, where $J_m(X)$ is the quotient space of X^m under the identification $(x_1, \ldots, x_j, e, \ldots, x_n) \sim (x_1, \ldots, e, x_j, \ldots, x_n)$. If (X, e) is a CW-pair, then J_m is obtained from X^m by glueing together its m subcomplexes where one of the coordinates is e. It is then clear J is a CW complex. ⌟

Def. (4.13.3.21) [Infinite Symmetric Product]. Let X be a space with a basepoint e, define the **infinite symmetric product** as the quotient of $J(X)$ by permutations. If X is a simplicial complex, then $SP(X)$ is a CW-complex. ⌟

Proof: Cf.[Hat02]P482. □

4 Homotopy Groups

Def. (4.13.4.1) [Homotopy Groups]. For $(X, *) \subset \mathcal{T}\mathrm{op}^{\mathrm{pt}}$ and $n \in \mathbb{N}$, define the **homotopy groups** $\pi_n(X) = \pi_n(X, *) = \langle \mathbb{S}^n, X \rangle$, which is a pointed set.

And $\pi_1(X)$ is a group as $\mathbb{S}^1$ has a cogroup structure: $\mathbb{S}^1 \to \mathbb{S}^1 \wedge \mathbb{S}^1$. Similarly, $\pi_n(X) = \pi_1(\Omega^{n-1}X)$ are also groups, and the group structure are given by the cogroup structure $\mathbb{S}^n \to \mathbb{S}^n \wedge \mathbb{S}^n$. ⌟

Prop. (4.13.4.2) [Loop Spaces and Homotopy Groups]. $\pi_{i+1}(M) \cong \pi_i(\Omega(M))$. ⌟

Proof: This follows from the fact $\mathbb{S}^n = \Sigma^n(\mathbb{S}^0)$ and(4.13.1.18). □

Prop. (4.13.4.3) [Homotopy Groups are Abelian]. For $X \in \mathcal{CG}^{\mathrm{pt}}$, the homotopy group $\pi_n(X)$ is an Abelian group for $n \geq 2$. ⌟

Proof: By(4.13.4.2), it suffices to show for $n = 2$, and $\pi_2(X) = \pi_1(\Omega X)$ is Abelian by(4.14.2.30) and(4.14.2.24). □

Cor. (4.13.4.4). For any $X \in \mathcal{CG}$, $\langle \Sigma(X), Y \rangle$ is a group and $\langle \Sigma^2(X), Y \rangle$ is an Abelian group. ⌟

Prop. (4.13.4.5) [Homotopy Groups and Change of Basepoints]. Let $X \in \mathcal{CG}$ and $\gamma : \mathbb{I} \to X$ be a path from a to b, then for any $n \in \mathbb{Z}_+$, we can define a map $\gamma_\# : \pi_n(X, a) \to \pi_n(X, b)$ as follows: For any $f : (\mathbb{I}^n, \partial I^n) \to (X, a)$, identity $\mathbb{I}^n$ with the subspace of $\mathbb{R}^n$ consisting of vectors $\mathtt{x}$ s.t. $d(\mathtt{x}) \leq \frac{1}{2}$, where $d((x_1, \ldots, x_n)) = \min(|x_i|)$, and

$$\gamma_\#(f) : (\mathbb{I}^n, \partial I^n) \to X : \mathtt{x} \mapsto \begin{cases} f(2\mathtt{x}) & , ||\mathtt{x}|| \leq \frac{1}{4} \\ \gamma(4||\mathtt{x}|| - 1) & , \frac{1}{4} \leq ||\mathtt{x}|| \leq 1 \end{cases}$$

Then for any $x_0 \in X$, this defines an actions of $\pi_1(X, x_0)$ on $\pi_n(X, x_0)$ by group homomorphisms for any $n \in \mathbb{Z}_+$. And for $n = 1$, this is just the conjugation action. ⌟

Proof: It is a well-defined action because any homotopy between two maps $f_1, f_2 : (\mathbb{I}^n, \partial I^n) \to (X, a)$ can generate a homotopy between $\gamma_\#(f_1)$ and $\gamma_\#(f_2)$, and it is an action by group homomorphism because there is a homotopy between $\gamma_\#(f) \cdot \gamma_\#(g)$ and $\gamma_\#(f \cdot g)$, which is easy to write out. □

Def. (4.13.4.6) [Simple Spaces]. A space $X \in \mathcal{CG}$ is called a **simple topological space** if for any $x_0 \in X$, the action of $\pi_1(X, x_0)$ defined in(4.13.4.5) is trivial. ⌟

Def. (4.13.4.7) [Weak Homotopy Equivalences]. $f : X \to Y \in \mathcal{CG}$ is called a **weak homotopy equivalence** iff it induces isomorphism $\pi_n((X, x_0)) \cong \pi_n(Y, f(x_0))$ for any $n \in \mathbb{N}$ and $x_0 \in X$. ⌟

Prop. (4.13.4.8). Let $f_0, f_1 : X \to Y \in \mathcal{CG}$ be maps and $h : \mathbb{I} \times X \to Y$ be a homotopy $x_0 \in X$, then if $\gamma : \mathbb{I} \to Y : t \mapsto h(t, x_0)$, then

$$\gamma_\# \circ \gamma_\#(f_0)_* = (f_1)_*.$$

⌟

Proof: For $f : f : (\mathbb{I}^n, \partial I^n) \to (X, x_0)$ is easy to write out a homotopy between $\gamma_\#(f_0)_*(f)$ and $(f_1)_*(f)$. □

Cor. (4.13.4.9). Any homotopy equivalence is a weak homotopy equivalence. ⌟

Def. (4.13.4.10) [Relative Homotopy Groups]. For an inclusion $i : (A, *) \subset (X, *) \in \mathcal{T}op^{\mathrm{pt}}$, $n \in \mathbb{Z}_+$, define the **relative homotopy groups** $\pi_n(X, A) = \pi_n(X, A, *) = \pi_{n-1}(P(X; *, A))$, where $P(X; *, A)$ is the homotopy fiber of i**?**. Equivalently, if we denote $\mathbb{J}^n = \partial\mathbb{I}^{n-1} \times \mathbb{I} \cup \mathbb{I}^{n-1} \times \{0\} \subset \mathbb{I}^n$ for $n \geq 2$ and $\mathbb{J}^1 = \{0\} \subset \mathbb{I}^1$, then

$$\pi_n(X, A) = [(\mathbb{I}^n, \partial\mathbb{I}^n, \mathbb{J}^n), (X, A, *)].$$

This is a pointed set for $n = 1$, a group for $n = 2$, and an Abelian group for $n \geq 3$. ⌟

Prop. (4.13.4.11) [Long Exact Sequence of Relative Homotopy Groups]. ⌟

Proof: □

Cor. (4.13.4.12) [Covering Spaces and Homotopy Groups]. If $E \to B$ is a covering space, then $\pi_n(E) \to \pi_n(B)$ is an isomorphism for $n \geq 2$. ⌟

Prop. (4.13.4.13). If $X \in \mathcal{CG}^{\mathrm{pt}}$ is contractible, then $\pi_n(X) = 0$ for any $n \geq 0$. ⌟

Prop. (4.13.4.14) [Products and Homotopy Groups]. For $X, Y \in \mathcal{CG}^{\mathrm{pt}}$, $\pi_n(X \times Y) = \pi_n(X) \times \pi_n(Y)$ for any $n \in \mathbb{N}$. ⌟

Prop. (4.13.4.15) [Colimits and Homotopy Groups]. If $X = \varinjlim_i X_i \in \mathcal{CG}^{\mathrm{pt}}$ is a filtered colimits, there are natural isomorphisms

$$\varinjlim_i \pi_n(X_i) \cong \pi_n(X)$$

for each $n \in \mathbb{N}$. ⌟

Proof: This follows from the fact any compact subset of X is contained in some X_i**?**. □

Def. (4.13.4.16)[n-Connectedness]. For $n \in \mathbb{N}$, $(X, A) \in \mathcal{CG}^{\mathrm{rel,pt}}$ is called **n-connected** if $\pi_i(X, A) = *$ for any $i \leq n$. $X \in \mathcal{T}\mathrm{op}^{\mathrm{pt}}$ is called n-connected if $\pi_i(X) = *$ for any $i \leq n$. ⌟

Def. (4.13.4.17) [n-Equivalences]. For $n \in \mathbb{Z}_+$, $f : (X, A) \to (Y, B) \in \mathcal{T}\mathrm{op}^{\mathrm{rel}}$ is called an **n-equivalence** if $f_* : \pi_p(X, A) \to \pi_p(Y, B)$ are isomorphisms for $p < n$, and surjective for $p = n$. ⌟

Thm. (4.13.4.18) [Excision for Homotopy Groups]. if $m, n \geq 0, (X; A, B)$ is an excisive triad s.t. $(A, A \cap B)$ is m-connected and $(B, A \cap B)$ is n-connected, then $(A, A \cap B) \to (A \cup B, A)$ is an $m + n$-equivalence. ⌟

Proof: Cf.[Hatcher P360]. □

Cor. (4.13.4.19). For $n > 1$, $\pi_n(\bigvee_\alpha S^\alpha)$ is free Abelian with $\pi_n(S^n)$ as generators. This is because $(\prod_\alpha S^n, \bigvee_\alpha S^n)$ is $(2n-1)$-connected thus use excision, because $\pi_n(\prod_\alpha S^n)$ is easy to calculate. ⌟

Prop. (4.13.4.20). If $f : X \to Y$ is an n-equivalence between $(n-1)$-connected spaces, then the quotient map $\mathrm{pr} : (M(f), X) \to (C(f), *)$ is an $2n$-equivalence. And if X, Y are both n-connected, then pr is an $2n+1$-equivalence. ⌟

Proof: □

Cor. (4.13.4.21)[Quotients and Homotopy Groups]. For $n \in \mathbb{Z}_+$, if $i : A \to X$ is a cofibration that is a n-equivalence of $(n-1)$-connected space, then the map $(X, A) \to (X/A, *)$ is a $2n$-equivalence. And if A, X are n-connected, then this is a $2n+1$-equivalence. ⌟

Proof: This follows from the commutative diagram

$$\begin{array}{ccc} (M(i), A) & \longrightarrow & (C(i), *) \\ \downarrow & & \downarrow \\ (X, A) & \longrightarrow & (X/A, *) \end{array}$$

where the vertical maps are homotopy equivalences, by(4.13.6.7). □

Prop. (4.13.4.22) [Suspension and Homotopy Groups, Freudenthal]. For $X \in \mathcal{CG}^{\text{well-pt}}$, there are maps

$$\Sigma_* : \pi_p(X) \to \pi_{p+1}(\Sigma(X)) : f \in \langle \mathbb{S}^p, X \rangle \mapsto \Sigma(f) \in \langle \mathbb{S}^{p+1} \cong \Sigma(\mathbb{S}^p), \Sigma(X) \rangle (4.13.1.13).$$

Then if $n \in \mathbb{N}, X \in \mathcal{CG}^{\text{well-pt}}$ and X is n-connected, then Σ_* is bijective for $p \leq 2n$ and surjective for $p = 2n+1$.

In particular, $\Sigma^n(X)$ is $(n-1)$-connected. ⌟

Proof: Cf.[May, P85]. □

Def. (4.13.4.23)[Stable Homotopy]. For $X \in \mathcal{CG}^{\text{well-pt}}$, using the suspension(4.13.4.22), we can form the colimit

$$\pi_p^s(X) = \varinjlim_{n\in\mathbb{N}} \pi_{p+n}(\Sigma^n(X)).$$

Then by(4.13.4.22),

$$\pi_p^s(X) = \pi_{p+n}(\Sigma^n(X)), \quad n \geq p+2.$$

⌟

Prop. (4.13.4.24). The homotopic direct limit of a family of homotopy equivalence is a homotopy equivalence. Cf.[Morse Theory Milnor]. ⌟

Fundamental Groups

Def. (4.13.4.25) [Simply Connected]. A space is called **simply connected** if it is connected and $\pi_1(X, x) = 0$ for some point $x \in X$. ⌟

Prop. (4.13.4.26). For a connected subset $K \subset \mathbb{C}$, the following are equivalent:

- K is simply-connected,
- For any Jordan curve $\gamma \subset K$, $\text{int}(\gamma) \subset K$.
- $\mathbb{P}^1(\mathbb{C}) \setminus K$ is connected.

Is this really true? ⌟

Proof: 3 → 2: If $\gamma \subset K$ is a Jordan curve, $\text{int}(\gamma)$ and $\text{Ext}(\gamma)$ is an open partition of $\mathbb{P}^1(\mathbb{C}) \setminus K$. As $\mathbb{P}^1(\mathbb{C}) \setminus K$ is connected, $\text{int}(\gamma) \setminus K = \varnothing$.
? □

Def. (4.13.4.27) [Semilocally Simply Connected]. A space is called **semilocally simply connected** if for any point $x \in X$, there is a nbhd U of x that the image of the inclusion-induced map $\pi_1(U, x) \to \pi_1(X, x)$ is trivial. ⌟

Prop. (4.13.4.28) [Van Kampen]. If X is a union of path-connected subsets A_α all containing x_0 that $A_\alpha \cap A_\beta$ and $A_\alpha \cap A_\beta \cap A_\gamma$ are all path-connected, then $*\pi_1(A_\alpha)/\sim$ where $\sim$ is generated by $i_*(\pi_1(A_\alpha \cap A_\beta)) \in \pi_1(A_\alpha) \sim i_*(\pi_1(A_\alpha \cap A_\beta)) \in A_\beta$ for every α, β. ⌟

Proof: Cf.[Hatcher P52]. □

Prop. (4.13.4.29) [Wedge Sums]. If $X_i \in \mathcal{CG}^{\text{well-pt}}$ and $X = \bigvee X_i$, then $\pi_1(X) = *_i\pi_1(X_i)$. ⌟

5 CW Approximations

Prop. (4.13.5.1) [CW Complex has Homotopy Extension Property]. For $(X, A) \in \mathcal{CW}^{\text{rel}}$, $X \times \{0\} \cup A \times I$ is a deformation retract of $X \times I$, thus (X, A) has the homotopy extension property(4.13.6.1). ⌟

Proof: Cf.[Hat02]P15. □

Lemma (4.13.5.2) [Compression and Homotopies]. For $n \in \mathbb{Z}_+$, $f : B \to Y \in \mathcal{CG}$, the following are equivalent:

- f_* induces an injection on π_n and a surjection on π_{n+1}.
- Any map $(\mathbb{D}^n, \mathbb{S}^n) \to (Y, B) \in \mathcal{T}\mathrm{op}^{\mathrm{rel}}$ is homotopic rel $\mathbb{S}^n$ to a map $\mathbb{D}^n \to B$.

⌟

Proof: Cf.[May, P70].? □

Thm. (4.13.5.3) [Compression Theorem]. If $n \in \mathbb{Z}_+$, $(X, A) \in \mathcal{CW}^{\mathrm{rel}}$ has relative dimension$\leq n$ and $f : B \to Y$ an n-equivalence, then any map $(X, A) \to (Y, B) \in \mathcal{CG}^{\mathrm{rel}}$ is homotopic rel A to a map $X \to B$.

In particular, (relative) homotopy doesn't depend on (2-degree)higher dimensional cells, (but might on lower one). ⌟

Proof: Use(4.13.5.2) on each cells. □

Thm. (4.13.5.4) [Whitehead]. If $f : Y \to Z \in \mathcal{CG}$ is an n-equivalence, then $[X, Y] \to [X, Z]$ is bijective for $X \in \mathcal{CW}^{\mathrm{pt}}$ of dimension$\leq n-1$, and surjective for $\dim X = n$. ⌟

Proof: The surjectivity follows from the compression theorem for the pair $(\varnothing, X) \in \mathcal{CW}^{\mathrm{rel}}$, and the injectivity follows from the compression theorem applied to $(X \times \mathbb{I}, X \times \partial\mathbb{I}) \in \mathcal{CW}^{\mathrm{rel}}$. □

Cor. (4.13.5.5). If $Y \to Z \in \mathcal{T}\mathrm{op}^{\mathrm{pt}}$ is a weak-equivalence, then $\langle X, Y\rangle \to \langle X, Z\rangle$ is an equivalence for any $X \in \mathcal{CW}^{\mathrm{pt}}$. ⌟

Cor. (4.13.5.6) [Whitehead]. For $n \in \mathbb{Z}_+$, an n-equivalence of CW complexes of dimension$\leq n-1$ is a homotopy equivalence.

A weak equivalence of CW complexes is a homotopy equivalence. ⌟

Proof: Let $e : Y \to Z \in \mathcal{CW}$ satisfies the hypothesis, then because $e_* : [Z, Y] \to [Z, Z]$ is a bijection by compression theorem(4.13.5.3), there exists $f : Z \to Y$ s.t. $e \circ f \cong \mathrm{id}$. Thus $e \circ f \circ e \cong e$. Then since $e_* : [Y, Y] \to [Y, Z]$ is also a bijection by compression theorem, $f \circ e \cong \mathrm{id}$. □

Cor. (4.13.5.7). If $X \in \mathcal{CW}^{\mathrm{pt}}$ and $\pi_n(X) = 0$ for all n, then X is contractible. ⌟

Cor. (4.13.5.8) [Whitehead Combinatorial Homotopy Theorem I]. ?If M and K is dominated by CW complexes, then any weak homotopy equivalence is an homotopy equivalence. If the map is an inclusion, then it is a deformation retract. In particular, if M is manifold, then it is dominated by its tubular nbhd, so this theorem is applied. ⌟

Proof: For inclusion, use compression, and in general use mapping cylinder and cellular approximation. □

Cellular and CW Approximations

Lemma (4.13.5.9). For $n \in \mathbb{Z}_+$, f $(X, A) \in \mathcal{CW}^{\mathrm{rel}}$ has no m-cells for $m \leq n$, then (X, A) is n-connected. In particular, (X, X^n) is n-connected. ⌟

Proof: It suffices to show that any map $f : (\mathbb{I}^n, \partial\mathbb{I}^n, \mathbb{J}^n) \to (X, A, *)$ is homotopic to a map $(\mathbb{I}^n, \mathbb{J}^n) \to (A, *)$ rel $\mathbb{J}^n$(4.13.4.1). For this, notice that the image is compact, thus we can assume that (X, A) is finite?. Thus by doing one cell by one cell, it suffices to show for $X = A \coprod_{f, \mathbb{S}^n} \mathbb{D}^n$. In this case, notice that by simplicial approximation, we can find a homotopic map $f \cong f'$ that f' avoids some point in $(\mathbb{D}^n)^o$?. Then we can use projection to construct a homotopy. □

Thm. (4.13.5.10) [Cellular Approximationss]. Any map $f : (X, A) \to (Y, B) \in \mathcal{CW}^{\text{rel}}$ is homotopic rel A to a cellular map.

In particular, any $f : X \to Y \in \mathcal{CW}$ is homotopic to a cellular map. ⌟

Proof: This follows from(4.13.5.9). □

Remark (4.13.5.11). The cellular approximation makes the computation of homotopy theoretically easier, but the difficulty comes from the complexity of the homotopy group of the sphere. ⌟

Remark (4.13.5.12). In fact, all the rest of this subsubsection can be rewritten by the geometric realization functor $\Gamma(X) \to X$(4.6.3.8). It is functorial in the level of spaces.? ⌟

Prop. (4.13.5.13) [n-Connected CW Models]. For a pair (A, X), if A is CW complex, then there is a n-connected(4.13.4.16) CW pairs $(Z, A) \to (X, A)$ that is identity on A, and $\pi_i(Z) \to \pi_i(X)$ is isomorphism for $i > n$ and injection for $i = n$.

Such a pair (Z, A) is called a n-connected CW model of (X, A), and moreover it can be constructed from A by attaching cells of dimension greater than n. ⌟

Proof: Cf.[Hatcher P353]. □

Cor. (4.13.5.14). For an n-connected CW pair (X, A), there exist a homotopic $(Z, A) \cong (X, A)$ rel A that $Z\backslash A$ has only cells of dimension greater than n. ⌟

Proof: Choose the n-connected approximation as above. The map induce and isomorphism on $\pi_{>n}$ by definition and on $\pi_{<n}$ because $\pi_i(A) \to \pi_i(Z)$ and $\pi_i(A) \to \pi_i(X)$ are isomorphisms. And on π_n, it is injective by definition and surjective because $\pi_n(A) \to \pi_n(Z) \to \pi_n(X)$ is isomorphism. Hence we know that the collapsed mapping cylinder at is weak-homotopy equivalent to Z, thus it deforms into Z by(4.13.5.8), thus $Z \to X$ rel A by(4.13.1.5). □

Cor. (4.13.5.15) [Functorial CW Approximations]. A **CW approximation** of a space X is a CW complex Z and a weak homotopy equivalence $Z \to X$. A **CW approximation** of a pair (X, A) is pair of CW complexes (Z, Z_0) and a morphism $(Z, Z_0) \to (X, A)$ that induces isomorphisms on both relative and absolute homotopy groups.

Thus there exists a CW approximation for any space A, and also there exists a CW approximation for any pair (X, X_0). ⌟

Proof: Just choose A to be a set containing a point for each connected component of X, then $\pi_0(Z) \to \pi_0(X)$ is surjective hence injective.

For pairs, first approximate X_0 and use the mapping cylinder to get a embedding.? □

Prop. (4.13.5.16) [Functoriality of CW Models]. Given n-connected CW model $f : (Z, A) \to (X, A)$ and $f' : (Z', A') \to (X', A')$, then any map of pairs $g : (X, A) \to (X', A')$ can be extended to a map of pairs $h : (Z, A) \to (Z', A')$ that $gf \cong f'h$ rel$A$. And such a map h is unique up to homotopy rel$A$. ⌟

Proof: Cf.[Hatcher, P355]. □

Cor. (4.13.5.17) [Uniqueness of CW approximation]. The CW approximation is unique up to homotopy. ⌟

Cor. (4.13.5.18) [Localizing Category]. Together with Whitehead combinatorial homotopy theorem(4.13.5.8) the homotopy category of spaces defined in(4.6.2.3) is the category of spaces $\mathcal{CG}$ localized by the class of weak homotopy equivalence classes. ⌟

Prop. (4.13.5.19) [CW Approximation of Excisive Triads]. Cf.[May, 79]. ⌟

6 Fibrations and Cofibrations

Cofibrations

Def. (4.13.6.1) [Homotopy Extension Property]. $(X, A) \in \mathcal{T}\mathrm{op}^{\mathrm{rel}}$ is said to satisfy the **homotopy extension property** if every map $X \times \{0\} \coprod_{A\times\{0\}} A \times I \to Y$ can be extended to a map $X \times I \to Y$. ⌟

Def. (4.13.6.2) [Cofibrations]. A **cofibration** is a map $j : A \to X$ that for every map $X \times \{0\} \coprod_{A\times\{0\}} A \times I \to Y$ can be extended to a map $X \times I \to Y$.

This implies $X \times \{0\} \cup A \times \mathbb{I} \to X \times \mathbb{I}$ has a left inverse. And the converse is clearly true.

Then a cofibration is just a topological embedding with closed image that (X, A) has the homotopy extension property(4.13.6.1).

Cofibrations is stable under cobase change and coproducts. ⌟

Proof: ? □

Def. (4.13.6.3) [NDR-Pairs]. An neighborhood deformation retraction pair, or an **NDR-pair** is a pair $(X, A) \in \mathcal{T}\mathrm{op}^{\mathrm{rel}}$ s.t. there is a map $u : X \to \mathbb{I}$ s.t. $u^{-1}(0) = A$, and a homotopy $f_t : X \to X \operatorname{rel} A$ s.t. $f_0 = \mathrm{id}_X$, and $f_1(u^{-1}([0, 1)) \subset A$. ⌟

Prop. (4.13.6.4) [NDR Pairs and Cofibrations]. If $A \subset X$ is closed, then (X, A) is a NDR-pair(4.13.6.3) iff $A \to X$ is a cofibration. ⌟

Proof: Cf.[May, P45].? □

Prop. (4.13.6.5) [CW-Pairs are Cofibrations]. By compression theorem(4.13.5.3), for any CW-pair (A, X), $A \to X$ is a cofibration. ⌟

Def. (4.13.6.6) [Hurewitz Cofibration]. A **closed Hurewicz cofibration** $i : A \subset B$ is a closed inclusion of spaces that $B \times \{0\} \coprod A \times \mathbb{I} \to B \times \mathbb{I}$ has left extension property w.r.t any map $Y \to \mathrm{pt}$. ⌟

Prop. (4.13.6.7) [Quotient a Contractible Cofibration]. If $A \to X$ is a cofibration and A is contractible, then the quotient map $X \to X/A$ is a homotopy equivalence. In particular, this applies to $(X, A) \in \mathcal{CW}^{\mathrm{rel}}$, by(4.13.5.1). ⌟

Proof: Let $f_t : X \to X$ be a homotopy extending a contraction of A to a point, with $f_0 = \mathrm{id}$. Since $f_t(A) \subset A$, they descends to a homotopy $\overline{f}_t : X/A \to X/A$. Because $f_1(A)$ is a point, there is a map g in the following diagram

$$\begin{array}{ccc} X & \xrightarrow{f_1} & X \\ \downarrow{\scriptstyle\pi} & \overset{g}{\nearrow} & \downarrow{\scriptstyle\pi} \\ X/A & \xrightarrow{\overline{f}_1} & X/A \end{array}.$$

So g and π are inverse homotopy equivalences, because $f_1 \cong f_0 = \mathrm{id}$ and $\overline{f}_1 \cong \overline{f}_0 = \mathrm{id}$. □

Prop. (4.13.6.8). Let X be a normal space, then an inclusion $j : A \hookrightarrow X$ is a cofibration iff $A \hookrightarrow V$ is a cofibration for some open nbhd V of $j(A) \subset X$. ⌟

Proof: Cf.[AGP02]P92. □

Prop. (4.13.6.9)[Homotopic Glueing Functions]. Let $A \to X_1$ be a cofibration with X Hausdorff, and we have attaching maps $f, g : A \to X_0$ that is homotopic, then $X_0 \coprod_f X_1 \cong X_0 \coprod_g X_1$ rel X_0. ⌟

Proof: Now choose a homotopy $H : A \times I \to X_0$ connecting f and g, then H induces a quotient space $Z = X_0 \coprod_H (X_1 \times I)$. Let $X = X_0 \coprod_f X_1, Y = X_0 \coprod_g X_1$, then there are natural inclusion maps $i : X_1 \to Z, j : \quad Y \to Z$, and there are also deformation retractions $Z \to X, Z \to Y$ constructed as follows:

Choose a deformation retraction r of $X_1 \times I$ onto $X_1 \times \{0\} \coprod A \times I$(4.13.6.1), and H induces a map $\overline{H} : D^n \times \{0\} \coprod S^n \times I \to S^n \coprod_f D^n$, making the following diagram commutative

$$\begin{array}{ccc} A \times I & \longrightarrow & X_1 \times I \\ & & \downarrow{\scriptstyle r} \\ \downarrow{\scriptstyle H} & & A \times I \coprod X_1 \times \{0\} \\ & & \downarrow{\scriptstyle \overline{H}} \\ X_0 & \xrightarrow{\text{id}} & X_0 \coprod_f X_1 \end{array}$$

which by definition defines a deformation retraction $r_1 : X_0 \coprod_H (X_1 \times I) \to X_0 \coprod_f X_1$. Similarly we have deformation retraction $r_2 : Z \to Y$. So $r_2 \circ i$ and $r_1 \circ j$ induce an homotopy equivalence between X and Y. □

Prop. (4.13.6.10). If $A \to X, A \to Y$ are cofibrations, and $f : X \to Y$ is a homotopy equivalence that $f|_A = \mathrm{id}_A$, then f is a homotopy equivalence rel A. ⌟

Proof: Cf.[Hatcher] P16. □

Cor. (4.13.6.11). If $j : A \to X$ is a cofibration which is also a homotopy equivalence, and X is Hausdorff, then A is a deformation retraction of X. ⌟

Serre Fibrations

Def. (4.13.6.12)[Serre Fibration]. A **Serre fibration** is the right lifting class of $D^n \times \{0\} \to D^n \times I$ for every n. This is equivalent to: for any homotopy of ∂D^n and a image D^n, there is a homotopy of D^n.

In particular, Serre fibrations are stable under base change, by(4.5.0.1). ⌟

Prop. (4.13.6.13). Being a Serre fibration is local on the target. ⌟

Proof: Cf.[Homotopical Point of View]P127. □

Prop. (4.13.6.14)[Long Exact Sequence of Serre Fibration]. Let $\pi : E \to X$ be a Serre fibration, let $b_0 \in B$ and $x_0 \in F = \pi^{-1}(b_0)$, then the map $\pi_* : \pi_n(E, F, x_0) \to \pi_n(B, b_0)$ is an isomorphism for all $n \geq 1$. In particular, there is a long exact sequence

$$\ldots \to \pi_n(F, x_0) \to \pi_n(E, x_0) \to \pi_n(B, b_0) \to \pi_{n-1}(F, x_0) \to \ldots \to \pi_0(B, b_0) \to 0.$$

by(4.13.4.11). ⌟

Proof: Cf.[Hat02]P376. [nLab]. □

Hurewicz Fibrations

Def. (4.13.6.15) [Hurewicz Fibrations]. A **Hurewicz fibration** is a map $p : X \to Y \in \mathcal{CG}$ that has right lifting property w.r.t maps $A \times \{0\} \to A \times [0,1]$ for any $A \in \mathcal{CG}$. in particular, a Hurewicz fibration is a Serre fibration(4.13.6.12).

Hurewicz fibrations are stable under base change. ⌟

Prop. (4.13.6.16) [Comparing Fibers of a Hurewicz Fibration]. If $\pi : E \to B$ is a Hurewicz fibration, then for any arc γ in B with $\gamma(0) = a, \gamma(1) = b$, there is a homotopy equivalence $f_\gamma : \pi^{-1}(a) \cong \pi^{-1}B$, and the homotopy class of f_γ only depends on the homotopy class of γ.

In other words, a Hurewicz fibration over B determines a contravariant functor $\Pi_1(B) \to \mathrm{Ho}(\mathcal{CG})$. ⌟

Proof: This follows from the homotopy lifting property. □

Cor. (4.13.6.17). For a Hurewicz fibration $E \to B$, if B is contractible, then it is fiber homotopy equivalent to a trivial fiber bundle. ⌟

Prop. (4.13.6.18). Let $\pi : E \to B, \pi' : E' \to B$ be Hurewicz fibrations and $f : E \to E'$ be a map over B that is also a homotopy equivalence, then f is a fiber homotopy equivalence. ⌟

Proof: Cf.[Miller, P141]**?** □

Prop. (4.13.6.19) [Homotopy Invariance of Pullbacks]. Let $\pi : E \to X$ be a Hurewicz fibration and $f_0, f_1 : Y \to X \in \mathcal{CG}$ are two maps that are homotopic, then the two Hurewicz fibrations $f_0^*E/Y, f_1^*E/Y$ are fiber homotopy equivalent. ⌟

Proof: Cf.[Miller, P140]**?** □

Prop. (4.13.6.20) [Homotopy Fiber of Contractible Fibration]. Let $f : E \to B$ be a Hurewicz fibration with E contractible, then the homotopy fibers(4.4.3.18) F over b_0 is weak homotopy equivalent to $\Omega(B, b_0)$. ⌟

Proof: Let $x_0 \in \pi^{-1}(b_0)$. If we compose the contraction of E to x_0 with π, then we get for each $x \in E$ a path γ_x from $\pi(x)$ to b_0. Then these give a map $E \to PB : x \mapsto \pi\gamma_x^{-1}$, which is a lift of π. Then this map gives a commutative diagram
$$\begin{array}{ccccc} F & \longrightarrow & E & \longrightarrow & B \\ \downarrow & & \downarrow & & \| \\ \Omega(B,b_0) & \longrightarrow & PB & \longrightarrow & B \end{array}$$
that gives a map of their corresponding long exact sequences(4.13.6.14). Thus $F \to \Omega(B, b_0)$ is a weak homotopy equivalence because E, PB are both contractible(4.4.3.20). □

Prop. (4.13.6.21) [Pathspaces are Hurewicz Fibrations]. For any map $f : A \to B$, the map $\pi : E_f \to B : (a, \gamma) \mapsto \gamma(1)$ from the pathspace(4.4.3.18) is a Hurewicz fibration.

In particular, take $A = \{x_0\}$, then the path space $PB \to B$ is a Hurewicz fibration. ⌟

Proof: Firstly this map is continuous by(4.4.3.5). To verify the homotopy lifting property, let $g_t : X \to B$ be a homotopy and $\widetilde{g}_0 : X \to E_f$ be a lifting, let $\widetilde{g}_0(x) = (h(x), \gamma_x)$. Define a lift $\widetilde{g}_t : X \to E_f$ by $\widetilde{g}_t(x) = (h(x), \gamma_x \cdot g_{[0,t]}(x))$. The second term is concatenation, which can be defined because $g_0(x) = \pi\widetilde{g}_0(x) = \gamma_x(1)$.

To check this is a continuous homotopy, by(4.4.3.7), it suffices to show $A \times I \times I \to B : (x, s, t) \mapsto \gamma_x \cdot g_{[0,s]}(x)(t) = \begin{cases} \gamma(x, (1+t)s) & s \le \frac{1}{1+t} \\ g_{(1+t)s-1}(x) & s \ge \frac{1}{1+t} \end{cases}$ is continuous. □

Cor. (4.13.6.22) [Homotopy Fibers]. We can embed A into E_f be mapping x to (x, γ_x), where γ_x is the trivial loop at x. Then A is a deformation contraction of E_f, by restricting to shorter and shorter initial segments: $H_t : E_f \to E_f : (a, \gamma) \mapsto (a, \gamma_t)$, where $\gamma_t(x) = \gamma(tx)$.

Then we factored f as a homotopy equivalence followed by a fibration: $A \to E_f \to B$.

If $x_0 \in X$ and F_f is the fiber of E_f over x_0, then a map $(I^{i+1}, \partial I^{i+1}, J^i) \to (A, B, x_0)$ is the same as a map $(I^i, \partial I^i) \to (F_f, \gamma_0)$, where γ_0 is the trivial loop at x_0. Thus $\pi_{i+1}(A, B, x_0) = \pi_i(F_f, \gamma_0)$. ⌟

Prop. (4.13.6.23) [Pathspace of a Hurewicz Fibration]. If $\pi : E \to B$ is a fibration, then the inclusion $E \to E_\pi$(4.13.6.22) is a fiber homotopy equivalence. In particular, the homotopy fibers of π are homotopy equivalent to the actual fibers. ⌟

Proof: □

Prop. (4.13.6.24) [Fibration Sequence]. Given a fibration $\pi : E \to B$ with $F = \pi^{-1}(b_0), x_0 \in F$, there is a sequence

$$\ldots \to \Omega^2(B, b_0) \to \Omega(F, x_0) \to \Omega(E, x_0) \to \Omega(B, b_0) \to F \to E \to B \to 0$$

where any two consecutive maps form a fibration, up to homotopy. ⌟

Proof: By(4.13.6.23), the inclusion i of F to the homotopy fiber F_π over π over p is a homotopy equivalence, and it extends to a map $i : F_p \to E : (x, \gamma) \mapsto x$, which is also a Hurewicz fibration, because it is the pullback of the fibration $PB \to B$(4.13.6.21).

Thus we can take the homotopy fiber F_i of $i : F_p \to E$ over x_0, and similarly there is a fibration $j : F_i \to F$, and F is naturally homotopic to the actual fiber of i, which is just $\Omega(B, b_0)$. □

Model Category Structures

Lemma (4.13.6.25)[Cofibrant Replacement]. Any map $f : X \to Y$ is a composition $X \to M_f \to Y$. Notice $M_f \to Y$ is a homotopy equivalence and $X \to M_f$ is cofibrant by(4.13.6.4). ⌟

Cor. (4.13.6.26) [Homotopy equivalence and mapping cylinder]. A map $f : X \to Y$ is a homotopy equivalence iff X is a deformation retraction of the mapping cylinder M_f. In particular, two spaces are homotopically equivalent iff there is a third space containing both of them as deformation retractions. ⌟

Proof: Cf.[Hatcher] P16. □

Lemma (4.13.6.27)[Fibrant Replacement]. Any map $f : X \to Y$ is a composition $X \to N(f) \to Y$, where $N(f) = X \times_Y Y^I$, where $Y^I \to Y$ is evaluation at $\{0\}$, and $X \to N(f)$ is given by $x \mapsto (x, c_{f(x)})$, where $c_{f(x)} \in Y^I$ is the constant map $f(x)$.

It is true that ⌟

Proof: $X \to N(f)$ is homotopy inverse to the projection map: We can use the homotopy $N(f) \times I \to N(f) : (\chi, a) \mapsto \chi_a : t \mapsto \chi(at)$.

To show that $N(f) \to Y$ is a fibration, Cf.[May, 50]**?**. □

Prop. (4.13.6.28)[Serre-Quillen]. The category $\mathcal{CG}$ can be given a **Serre-Quillen model structure** with

- Weak equivalences: weak homotopy equivalence,

- Fibrations: Serre fibrations,
- Cofibrations: Retracts of morphisms $X \to Y$ where Y is obtained from X by attaching cells.

⌟

Proof: Cf.[Homotopy Theories and Model Categories, Chap8]. □

Prop. (4.13.6.29). The homotopy category Ho($\mathcal{T}$op) of the Serre-Quillen model structure is equivalent to the homotopy category of spaces $\mathcal{H}$. ⌟

Proof:

□

Lemma (4.13.6.30). Every map can be decomposed as a homotopy equivalence followed by a fibration, by the construction of homotopy fibers. ⌟

Proof: □

Prop. (4.13.6.31) [Hurewicz-Str∅m]. The category $\mathcal{CG}$ can be given a **Hurewicz-Str∅m model structure** with

- Weak equivalences: homotopy equivalences.
- Cofibrations: closed Hurewicz cofibrations.
- Fibrations: Hurewitz fibrations.

⌟

Proof: Cf.[strum paper]. □

Prop. (4.13.6.32). The homotopy category of the Hurewicz-Str∅m model structure is equivalent to the usual category of homotopy types. ⌟

7 Calculations of Homotopy Groups

Prop. (4.13.7.1). For $0 < k < n \in \mathbb{Z}$, $\pi_k(\mathbb{S}^n) = 0$. And for $0 < n, \pi_0(\mathbb{S}^n) = *$. ⌟

Proof: This follows from cellular approximation(4.13.5.10) and the canonical CW structure on $\mathbb{S}^n$. □

Prop. (4.13.7.2). For $i \geq 2$, $\pi_1(\mathbb{RP}^i) \cong \mathbb{Z}/(2)$, and $\pi_n(\mathbb{RP}^i) \cong \pi_n(\mathbb{S}^i)$ for $n \neq 1$. ⌟

Proof: This follows from the fiber sequence $\mathbb{Z}/(2) \to \mathbb{S}^n \to \mathbb{RP}^n$ and(4.13.4.12). □

Lemma (4.13.7.3). There is a covering space $\mathbb{R} \to \mathbb{S}^1$ with fiber $\mathbb{Z}$, thus $\pi_1(\mathbb{S}^1) \cong \mathbb{Z}$. ⌟

Prop. (4.13.7.4) [Hopf Fibration]. By(4.15.1.12) and(4.13.6.14), there is a long exact sequence

$$\ldots \to \pi_i(\mathbb{S}^1) \to \pi_i(\mathbb{S}^3) \to \pi_i(\mathbb{S}^2) \to \pi_{i-1}(\mathbb{S}^1) \to \ldots \to \pi_0(\mathbb{S}^2) \to 1.$$

Thus $\pi_i(\mathbb{S}^3) \cong \pi_i(\mathbb{S}^2)$ for $i \geq 3$, and $\pi_2(\mathbb{S}^2) \cong \pi_1(\mathbb{S}^1) \cong \mathbb{Z}$(4.13.7.3). ⌟

Prop. (4.13.7.5) [Finiteness of Sphere Homotopy]. For $p > n > 1$, $\pi_p(\mathbb{S}^n)$ are all finite except for $\pi_{4n-1}(\mathbb{S}^{2n})$. ⌟

Proof: □

Prop. (4.13.7.6)[Basic Sphere Homotopy]. For $n \in \mathbb{Z}_+$, there are maps $\pi_i(S^n) \to \pi_{i+1}(S^{n+1})$ that is an isomorphism for $i < 2n-1$ and surjective for $i = 2n-1$.

In particular, $\pi_n(\mathbb{S}^n) \cong \pi_2(\mathbb{S}^2) \cong \mathbb{Z}$ for any $n \geq 2$. ⌟

Proof: This follows from Freudenthal suspension theorem(4.13.4.22). The last assertion follows from(4.13.7.3). □

Prop. (4.13.7.7). $\pi_4(\mathbb{S}^3) \cong \pi_4(\mathbb{S}^2) \cong \mathbb{Z}/(2)$. ⌟

Proof: □

Prop. (4.13.7.8). for $i \leq 2m$, $\pi_i G_m(\mathbb{C}^{2m}) \cong \pi_{i-1}U(m)$, and

$$\pi_{i-1}U(m) \cong \pi_{i-1}U(m+1) \cong \cdots .$$

and for $j \neq 1$, $\pi_j U(m) \cong \pi_j SU(m)$.

Similarly, $\pi_i \Omega_1(2m) \cong \pi_{i+1}O(2m)$ for $i \leq n-4$.(12.1.8.12),Cf[Morse Theory Milnor Prop23.4]. ⌟

Cor. (4.13.7.9)[Bott Periodicity theorem for Unitary Groups]. The stable homotopy group $\pi_i U$ has period 2. $\pi_{2k+1}U \cong 0$ and $\pi_{2k}U \cong \mathbb{Z}$. ⌟

Proof: Use the last proposition and long exact sequence to show that for $1 \leq i \leq 2m$,

$$\pi_{i-1}U = \pi_{i-1}U(m) \cong \pi_i G_m(\mathbb{C}^{2m}) \cong \pi_{i+1}SU(2m) \cong \pi_{i+1}U.$$

Notice that $U(m) \to U(2m)/U(m) \to G_m(\mathbb{C}^{2m})$ □

Prop. (4.13.7.10) [Bott Periodicity for O]. For the infinite dimensional orthogonal space O, $\Omega_8(16r) \cong O(r), \Omega_4(8r) \cong Sp(2r)$. So $\Omega_8 \cong O$ and $\Omega_4 O \cong Sp$. Thus by (4.13.4.2),

$$\pi_i(O) = \mathbb{Z}/(2), \mathbb{Z}/(2), 0, \mathbb{Z}, 0, 0, 0, \mathbb{Z} \ldots, \quad \pi_i(Sp) = 0, 0, 0, \mathbb{Z}, \mathbb{Z}/(2), \mathbb{Z}/(2), 0, \mathbb{Z} \ldots$$

respectively. (Use (12.1.8.13)) Cf.[Morse Theory Prop24.7]. ⌟

Prop. (4.13.7.11). If a simply-connected finite complex X is not contractible, then infinitely many of its homotopy groups are non-zero. ⌟

Proof: Cf.[Jean-Pierre Serre, Cohomologie modulo 2 des complexes d'Eilenberg-Maclane] □

4.14 Algebraic Topology II: Homologies and Cohomologies

Notation (4.14.0.1).

- Use notations defined in Algebraic Topology I: Homotopies.

⌟

1 Homologies

Axiomatic Homologies

Def. (4.14.1.1) [Eilenberg-Steenrod Homology Theories, Eilenberg-Steenrod1945]. A **Eilenberg-Steenrod homology theory** is given by the following data:

- A functor $E_p(-) : \mathrm{Ho}(\mathcal{T}\mathrm{op}^{\mathrm{rel}}) \to \mathcal{A}\mathrm{b}$ for any $p \in \mathbb{Z}$. For $X \in \mathcal{T}\mathrm{op}$, denote $H_p(X, \varnothing)$ by $E_p(X)$.
- For any $p \in \mathbb{Z}$, an equivariant **boundary map** $\partial : E_p(X, A) \to E_{p-1}(A)$ for any $(X, A) \in \mathrm{Ho}(\mathcal{T}\mathrm{op}^{\mathrm{rel}})$.

that satisfies

Exact Sequence: For $(X, A) \in \mathcal{T}\mathrm{op}^{\mathrm{rel}}$, there is a natural long exact sequence

$$\cdots \to E_p(A) \to E_p(X) \to E_p(X, A) \xrightarrow{\partial} E_{p-1}(A) \to \cdots .$$

Excision: For any excisive triad $(X; A, B)$(4.13.1.6), the inclusion $(A, A \cap B) \to (X, B)$ induces an isomorphism

$$E_p(A, A \cap B) \cong E_p(X, B)$$

Additivity: If $(X, A) = \coprod_\alpha (X_\alpha, A_\alpha)$, then there are natural isomorphisms

$$\bigoplus_\alpha E_p(X_\alpha, A_\alpha) \cong E_p(X, A).$$

By functorial CW approximations on relative spaces(4.13.5.15), CW approximation of excisive triads(4.13.5.19) and Whitehead theorem(4.13.5.6), such a theory is equivalent to a theory restricted to all CW complexes with cellular maps as morphisms. ⌟

Prop. (4.14.1.2)[Cofibrations]. Given an Eilenberg-Steenrod homology theory E_*, for any cofibration $i : A \to X \in \mathcal{T}\mathrm{op}$, there is a natural isomorphism

$$E_*(X, A) \cong E_*(X/A, *).$$

⌟

Proof: As i is a cofibration, $C(A) \to C(i) = X \coprod_{A\times\{0\}} C(A)$ is also a cofibration. Consider the commutative diagram

$$\begin{array}{ccc} E_*(X \coprod_{A\times\{0\}}(A \times [0, 2/3]), A \times [1/3, 2/3]) & \longrightarrow & E_*(C(i), (A \times [1/3, 1])/(A \times \{1\})) \\ \downarrow & & \downarrow \\ E_*(X, A) & \longrightarrow & E_*(X/A, *) \end{array} .$$

Then the upper horizontal map is an isomorphism by excision, and the vertical maps are isomorphisms by homotopy invariance: The right vertical map is

$$(C(i), (A \times [1/3, 1])/(A \times \{1\})) \cong (C(i), C(A)) \cong (X/A, *)$$

by(4.13.6.7). Then the lower horizontal map is also an isomorphism. □

Def. (4.14.1.3)[Reduced Homology Theories]. A **reduced Eilenberg-Steenrod homology theory** is given by the following data: A functor $\widetilde{E}_*(-) : \mathrm{Ho}(\mathcal{CG}^{\text{well-pt}}) \to \mathcal{A}\mathrm{b}$ for any $p \in \mathbb{Z}$ that satisfies
Exactness: For any cofibration $i : A \to X \in \mathcal{CG}^{\text{well-pt}}$, the sequences

$$\widetilde{E}_p(A) \to \widetilde{E}_p(X) \to \widetilde{E}_p(X/A)$$

are exact.
Suspension: For any $X \in \mathcal{CG}^{\text{well-pt}}$, there are natural isomorphisms

$$\Sigma_* : \widetilde{E}_p(X) \cong \widetilde{E}_{p+1}(\Sigma X).$$

Additivity: If $X = \bigvee_\alpha X_\alpha$, then there are natural isomorphisms

$$\bigoplus_\alpha \widetilde{E}_p(X_\alpha) \cong \widetilde{E}_p(X).$$

By functorial CW approximations on pointed spaces(4.13.5.15), such a theory is equivalent to a theory restricted to all CW complexes with cellular maps as morphisms. ⌟

Prop. (4.14.1.4)[Reduction to Reduced Homology Theories]. Giving an Eilenberg-Steenrod homology theory is equivalent to giving a reduced Eilenberg-Steenrod homology theory. Thus from now on we will not distinguish from a reduced ES-homology theory and an ES-homology theory. ⌟

Proof: Given an ES homology theory E_*, for $X \in \mathcal{T}\mathrm{op}^{\mathrm{pt}}$, define $\widetilde{E}_*(X) = E_*(X, *)$, then the maps $* \to X \to *$ induce a natural splitting $E_*(X) \cong \widetilde{E}_*(X) \oplus E_*(*)$. Then it is easy to show $\widetilde{E}_*$ is a reduced ES homology theory by(4.14.1.2): For suspension, because $C(X)$ is contractible and $X \to C(X)$ is a cofibration, the long exact sequence for $C(X)/X \cong \Sigma(X)$ and(4.14.1.2) implies the isomorphism

$$\Sigma^{-1} : \widetilde{E}_{p+1}(\Sigma(X)) \cong \widetilde{E}_{p+1}(C(X)/X) \cong E_{p+1}(C(X), X) \xrightarrow{\partial} \widetilde{E}_p(X).$$

Conversely, if $\widetilde{E}_*$ is a reduced ES homology theory, define $E_*(X, A) = \widetilde{E}_*(C(A \to X))$ where $C(A \to X)$ is pointed over the cone point. In particular, $E_*(X) = \widetilde{E}_*(X_+)$(4.13.1.16). We also define the boundary map as

$$\partial : E_*(X, A) \cong \widetilde{E}_*(C(i_+)) \xrightarrow{\partial} \widetilde{E}_*(\Sigma(A_+)) \xrightarrow{\Sigma^{-1}} E_{*-1}(A_+),$$

where ∂ comes from $\Sigma(A_+) \cong C(i_+)/X_+$.

To show E_* is a ES homology theory: additivity is clear. The homotopy invariance follows from(4.13.1.17). To show exactness**?**. To show excision**?**. Cf.[May, P110].

To show that these two constructions are inverse to each other, it suffices to show that the ∂ and Σ defined are inverse to each other**?**. □

Lemma (4.14.1.5). Let E be an ES-homology theory and $B \subset A \subset X$, then there is a functorial long exact sequence

$$\cdots \to E_p(A, B) \to E_p(X, B) \to E_p(X, A) \xrightarrow{\partial} E_{p-1}(A, B) \to \cdot,$$

where $\partial : E_p(X, A) \to E_{p-1}(A) \to E_{p-1}(A, B)$. ⌟

Proof: This follows from diagram chase or using the functorial CW approximations(4.13.5.15). □

Lemma (4.14.1.6). If E be an ES-homology theory and $(X; A, B)$ is an excisive triad, then the natural map

$$E_*(A, A\cap B)\oplus E_*(B, A\cap B)\to E_*(X, A\cap B)$$

is an isomorphism. ⌟

Proof: This is done by using the CW approximations for excisive triads(4.13.5.19). □

Prop. (4.14.1.7) [Mayer-Vietoris Sequences]. Let E be an ES-homology theory and $(X; A, B)$ be an excisive triad, then there is a long exact sequence

$$\cdots\to E_p(A\cap B)\xrightarrow{((i_1)_*,(i_2)_*)} E_p(A)\oplus E_p(B)\xrightarrow{(j_1)_*-(j_2)_*} E_p(X)\xrightarrow{\Delta} E_{p-1}(A\cap B)\to\cdots,$$

where Δ is the composite

$$E_p(X)\to E_p(X,B)\cong E_p(A, A\cap B)\xrightarrow{\partial} E_{p-1}(A\cap B).$$

⌟

Proof: Cf.[May, P112]. □

Prop. (4.14.1.8) [Relative Mayer-Vietoris Sequences]. The relative MV-sequence is related to the MV-sequence(4.14.1.7) by

$$\begin{array}{ccccccccc}
\cdots\longrightarrow & E_p(Y, A\cap B) & \longrightarrow & E_p(Y,A)\oplus E_p(Y,B) & \longrightarrow & E_p(Y,X) & \longrightarrow & E_{p-1}(Y, A\cap B) & \longrightarrow\cdots \\
& \downarrow\partial & & \downarrow\partial\oplus\partial & & \downarrow\partial & & \downarrow\partial & \\
\cdots\longrightarrow & E_p(A\cap B) & \longrightarrow & E_p(A)\oplus E_p(B) & \longrightarrow & E_p(X) & \longrightarrow & E_{p-1}(A\cap B) & \longrightarrow\cdots
\end{array}$$

⌟

Prop. (4.14.1.9) [Colimits]. If $X=\varinjlim_{i\in\mathbb{N}} X_i$, then there is a natural isomorphism

$$\varinjlim E_*(X_i)\cong E_*(X).$$

⌟

Proof: Cf.[May, P115]. □

Cor. (4.14.1.10). For a reduced ES-homology theory $\widetilde{E}_*$ and $(X_i)_{i\in\mathbb{N}}\in\mathcal{T}\mathrm{op}^{\mathrm{pt}}$, there are natural isomorphisms

$$\varinjlim \widetilde{E}_*(X_i)\cong \widetilde{E}_*(\prod_i{}' X_i)(4.13.1.19).$$

⌟

<u>**The Ordinary Homology Theory**</u>

Def. (4.14.1.11) [Ordinary Homology Theories]. For $\Lambda\in\mathcal{A}\mathrm{b}$, an **ordinary homology theory** with coefficients in Λ is a generalized homology theory(4.14.2.1) that satisfies the additional axiom

Dimension: $E_p(\mathrm{pt})=\begin{cases}\Lambda & ,p=0\\ 0 & ,p\neq 0\end{cases}.$

⌟

Def. (4.14.1.12) [Ordinary Reduced Homology Theories]. For $\Lambda \in \mathcal{A}b$, an **ordinary reduced homology theory** with coefficients in Λ is a reduced homology theory(4.14.1.3) that satisfies the additional axiom

Dimension: $\widetilde{E}_p(S^0) = \begin{cases} \Lambda & , p = 0 \\ 0 & , p \neq 0 \end{cases}.$

⌟

Def. (4.14.1.13)[Hurewicz Homomorphism]. For an ordinary homology theory H_*, if we denote the generator of $\widetilde{H}_0(\mathbb{S}^0)$ by a_0, and $a_n = \Sigma^n(a) \in \widetilde{H}_n(\mathbb{S}^n)$, then for any $X \in \mathcal{CG}^{\mathrm{pt}}$, define the **Hurewicz homomorphism**

$$\mathrm{Hur}_X : \pi_n(X) \to \widetilde{H}_n(X) : f \mapsto f_*(a_n).$$

⌟

Prop. (4.14.1.14). For $n \in \mathbb{Z}_+, X \in \mathcal{T}\mathrm{op}^{\mathrm{pt}}$, Hur_X is a homomorphism of groups. ⌟

Proof: Cf.[May, P117]. □

Prop. (4.14.1.15) [Generalized Hurewicz theorem]. If $n \geq 2$ and (X, A) is a $(n-1)$-connected pair of spaces, then the Hurewicz map induces an isomorphism

$$\pi_n(X, A)/ \sim \pi_1(A) \cong H_n(X, A),$$

and $H_k(X, A) = 0, k < n$. Moreover, the Hurewicz map $\pi_{n+1}(X, A) \to H_{n+1}(X, A)$ is surjective. ⌟

Proof: Cf.[Hatcher P371 and 390Ex23].? □

Cor. (4.14.1.16)[Converse Whitehead]. If $f : X \to Y$ is a map of simple pointed spaces that induces isomorphisms on all homology groups, then f is a weak homotopy equivalence. ⌟

Proof: We may change Y to the mapping cylinder of f, then notice all the relative homology groups $H_n(Y, X)$ vanishes by long exact sequence, and then by the generalized Hurewicz theorem, $\pi_n(Y, X) = 0$, and then f is a weak homotopy equivalence, by(4.13.4.11). □

Thm. (4.14.1.17) [Hurewicz]. For $n \in \mathbb{Z}_+$, if $X \in \mathcal{CG}^{\mathrm{pt}}$ is $(n-1)$-connected, then $\mathrm{Hur}_X : \pi_n(X) \to \widetilde{H}_n(X)$ induces an isomorphism $\pi_n(X)^{\mathrm{ab}} \cong \widetilde{H}_n(X)$. In particular, if $n > 1$, $\pi_n(X) \cong \widetilde{H}_n(X)$(4.13.4.1). ⌟

Proof: Cf.[May, P118]. □

The Cellular and Singular Realizations

Def. (4.14.1.18) [Degree of Maps]. For any $f : \mathbb{S}^n \to \mathbb{S}^n \in \mathcal{T}\mathrm{op}$, we can choose a base point and use cellular approximation to make it homotopic to a cellular map $(\mathbb{S}^n, *) \to (\mathbb{S}^n, *)$, and define the **degree of** f to be the multiplying factor of $f_* : \pi_n(\mathbb{S}^n) \cong \mathbb{Z} \to \pi_n(\mathbb{S}^n) \cong \mathbb{Z}$(4.13.7.6).

Then this degree is independent of the base point chosen simply by rotation. ⌟

Prop. (4.14.1.19). The antipodal map $\mathbb{S}^n \to \mathbb{S}^n$ has degree $(-1)^{n-1}$. ⌟

Proof: This is because the antipodal map is a composition of $n+1$ reflections, and each reflection is an n-suspension of a reflection on $\mathbb{S}^1 \to \mathbb{S}^1$, which clearly has degree -1. Thus we finish by(4.13.7.6). □

Def. (4.14.1.20) [Cellular Complex on $\mathcal{CW}$]. Given $X \in \mathcal{CW}$ with presentation $X = \cup_i X^i$, we can define the **cellular homology groups** as follows: Let $C_\bullet(X)$ be the complex with $C_p(X)$ the free Abelian group generated by the p-cells of X, and the map $C_p(X) \to C_{p-1}(X)$ is given by $e_\alpha \mapsto a_{\alpha\beta}e_\beta$, where for any n-cell α and $n-1$-cell β, $a_{\alpha\beta}$ is the degree(4.14.1.18) of the map

$$S^{p-1} \xrightarrow{\alpha} X^{p-1} \to X^{p-1}/X^{p-2} \xrightarrow{\beta^{-1}} S^{p-1}.$$

Then $C_\bullet(X)$ is truly a complex. More generally, for any $\Lambda \in \mathcal{A}\mathrm{b}$, we can define $C_\bullet(X;\Lambda) = C_\bullet(X) \otimes \Lambda$. ⌟

Proof: Cf.[May, P99]**?**. □

Def. (4.14.1.21) [Cellular Homology Groups]. For $X \in \mathcal{CW}$ and a subcomplex $A \subset X$, there is an inclusion $C_*(A) \to C_*(X)$. If we define $C_*(X, A) = C_*(X)/C_*(A)$. Define the homology groups $H_p(X) = H_p(C_\bullet(X)), H_p(X, A) = H_p(C_\bullet(X, A))$.

then the long exact sequence associated to the exact sequence $0 \to C_*(A) \to C_*(X) \to C_*(X, A) \to 0$ gives a boundary map $\partial : H_p(X, A) \to H_{p-1}(A)$.

More generally, for any $\Lambda \in \mathcal{A}\mathrm{b}$, we can define $C_\bullet(X, A; \Lambda)$ and also $H_p(X; \Lambda), H_p(X, A; \Lambda)$. ⌟

Def. (4.14.1.22)[Cellular Complex of Products]. For $X, Y \in \mathcal{CW}$, with the CW structure on $X \times Y$ given in(4.13.3.8), then

$$C_\bullet(X) \otimes C_\bullet(Y) \cong C_\bullet(X \times Y).$$

⌟

Proof: The map $C_\bullet(X) \otimes C_\bullet(Y) \cong C_\bullet(X \times Y)$ is given by $e_\alpha \otimes e_\beta \mapsto (-1)^{|\alpha||\beta|} e_{\alpha\times\beta}$.

It is clear that this is an isomorphism up to sign. Fo the sign problem, see [May, P101]. □

Prop. (4.14.1.23). The cellular homology groups in(4.14.1.21) defines a ES-homology theory(4.14.2.1). ⌟

Proof: For homotopy invariance, notice a homotopy $X \times I \to Y$ between $f, g : X \to Y$ will induce a map

$$C_\bullet(X) \otimes C_\bullet(\mathbb{I}) \to C_\bullet(Y)$$

by(4.14.1.22), and with the canonical CW structure, $C_\bullet(\mathbb{I})$ is just $0 \to \mathbb{Z} \xrightarrow{(1,-1)} \mathbb{Z} \oplus \mathbb{Z} \to 0$. By writting it out, this gives exactly a homotopy between the two maps f_*, g_*. Additivity, excision and exactness is clear. □

Def. (4.14.1.24) [Singular Homologies]. For $X \in \mathcal{T}\mathrm{op}, \Lambda \in \mathcal{A}\mathrm{b}$, the **singular cohomology groups** with coefficients in R is defined to be $H_{\mathrm{sing},*}(X; \Lambda) = H_*(\Gamma(X); R)$(4.6.3.8). This is the just the homology on $\mathcal{T}\mathrm{op}^{\mathrm{rel}}$ corresponding to the cellular homology on CW-pairs. ⌟

Thm. (4.14.1.25) [Uniqueness of Ordinary Homology Theories]. There exists a unique ordinary homology theory, i.e. the one defined in(4.14.1.21). ⌟

Proof: Cf.[May, P119]. □

2 Cohomologies

Remark (4.14.2.1) [Eilenberg-Steenrod Cohomology Theories]. The whole basic theory of cohomologies is dual to that of homologies, so it is omitted here.

We only focus on new features appearing. ⌟

Def. (4.14.2.2) [Cohomological Operators]. Given reduced ES-cohomology theories $\widetilde{E}^*, \widetilde{F}^*$, $p, n \in \mathbb{Z}$, a **cohomological operator** of type p and degree n is a natural homomorphism $\widetilde{E}^p \to \widetilde{F}^{p+n}$.

A **stable cohomological operator** of degree n is a sequence of cohomological operators Φ_p^n of type p and degree n that commutes with the suspension isomorphism. ⌟

Ordinary Cohomology Theories

Thm. (4.14.2.3) [Uniqueness of Ordinary Homology Theories]. There exists a unique ordinary cohomology theory, i.e. the one give by cellular cohomology groups. ⌟

Proof: The proof is the same as that of(4.14.1.25). □

Prop. (4.14.2.4) [Universal Coefficient Theorem]. See (4.8.7.6). ⌟

Cor. (4.14.2.5). A map between topological spaces that induce isomorphism on arbitrary homology group induce isomorphisms on cohomology groups. ⌟

Def. (4.14.2.6) [Cup Product]. For $X, Y \in \mathcal{CW}$, as $C_\bullet(X) \otimes C_\bullet(Y) \cong C_\bullet(X \times Y)$(4.14.1.22), for any $R \in \mathcal{CA}\mathrm{lg}$, there is a chain homomorphism

$$\mathrm{Hom}^\bullet(C_\bullet(X), R) \otimes \mathrm{Hom}^\bullet(C_\bullet(Y), R) \to \mathrm{Hom}^\bullet(C_\bullet(X \times Y), R),$$

which induces a natural **cross product map**

$$H^*(X; R) \otimes H^*(Y; R) \to H^*(X \times Y; R).$$

And composing with the diagonal map $\Delta_X : X \to X \times X$ gives a **cup product map**

$$H^*(X; R) \times H^*(X; R) \to H^*(X \times Y; R)$$

that makes $H^*(X; R)$ into a unital commutative graded R-algebra. ⌟

Proof: Cf.[May, P139]. □

Def. (4.14.2.7) [Bockstein Homomorphism]. ⌟

Prop. (4.14.2.8). the square of the Bockstein homomorphism $H^n(X, \mathbb{F}_p) \to H^{n+2}(X, \mathbb{F}_p)$ is trivial. ⌟

Proof: There is a commutative diagram of commutative rings

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times m} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/(m) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}/(m) & \xrightarrow{\times m} & \mathbb{Z}/(m^2) & \longrightarrow & \mathbb{Z}/(m) & \longrightarrow & 0 \end{array}$$

which induces commutative diagrams

$$\begin{array}{ccc} H^n(X,\mathbb{Z}/(m)) & \xrightarrow{\widetilde{\beta}} & H^{n+1}(X,\mathbb{Z}) \\ \| & & \downarrow \rho \\ H^n(X,\mathbb{Z}/(m)) & \xrightarrow{\beta} & H^n(X,\mathbb{Z}/(m)) \end{array}$$

so $\beta = \rho\widetilde{\beta}$, and $\beta^2 = \rho\widetilde{\beta}\rho\widetilde{\beta} = 0$, as $\widetilde{\beta}\rho = 0$ by long exact sequence. □

Prop. (4.14.2.9) [Lefschetz Fixed Point Theorem]. ⌟

Prop. (4.14.2.10) [Wedge Sums]. For $M, N \in \mathcal{T}\mathrm{op}$, $\widetilde{H}^i(M \wedge N) = \widetilde{H}^i(M) \otimes \widetilde{H}^i(N)$. ⌟

Proof: □

Prop. (4.14.2.11) [Connected Sums]. Let $M, N \in \mathcal{M}\mathrm{ani}^d_{,\mathrm{cntd},\mathrm{cpct}}$, the cohomology of $M\#N$ is **?**

And if M, N are orientable, then $H^*(M\#N) = 1 \oplus [\widetilde{H}^*(M) \oplus \widetilde{H}^*(N)/([M]-[N])]$. ⌟

Proof: As $M\#N/S^{d-1} = M \vee N$, there is a long exact sequence

$$\ldots \to \widetilde{H}^i(M \vee N) \to \widetilde{H}^i(M\#N) \to \widetilde{H}^i(S^{d-1}) \to \widetilde{H}^{i+1}(M\#N) \to \ldots$$

Thus by(4.14.2.10), $\widetilde{H}^i(M\#N) = \widetilde{H}^i(M) \oplus \widetilde{H}^i(N)$ for $i \neq d-1, d$. And there is an exact sequence

$$0 \to \widetilde{H}^{d-1}(M \vee N) \to \widetilde{H}^{d-1}(M\#N) \to \mathbb{Z} \to \widetilde{H}^d(M \vee N) \to \widetilde{H}^d(M\#N) \to 0.$$

If M, N are both orientable, then so does $M\#N$, and the sequence looks like

$$0 \to \widetilde{H}^{d-1}(M \vee N) \to \widetilde{H}^{d-1}(M\#N) \xrightarrow{0} \mathbb{Z} \to \mathbb{Z} \otimes \mathbb{Z} \to \mathbb{Z} \to 0.$$

and $\widetilde{H}^{d-1}(M \vee N) \cong \widetilde{H}^{d-1}(M\#N)$.

If only one of M, N is orientable, then similarly, $\widetilde{H}^{d-1}(M \vee N) \cong \widetilde{H}^{d-1}(M\#N)$.

If neither M, N are orientable, then nor does $M\#N$, and the sequence looks like

$$0 \to \widetilde{H}^{d-1}(M \vee N) \to \widetilde{H}^{d-1}(M\#N) \to \mathbb{Z} \to 0 \otimes 0 \to 0 \to 0.$$

which splits**?**, so $\widetilde{H}^{d-1}(M\#N) \cong \widetilde{H}^{d-1}(M \vee N) \oplus \mathbb{Z}$. □

Cup and Cap Products

Main references are [Hat02]Chap3.2.

Prop. (4.14.2.12). The cup product will restrict to a relative version:

$$H^*(X, A) \times H^*(X, B) \to H^*(X, A \cup B),$$

This implies that if X is a union of n contractible open set, then the cup product of n-elements vanish. In particular, the cup product in a suspension vanishes. ⌟

Prop. (4.14.2.13) [Künneth Formula]. The cross product $H^*(X,\mathbb{R}) \otimes_R H^*(Y,\mathbb{R}) \to H^*(X \times Y,\mathbb{R})$ is an isomorphisms of rings if X, Y are CW complexes and $H^*(Y,\mathbb{R})$ are a finite free R-modules for any k. ⌟

Proof: Cf.[Hat02]P219. □

Def. (4.14.2.14) [Cap Products]. ⌟

Cohomology of Fiber Bundles

Prop. (4.14.2.15) [Leray-Hirsch]. For a fiber bundle $F \to E \to B$ and a ring R s.t. $H^n(F,R)$ is f.g free for all n, and there exist classes c_j of $H^*(E)$ that constitute a basis for each fiber F, then

$$H^*(B,R) \otimes H^*(F,R) \to H^*(E,R)$$

is an isomorphism of $H^*(B,R)$-modules. ⌟

Proof:

□

Cor. (4.14.2.16).
- $H^*(U(n);\mathbb{Z}) = \Lambda_{\mathbb{Z}}[x_1, x_3, \ldots, x_{2n-1}]$.
- $H^*(SU(n,\mathbb{R});\mathbb{Z}) = \Lambda_{\mathbb{Z}}[x_3, \ldots, x_{2n-1}]$.
- $H^*(Sp(n);\mathbb{Z}) = \Lambda_{\mathbb{Z}}[x_3, x_7, \ldots, x_{4n-1}]$.

⌟

Prop. (4.14.2.17). $H^*(\mathbb{G}(n,\mathbb{K}^\infty);\mathbb{Z})$ where $\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{H}$ is generated by the symmetric polynomials, where for $\mathbb{R}$ the coefficient is $\mathbb{Z}_2$. ⌟

Proof: Use the flag variety and first calculate for ∞. Then use Poincare duality to show it is mapped onto the symmetric polynomials. Cf.[Hatcher P435]. □

Prop. (4.14.2.18) [Leray-Serre]. For a Serre fibration, e.g. fiber bundle, $F \to E \to B$, that B is simply connected, then there is a spectral sequence

$$E_2^{pq} = H_p(B, H_q(F)) \Rightarrow H_{p+q}(E) \quad E_2^{pq} = H^p(B, H^q(F)) \Rightarrow H^{p+q}(E)$$

⌟

Cor. (4.14.2.19) [Wang Sequence]. When $B = S^n$, there is a long exact sequence:

$$\cdots \to H_q(F) \to H_q(E) \to H_{q-n}(F) \to H_{q-1}(F) \to H_{q-1}(E) \to \cdots$$

⌟

Cor. (4.14.2.20) [Gysin Sequence]. When $F = S^n$, there is a long exact sequence:

$$\cdots \to H_{p-n}(B) \to H_p(E) \to H_p(B) \to H_{p-n-1}(B) \to H_{p-1}(E) \to \cdots$$

⌟

H-Spaces

Def. (4.14.2.21) [H-Spaces]. An **H-space** is a unital magma object in $\mathrm{Ho}(\mathcal{CG}^{\mathrm{pt}})$. Equivalently, an H-space is a pointed space $X \in \mathcal{CG}^{\mathrm{pt}}$ with a map $\mu : X \times X \to X \in \mathrm{Ho}(\mathcal{CG}^{\mathrm{pt}})$ s.t. $X \to \{*\} \times X \to X$ and $X \to X \times \{*\} \to X$ is homotopic to id_X.

An **associative H-space** is an H-space s.t. μ_X is associative in $\mathcal{T}\mathrm{op}^{\mathrm{pt}} / \sim$. Similarly, we can define group-H-spaces and commutative H-spaces.

An H-space is called strictly associative(or a monoid space) if it comes from a unital associative object in the category of spaces. ⌟

Remark (4.14.2.22). The definition of a H-space structure can be modified when X is a CW complex. In fact, when (X, e) is a CW-pair, if there exists a map $\mu : X \times X \to X$ and a point $e \in X$ that $X \to \{e\} \times X \to X$ and $X \to X \times \{e\} \to X$ is homotopic to id_X, then μ can be homotoped that e is a strict identity. ⌟

Proof: ? □

Prop. (4.14.2.23). If H is an H-space, then for any $X \in \mathcal{T}\mathrm{op}^{\mathrm{pt}}$, $\langle X, H\rangle$ is a magma. Moreover, if H is a commutative associative group H-space, then $\langle X, H\rangle \in \mathcal{A}\mathrm{b}$. ⌟

Prop. (4.14.2.24) [Loop Spaces are H-Spaces]. For any $X \in \mathcal{T}\mathrm{op}^{\mathrm{pt}}$, $\Omega(X)$ is an associative group-H-space, and $\Omega^2(X)$ is a associative commutative group-H-space. ⌟

Proof: The multiplication is given by concatenation of loops. It is continuous by adjunction arguments. □

Prop. (4.14.2.25). $\mathbb{CP}^\infty$ can be given a commutative strictly associative H-space structure. More generally, $B(\mathbb{Z}/n) \cong (\mathbb{C}^\infty\backslash\{0\})/(\mathbb{R}^+ \times \mu_n)$(4.15.3.13) can be given a commutative strictly associative H-space structure. In particular this applies to $\mathbb{RP}^\infty$. ⌟

Proof: We can regard $\mathbb{C}^\infty$ as the space of polynomials with complex coefficients, then the polynomial multiplication gives a map $(\mathbb{C}^\infty\backslash\{0\}) \times (\mathbb{C}^\infty\backslash\{0\}) \to \mathbb{C}^\infty\backslash\{0\}$ that descends to a map $B(\mathbb{Z}/n) \times B(\mathbb{Z}/n) \to B(\mathbb{Z}/n)$. And $e = (1, 0, \ldots, 0, \ldots)$ is the unit. □

Prop. (4.14.2.26). The James reduced product $J(X)$(4.13.3.20) is a strictly associative H-space with multiplication given by $(x_1, \ldots, x_n)(y_1, \ldots, y_m) = (x_1, \ldots, x_n, y_1, \ldots, y_m)$, and the identity e. This H-space structure also descends to a H-space structure on $SP(X)$(4.13.3.21). ⌟

Prop. (4.14.2.27). The universal cover of a H-space is a H-space. ⌟

Proof: Take an arbitrary lift that maps $(\tilde{e}, \tilde{e})$ to $\tilde{e}$. Notice the homotopy can also be lifted. □

Prop. (4.14.2.28) [Cohomology Ring]. The cohomology ring of a H-space is a topologists' Hopf algebra, by Kunneth formula and naturality. ⌟

Cor. (4.14.2.29). $\mathbb{CP}^n$ is not a H-space. ⌟

Proof: This is because $H^*(\mathbb{CP}^n, \mathbb{Z}) = \mathbb{Z}[\alpha]/\alpha^n, |\alpha| = 2$, which is a not a topologist's Hopf algebra, by(3.11.3.13). □

Prop. (4.14.2.30). The fundamental group of an H-space is Abelian. ⌟

Proof: This is because π_1 preserves products, so takes unital magma space to unital magma objects(4.1.1.71). And the unital magma objects in the category of groups is the Abelian groups(4.1.1.70). □

Prop. (4.14.2.31) [Adam]. $\mathbb{S}^0, \mathbb{S}^1, \mathbb{S}^3, \mathbb{S}^7$ are the only spheres that have H-structures. ⌟

Proof: Firstly $S^1 \subset \mathbb{C}, S^3 \subset \mathbb{H}, S^7 \subset \mathbb{O}$ are submonoids, so they have H-structures. ? □

Cor. (4.14.2.32). $\mathbb{RP}^n$ has a H-structure iff $n = 1, 3, 7$. ⌟

Proof: This is because the universal cover of a H-space is a H-space(4.14.2.27). Also $\mathbb{S}^1, \mathbb{S}^2, \mathbb{S}^3, \mathbb{S}^7$ are monoid spaces, and -1 are in their center, so the quotients are also monoid spaces. □

Examples of Calculations

Cor. (4.14.2.33).

$$H^*(\mathbb{RP}^n, \mathbb{F}_2) = \mathbb{Z}/(2)[a]/a^{n+1}, |a| = 1, \quad H^*(\mathbb{CP}^n, \mathbb{Z}) = \mathbb{Z}[\alpha]/\alpha^{n+1}, |\alpha| = 2$$

⌟

Proof: We prove for $\mathbb{RP}^n$, the $\mathbb{CP}^n$ case is similar. Use induction. For $n = 1$, this is clear. For $n > 1$, notice $\mathbb{RP}^n$ is the $n-1$-skeleton of $\mathbb{RP}^n$, thus the map of rings $H^*(\mathbb{RP}^n, \mathbb{F}_2) \to H^*(\mathbb{RP}^{n-1}, \mathbb{F}_2)$ maps the generator of $H^2(\mathbb{RP}^n, \mathbb{F}_2)$ to the generator a of $H^2(\mathbb{RP}^{n-1}, \mathbb{F}_2)$. Then by hypothesis $a^{n-1} \neq 0$. The $H^{n-1}(\mathbb{RP}^n, \mathbb{F}_2) \cong H_1(\mathbb{RP}^n, \mathbb{F}_2) \cong \mathbb{Z}/(2)$ is generated by α^{n-1}. Then the Poincaré duality shows that $\alpha \cup \alpha^{n-1} \neq 0$, so we are done. □

Cor. (4.14.2.34). For $n > 1$, the natural homomorphism $H^n(\mathbb{RP}^n, \mathbb{Z}/2\mathbb{Z}) \to H^n(\mathbb{S}^n, \mathbb{Z}/2\mathbb{Z})$ is 0. ⌟

Proof: Because the cohomology ring map maps $a \in H^1(\mathbb{RP}^n, \mathbb{Z}/2\mathbb{Z})$ to $0 \in H^1(S^n, \mathbb{Z}/2\mathbb{Z}) = 0$. □

Prop. (4.14.2.35) [$H^*(K, \mathbb{F}_2)$]. The cohomology ring of the Klein bottle K is $H^*(K, \mathbb{Z}/(2)) = \mathbb{F}_2[x, y]/(xy, x^2 - y^2, x^3, y^3)$. ⌟

Proof: Let $\varphi \in C^0(K, \mathbb{Z}/(2))$ be the dual of v, $\alpha, \beta, \gamma \in C^1(K, \mathbb{Z}/(2))$ be the dual of a, b, c, and $\mu, \lambda \in C^2(K, \mathbb{Z}/(2))$ be the dual of A, B, then

$$\partial(\varphi)(a) = \partial(\varphi)(b) = \partial(\varphi)(c) = 0$$

$$\delta(\alpha)(A) = \alpha(\partial(A)) = \alpha(a + b - c) = 1, \quad \delta(\alpha)(B) = \alpha(\partial B) = \alpha(b + c - a) = -1$$
$$\delta(\beta)(A) = \beta(\partial(A)) = \beta(a + b - c) = 1, \quad \delta(\beta)(B) = \beta(\partial(B)) = \beta(b + c - a) = 1$$
$$\delta(\gamma)(A) = \gamma(\partial(A)) = \gamma(a + b - c) = -1, \quad \delta(\gamma)(B) = \gamma(\partial(B)) = \gamma(b + c - a) = 1$$

So

$$H^0(K, \mathbb{Z}/(2)) = \mathbb{Z}/(2)\varphi, \quad H^1(K, \mathbb{F}_2) = \mathbb{F}_2(\alpha+\beta) \oplus \mathbb{F}_2(\alpha+\gamma), \quad H^2(K, \mathbb{F}_2) = (\mathbb{F}_2\mu \oplus \mathbb{F}_2\lambda)/(\mu+\lambda).$$

Now we calculate the cup product:

$$(\alpha + \beta) \cup (\alpha + \beta)(A) = (\alpha + \beta)(a) \cdot (\alpha + \beta)(b) = 1$$
$$(\alpha + \beta) \cup (\alpha + \gamma)(A) = (\alpha + \beta)(a) \cdot (\alpha + \gamma)(b) = 0$$
$$(\alpha + \gamma) \cup (\alpha + \gamma)(A) = (\alpha + \gamma)(a) \cdot (\alpha + \gamma)(b) = 0$$
$$(\alpha + \beta) \cup (\alpha + \beta)(B) = (\alpha + \beta)(b) \cdot (\alpha + \beta)(c) = 0$$
$$(\alpha + \beta) \cup (\alpha + \gamma)(B) = (\alpha + \beta)(b) \cdot (\alpha + \gamma)(c) = 1$$
$$(\alpha + \gamma) \cup (\alpha + \gamma)(B) = (\alpha + \gamma)(b) \cdot (\alpha + \gamma)(c) = 0$$

Then $(\alpha + \beta) \cup (\alpha + \beta) = (\alpha + \beta) \cup (\alpha + \gamma) = \mu \in H^2(K, \mathbb{Z}/(2))$. Now if we set $\alpha + \beta = x, \beta + \gamma = y$, then the cohomology ring

$$H^*(K, \mathbb{Z}/(2)) = \mathbb{Z}/(2)[x, y]/(xy, x^2 - y^2, x^3, y^3).$$

□

Prop. (4.14.2.36) [$H^*(L, \mathbb{Z}/(m))$]. Let L be the Lens space, then the cohomology ring is calculated at [Hat02]P304. ⌟

Proof: □

3 Manifolds

Orientations

Prop. (4.14.3.1). Let $d \in \mathbb{Z}_+, R \in \mathcal{CA}\mathrm{lg}, M \in \mathcal{M}\mathrm{ani}^d, X \subset M$, then for any $x \in M$, choose a nbhd U of $x \in M$ s.t. $U \cong \mathbb{R}^n$, then by excision and exactness,

$$H_d(M, M\backslash x) \cong H_d(U, U\backslash x) \cong \widetilde{H}_{d-1}(U\backslash\{x\}) \cong \widetilde{H}_{d-1}(\mathbb{S}^{d-1}) \cong R.$$

⌟

Prop. (4.14.3.2) [Vanishing]. For $M \in \mathcal{M}\mathrm{ani}^d_{\mathrm{cpct,cntd},\partial}, \Lambda \in \mathcal{A}\mathrm{b}$, $H_i(M;\Lambda) = 0$ for $i > d$, and $\widetilde{H}_d(M;\Lambda) = 0$ unless M is compact without boundary. ⌟

Proof: □

Def. (4.14.3.3) [R-Fundamental Class]. Let $R \in \mathcal{CA}\mathrm{lg}, M \in \mathcal{M}\mathrm{ani}^d_{\mathrm{cntd}}, X \subset M$, an **$R$-fundamental class** of M at X is an element $z \in H_d(M, M\backslash X)$ s.t. for any $x \in X$, the map

$$H_d(M, M\backslash X) \to H_d(M, M\backslash\{x\})$$

maps z to a generator of $H_d(M, M\backslash\{x\}) \cong R$(4.14.3.1). ⌟

Def. (4.14.3.4) [R-Orientation]. Let $R \in \mathcal{CA}\mathrm{lg}, M \in \mathcal{M}\mathrm{ani}^d_{\mathrm{cntd}}, X \subset M$, an **$R$-orientation** of M is an open cover $\{U_i\}$ of M and R-fundamental classes z_i of M at U_i s.t. z_i, z_j restricts to the same element in $H_d(M, M\backslash(U_i \cup U_j))$.

For $M \in \mathcal{M}\mathrm{ani}^d_{\mathrm{cntd},\partial}$, an R-orientation is an R-orientation of M^o. ⌟

Prop. (4.14.3.5) [R-Fundamental Classes and R-Orientations]. For $R \in \mathcal{CA}\mathrm{lg}, M \in \mathcal{M}\mathrm{ani}^d$ and $K \subset M$ compact, then

- $H_i(M, M\backslash K, R) = 0$ for $i > d$.
- Any R-orientation of M defines an R-fundamental class of M at K that is compatible for $x \in K$.

In particular, if M is compact, then an R-orientation is equivalent to an R-fundamental class. ⌟

Proof: Firstly, if $K \subset U$ and $U \cong \mathbb{R}^n$ is a coordinate chart on which the R-orientation is defined, then by excision and exactness,

$$H_i(M, M\backslash K, R) \cong H_i(U, U\backslash K, R) \cong H_{i-1}(U\backslash K, R)$$

which vanishes for $i > n$ by vanishing theorem(4.14.3.2). And the R-orientation restricts to K.

In general, K can be written as a sum of compact subsets each contained in a coordinate char on which the R-orientation is defined. Then using induction, it suffices to show that if the results hold for $K, L, K \cap L$, then it holds for $K \cup L$: item1 follows from the MV-sequence

$$H_{i+1}(M, M\backslash(K \cup L)) \to H_i(M, M\backslash(K \cup L)) \to H_i(M, M\backslash K) \oplus H_i(M, M\backslash L) \to H_i(M, M\backslash(K \cap L)).$$

For item2, the same MV-sequence with R-coefficients and $i = d$ together with the definition of R-orientation classes(4.14.3.4) shows there exists a fundamental class at $K \cap L$ that restricts to the fundamental classes at K and L. □

Prop. (4.14.3.6) [Orientation Dichotomy]. For $d \in \mathbb{Z}_+$, $M \in \mathcal{M}\text{ani}^d_{\text{cntd,cpct}}$, there are only two cases:

- M is non-orientable, and $H_d(M) = 0$.
- M is orientable, and the map $H_d(M) \to H_d(M, M\backslash\{x\}) \cong \mathbb{Z}$(4.14.3.1) is an isomorphism for any $x \in M$.

⌟

Proof: For any $R \in \mathcal{CA}\text{lg}$, as $M\backslash\{x\}$ is connected and non-compact, $H_d(M\backslash\{x\}; R) = 0$ by(4.14.3.2), thus

$$H_d(M, R) \to H_d(M, M\backslash\{x\}; R) \cong R$$

is injective. Thus $H_d(M) \cong 0$ or $\mathbb{Z}$. In particular, by universal coefficients theorem,

$$H_d(M) \otimes \mathbb{F}_p \to H_d(M, M\backslash\{x\}) \otimes \mathbb{F}_p$$

is injective for any $p \in \mathbf{P}$. Then it is clear to see that $H_d(M) \to H_d(M, M\backslash\{x\})$ is an isomorphism for any $x \in M$. □

Prop. (4.14.3.7) [Fundamental Classes on Manifolds with Boundaries]. For $M \in \mathcal{M}\text{ani}^d_\partial, \partial M \neq 0$, an R-orientation on M determines an R-orientation of ∂M. Moreover, the fundamental class $[\partial M]_R$ defined by(4.14.3.5) comes from the partial of a unique element $[M]_R \in H_d(M, \partial M; R)$, called the **$R$-fundamental class determined the orientation**. ⌟

Proof: By collar nbhd theorem, $M \cong M^o$, and by vanishing theorem, $H_d(M) \cong H_d(M^o) = 0$, thus $H_d(M, \partial M; R) \to H_{d-1}(\partial M; R)$ is injective. Let N be an open collar of ∂M, then $H_d(M^o, M^o \cap N; R) \cong H_n(M, \partial M; R)$. Also, $M\backslash N$ is compact, so the orientation on M^o defines a fundamental class in $H_d(M, M^o \cap N; R) \cong H_n(M, \partial M; R)$. Then this class determined the orientation on every point of M^o, and determines the orientation on ∂M, Cf.[May, P170]**?**. □

Prop. (4.14.3.8) [Orientation Coverings]. ⌟

Proof: □

Cor. (4.14.3.9). If $M \in \mathcal{M}\text{ani}^d_{\text{cntd}}$, then if M is orientable, it has exactly two orientations. And if M is simply connected or $\pi_1(M)$ has no subgroup of index 2, then M is orientable. ⌟

Def. (4.14.3.10) [Connected Sums]. For $M, N \in \mathcal{M}\text{ani}^d_{\text{cntd,cpct}}$, define the **connected sum** $M\#N$ as follows: Take a subset $D \subset M, D' \subset N$ that are contained in coordinate charts(orientable coordinates charts if M, N are oriented). $\varphi : U \cong \mathbb{R}^d, \varphi' : U' \cong \mathbb{R}^d$ s.t. $\varphi(D) \cong \mathbb{D}^d \cong \varphi(D')$. Then define

$$M\#N = (M\backslash D) \coprod_{\partial D \cong \partial D'} (N\backslash D')$$

where $\partial D \cong \partial D'$ is an orientation-reversing homeomorphism when M, N are both orientable. This is independent of D, D' and the homeomorphism $\partial D \cong \partial D'$ chosen. ⌟

Proof: Firstly we show that $M\backslash D$ is independent of D chosen: As M is locally path connected and connected, it is path connected, Then we can consider a chain of charts isomorphic to $\mathbb{R}^d$ that connects any two such subsets D, D'. Then reducing to affine charts, it suffices to show for the case $M \cong \mathbb{R}^d$. In this case, we can use isotopy of M to make $D \subset D'$, and then use the coordinate charts and annulus theorem(4.4.11.2) to show that $D'\backslash D$ is isomorphic to $\mathbb{S}^{d-1} \times \mathbb{I}$. Then the homeomorphism $M\backslash D \cong M\backslash D'$ can be easily given.

Now we show the connected sum is independent of the homeomorphism chosen: ∂D and $\partial D'$ are given orientations by the coordinate charts, and in the non-orientable case, use the argument above on the orientation covering of M(4.14.3.8), we know there exists a self-homeomorphism of M that is isotopic to id_M that reverses the orientation on ∂D. Thus in both cases, we can assume $\partial D \cong \partial D'$ is orientation-preserving. Now(4.13.2.3) shows any such homeomorphism is isotopic, and using the coordinate charts, we can extend the isotopy to a nbhd of nbhd of ∂D. Thus the connected sum is well-define. □

Remark (4.14.3.11). WARNING: The connected sum may be different in the orientable case if we change one of the orientations: $\mathbb{CP}^2\#\mathbb{CP}^2$ is not homeomorphic to $\mathbb{CP}^2\#\overline{\mathbb{CP}^2}$. ⌟

Proof:

□

Poincaré Duality

Lemma (4.14.3.12) [Poincaré Duality]. For $R \in \mathcal{C}\mathcal{A}\mathrm{lg}$, if $M \in \mathcal{M}\mathrm{ani}^d_{\mathrm{cntd,cpct}}$ is R-oriented, then for any $p \in \mathbb{Z}$, there is an isomorphism

$$D = - \cap [M]_R : H^p(M;R) \cong H_{n-p}(M;R).$$

In particular, $H^n(X, \mathbb{F}_2) \cong \mathbb{Z}/(2)$, and the non-trivial element is called the **fundamental homology class mod 2**, denoted by $[M]_2$. ⌟

Proof: which follows immediately from(6.8.6.30) and(6.3.5.9). (Should also attain the compact cohomology case if we know the relation of compact sheaf cohomology better). □

Prop. (4.14.3.13) [Relative Poincaré Duality]. Let $R \in \mathcal{C}\mathcal{A}\mathrm{lg}, M \in \mathcal{M}\mathrm{ani}^d_{\mathrm{cpct},\partial}$ be R-orientable with fundamental class $[M]_R \in H_d(M, \partial M; R)$, then for any $\Lambda \in \mathcal{M}\mathrm{od}_R$, capping with $[M]_R$ defines isomorphisms

$$H^p(M, \partial M; \Lambda) \cong H_{d-p}(M), \quad H^p(M;\Lambda) \cong H_{d-p}(M, \partial M; \Lambda).$$

⌟

Proof: Cf.[May, P170]**?**. □

Cor. (4.14.3.14). For $M \in \mathcal{M}\mathrm{ani}^d_{\mathrm{cntd,cpct,orntd}}$, for any $p \in \mathbb{Z}$, there is a perfect pairing

$$H^p(M)_{\mathrm{lf}} \times H^{n-p}(M)_{\mathrm{lf}} \to \mathbb{Z} : (\alpha, \beta) \mapsto \langle \alpha \cup \beta, [M] \rangle.$$

⌟

Proof: By universal coefficient theorem**?**, $H^p(M)_{lf} \cong \mathrm{Hom}(H_p(M), \mathbb{Z})$. So if $\alpha \in H^p(M)$ is non-zero in $H^p(M)_{\mathrm{lf}}$, there exists $a \in H_p(M)$ s.t. $\langle a, \alpha \rangle = 1$. Then by Poincaré duality(4.14.3.12), there exists $\beta \in H^{d-p}(M)$ s.t. $\beta \cap [M] = a$. Thus $\langle \alpha \cup \beta, [M] \rangle = \langle \alpha, \beta \cap [M] \rangle = 1$. □

Def. (4.14.3.15) [Intersection Pairing]. Let $k \in \mathbb{N}, M \in \mathcal{M}\mathrm{ani}^{2k}_{\mathrm{cpct,orntd,cntd}}$, The Poincaré duality(4.14.3.14) shows the cup product pairing

$$H^k(M;\mathbb{Q}) \times H^k(N;\mathbb{Q}) \to \mathbb{Q} : (\alpha, \beta) \mapsto \langle \alpha \cup \beta, [M] \rangle$$

is non-degenerate, called the **intersection pairing** of M. Notice if k is odd, it is skew-symmetric, and if k is even, it is symmetric. ⌟

Def. (4.14.3.16) [Index]. For $M \in \mathcal{M}\mathrm{ani}^d_{\mathrm{cpct,orntd,cntd}}$, define the **index of** M as the index of the symmetric intersection pairing of M if $d = 4k$, and 0 otherwise. The index of M is denoted by $I(M)$. ⌟

Prop. (4.14.3.17). For $M, N \in \mathcal{M}\mathrm{ani}_{\mathrm{cpct,orntd,cntd}}$, $I(M \times N) = I(M)I(N)$. ⌟

Proof: Cf.[May, P167]. □

Prop. (4.14.3.18). For $k \in \mathbb{N}, k \in$ `Field`, $M \in \mathcal{M}\mathrm{ani}^{2k+1}_{\mathrm{cpct},\partial}$, then

$$\dim_k H_k(\partial M; k) = 2 \dim \ker(H_k(\partial M; k) \xrightarrow{i_*} H_k(M; k)) = 2 \dim \mathrm{Im}(H^k(\partial M; k) \xrightarrow{i^*} H^k(M; k)).$$

⌟

Proof: There is a commutative diagram

$$\begin{array}{ccccc} H^k(\partial M; k) & \xrightarrow{i^*} & H^k(M; k) & \xrightarrow{\partial} & H^{k+1}(M, \partial M; k) \\ \downarrow D & & \downarrow D & & \downarrow D \\ H_{k+1}(M, \partial M; k) & \xrightarrow{\partial} & H_k(M; k) & \xrightarrow{i_*} & H_k(\partial M; k) \end{array}$$

where the vertical arrows are isomorphisms and i_* is the vector dual of i^* by universal coefficient theorem. Thus the theorem follows. □

Prop. (4.14.3.19) [Gysin Sequence]. Cf.[姜伯驹同调论]. ⌟

Euler Characteristic

Def. (4.14.3.20)[Euler Characteristic]. For any $X \in \mathcal{T}\mathrm{op}$ with finite $\mathbb{Z}$-homologies, define the **Euler character** of X to be

$$\chi(X) = \sum_i (-1)^i H_i(X; \mathbb{Z}).$$

Then by universal coefficients theorem(4.14.2.4),

$$\chi(X) = \sum_i (-1)^i H_i(X; k)$$

for any $k \in$ `Field`.

The condition holds for $X \in \mathcal{CW}^{\mathrm{fin}}$, in particular any $X \in \mathcal{M}\mathrm{ani}_{\mathrm{cpct}}$(4.13.3.10). ⌟

Prop. (4.14.3.21). For any $i \in \mathbb{N}, X \in \mathcal{M}\mathrm{ani}^{2i+1}_{\mathrm{cpct,cntd}}$, $\chi(X) = 0$. ⌟

Proof: This follows from Poincaré duality for $\mathbb{F}_2$-coefficients. □

Prop. (4.14.3.22) [Euler Characteristic and Boundary]. For $i \in \mathbb{N}, M \in \mathcal{M}\mathrm{ani}^{2i+1}_{\mathrm{cpct},\partial}$, then $\chi(\partial M) = 2\chi(M)$. ⌟

Proof: Consider the "double" $\widetilde{M}$ of M along ∂M, then $\widetilde{M} \in \mathcal{M}\mathrm{ani}^{2i+1}_{\mathrm{cpct}}$. It is clear by excision and collar neighborhood theorem that $\chi(\widetilde{M}) + \chi(\partial M) = 2\chi(M)$. Then we use(4.14.3.21). □

Cor. (4.14.3.23). If $N \in \mathcal{M}\mathrm{ani}_{\mathrm{cpct}}$ is a boundary of some other $M \in \mathcal{M}\mathrm{ani}_{\mathrm{cpct},\partial}$, then $\chi(N) = 0$. ⌟

Proof: If $\dim N$ is odd, this is(4.14.3.21). If $\dim N$ is even, this is(4.14.3.22). □

Prop. (4.14.3.24). For any $i \in \mathbb{N}$, $M \in \mathcal{M}\mathrm{ani}^{4i+2}_{\mathrm{cpct,orntd}}$, $\chi(M)$ is even. ⌟

Proof: The parity of $\chi(M)$ is the same as $H^{2i+1}(M,\mathbb{Q})$, which is odd by(4.14.3.15) and(3.5.10.22). □

Prop. (4.14.3.25) [Morse Inequality]. For any $X \in \mathcal{CW}$,

$$\chi(X) \leq \sum (-1)^i c_i(X),$$

where $c_i(X)$ is the number of I-dimensional cells. (Use the dimension counting of the long exact sequence). ⌟

Prop. (4.14.3.26). For $M \in \mathcal{M}\mathrm{ani}^d_{\mathrm{cpct,orntd,cntd}}$, $I(M) \equiv \chi(M) (\mathrm{mod}\ 2)$. ⌟

Proof: If d is odd, $I(M) = 0 = \chi(M)$ is even by(4.14.3.21). If $d = 4k+2$, then $I(M) = 0$ and $\chi(M)$ is even by(4.14.3.24). if $d = 4k$, then $I(M) \equiv \chi(M) \equiv \dim H^{2k}(M,\mathbb{Q})$. □

deRham Cohomology

Prop. (4.14.3.27) [de Rham Comparison]. For $X \in \mathcal{M}\mathrm{ani}_{\mathrm{sm}}, G \in \mathcal{A}\mathrm{b}$, by(6.3.5.11).

$$H^*_{\mathrm{dR}}(X,G) \cong H^*(X,\underline{G}).$$

⌟

Prop. (4.14.3.28)[Homotopy Axiom for deRham Cohomology]. For two homotopic map between two smooth manifold, they induce the same map on deRham Cohomology. ⌟

Proof: We only have to prove the case of $M \times \mathbb{R} \to M$, where any constant section map induces an isomorphism $H^*_{\mathrm{dR}}(M \times I) \cong H^*_{\mathrm{dR}}(M)$. Because any homotopy is a morphism $M \times I \to N$ where f and g are the sections 0 and 1.

For the zero section, we define $K : a + bdt \mapsto \int_0^t b$. This is the desired homotopy, Cf.[Differential Forms in Algebraic Topology Bott Tu]. □

4 Applications

Prop. (4.14.4.1) [No Contraction to the Boundary]. For $M \in \mathcal{M}\mathrm{ani}^d_{\mathrm{cpct},\partial}$, there are no retraction from M onto ∂M. ⌟

Proof: We may assume ∂M is connected and non-empty, otherwise clearly there are no retraction. If it has a retraction, $H_{d-1}(\partial M, \mathbb{F}_2) \to H_{d-1}(M, \mathbb{F}_2)$ has a left inverse. Thus It suffices to show that $H_{d-1}(\partial M, \mathbb{Z}/(2)) \to H_{d-1}(M, \mathbb{Z}/(2))$ is 0. So it suffices to show that $H_d(M, \partial M, \mathbb{Z}/(2)) \to H_{d-1}(\partial M, \mathbb{Z}/(2))$ is surjective. And this follows from(4.14.3.7) and(4.14.3.6) as the image of $[M]_2$ is $[\partial M]_2$, which generates $H_{d-1}(\partial M, \mathbb{F}_2)$. □

Prop. (4.14.4.2) [Brouwer Fixed Point Theorem]. For any $f : \mathbb{D}^n \to \mathbb{D}^n \in \mathcal{T}\mathrm{op}$, $\mathrm{Fix}(f) \neq \varnothing$. ⌟

Proof: If $\mathrm{Fix}(f) = \varnothing$, consider the intersection of the ray $f(x)x$ with S^{n-1}, then it depends continuously on x, and this defines a function from D^n to S_n that is identity on S^n, but then this is a retraction from $\mathbb{D}^n \to \mathbb{S}^n$, which is impossible by(4.14.4.1). □

Prop. (4.14.4.3). If $M \in \mathcal{M}\mathrm{ani}^d_{\mathrm{cntd},\partial}$, then if M is contractible and $\partial M \neq \varnothing$, ∂M is a homotopy sphere. ⌟

Proof: As $M^o \sim M$ is contractible, it is orientable by(4.14.3.9). Then by relative Poincaré duality(4.14.3.13) and the long exact sequence,

$$H_p(\partial M) \cong H_{p+1}(M, \partial M) \cong H^{d-p-1}(M) = 0.$$

□

Lemma (4.14.4.4). If $m > n \in \mathbb{Z}_+$, any map $f : \mathbb{RP}^m \to \mathbb{RP}^n$ induces $f_* = 0 : \pi_1(\mathbb{RP}^m) \to \pi_1(\mathbb{RP}^n)$. ⌟

Proof: As $\pi_1(\mathbb{RP}^m) = \begin{cases} \mathbb{Z}/(2) & , m > 1 \\ \mathbb{Z} & , m = 1 \end{cases}$. The assertion is clearly true for $n = 1$. And if $n \in \mathbb{Z}_+, f_* \neq 0$, then by the naturality of Hurewicz homomorphism(4.14.1.17), $f_* \neq 0 : H_1(\mathbb{RP}^m) \to H_1(\mathbb{RP}^n)$. Then by universal coefficient theorem, so is $f^* \neq 0 : H^1(\mathbb{RP}^n, \mathbb{F}_2) \to H^1(\mathbb{RP}^m, \mathbb{F}_2)$. But f^* is a ring homomorphism and $H^*(\mathbb{RP}^m)$ is generated by $a = f^*(a') \in H^1(\mathbb{RP}^m)$(4.14.2.33), so $a^{n+1} = f^*((a')^{n+1}) = 0$, contradiction. □

Lemma (4.14.4.5). If $m > n \geq 1$, there are no antipodal maps: $f : \mathbb{S}^m \to \mathbb{S}^n$, i.e. $f(x) = -f(-x)$. ⌟

Proof: Any such map induces a map $\mathbb{RP}^m \to \mathbb{RP}^n$, which induces 0 on π_1, so by covering space theory, there exists a lifting $\mathbb{RP}^m \to \mathbb{S}^n$. The composition $\mathbb{S}^m \to \mathbb{RP}^m \to \mathbb{S}^n$ is the original map, by the theory of covering spaces, as $\mathbb{S}^n$ is connected and they agree at least on one point. But then f takes antipodal maps to the same point, contradiction. □

Thm. (4.14.4.6) [Borsuk-Ulam]. For ant map $f : \mathbb{S}^n \to \mathbb{R}^n$, there exists $x \in \mathbb{S}^n$ s.t. $f(x) = f(-x)$. ⌟

Proof: If $f(x) \neq f(-x)$ for any $x \in \mathbb{S}^n$, then we can define a map $\mathbb{S}^n \to \mathbb{S}^{n-1}$ that maps x to the intersection of the ray $0, f(x) - f(-x)$ with $\mathbb{S}^n$. Then this map is antipodal, which contradicts(4.14.4.5). □

5 Obstruction Theory & General Cohomology Theory

Towers

Prop. (4.14.5.1) [Towers]. There are Whitehead Towers and Postnikov Towers for a CW complex X.

$$\cdots \to Z_2 \to Z_1 \to Z_0 \to X \to \cdots \to X_2 \to X_1 \to X_0$$

Z_n annihilate $\pi_{\leq n}(X)$, X_n remains only $\pi_{\leq n}(X)$. The towers can be chosen to be fibrations, with fibers $K(\pi_n X, n)$ by(4.13.6.30). ⌟

Prop. (4.14.5.2). There is a Postnikov towers of :

$$B\mathrm{String}(n) \to B\mathrm{Spin}(n) \to BSO(n) \to BO(n)$$

with corresponding obstructions $w_1(X), w_2(X)$ and $p_1(X)/2$. ⌟

Prop. (4.14.5.3) [Obstructions]. If a connected abelian CW complex X ($\pi_1(X)$ abelian and action on higher homotopy trivial) and (W, A) satisfies $H^{n+1}(W, A; \pi_n X) =$ for all n, then $A \to X$ can extend to a map $M \to X$. ⌟

Proof: Cf.[Hatcher P417]. □

Cor. (4.14.5.4). A map between Abelian CW complexes that induce isomorphisms on homology is a homotopy equivalence. ⌟

Proof: Notice that $\pi_1(X)$ acts trivially on $\pi_1(Y, X)$ and use Hurewicz. □

6 Brown Representability

Prop. (4.14.6.1). For any $Z \in \mathcal{T}\text{op}^{\text{pt}}$, the functor

$$\langle -, Z\rangle : \mathcal{CW}^{\text{pt}} \to \mathcal{S}\text{et}^{\text{pt}}$$

satisfies:
Exactness: If $A \subset X$ is a subcomplex, then there is an exact sequence

$$\langle X/A, Z\rangle \to \langle X, Z\rangle \to \langle A, Z\rangle.$$

Additivity: If $X = \bigvee_i X_i \in \mathcal{CW}^{\text{pt}}$, then

$$\langle X, Z\rangle \cong \prod_i \langle X_i, Z\rangle.$$

⌟

Proof: 1 follows from the fact that $A \to X$ is a cofibration(4.13.6.5). 2 is trivial. □

Spectrum

Def. (4.14.6.2) [Prespectrums]. A **prespectrum** is a sequence of pointed spaces $(T_n)_{n\in\mathbb{Z}}$ together with maps $\sigma_n \in \langle \Sigma T_n \to T_{n+1}\rangle \cong \langle T_n, \Omega T_{n+1}\rangle$.

An **Ω-Spectrum** is an prespectrum $(T_n)_{m\in\mathbb{Z}}$ s.t. σ_n are all weak-homotopy equivalences. ⌟

Def. (4.14.6.3) [Suspension Prespectrums]. For $X \in \mathcal{T}\text{op}^{\text{pt}}$, the sequence of pointed spaces $(\Sigma^n(X))_{n\in\mathbb{Z}}$(where we define $\Sigma^{-1} = \Omega$) is a prespectrum, called the **suspension prespectrum** of X. If $X = S^0$, this is called the **sphere spectrum**. ⌟

Prop. (4.14.6.4) [Prespectrum and Homotopy Theories]. Let $(T_n)_{n\in\mathbb{N}}$ be a prespectrum consisting of pointed CW complexes s.t. T_n is $(n-1)$-connected for any $n \in \mathbb{N}$, then

$$\widetilde{E}_p(X) = \varinjlim_n \pi_{p+n}(X \wedge T_n)$$

is a reduced homology theory on $\mathcal{CW}^{\text{pt}}$. ⌟

Proof: Cf.[May, P176]. □

Prop. (4.14.6.5) [Ω-Prespectrum and ES-Cohomology theories]. If K_n is an Ω-spectrum, i.e. $K_n \cong \Omega K_{n+1}$ weak equivalence, then the functors $X \mapsto \langle X, K_n\rangle$ define a reduces ES-cohomology theory on $\mathcal{CW}^{\text{pt}}$ ⌟

Proof: By(4.14.6.1), these functors satisfy the additivity and exactness. The natural suspension isomorphism is given by

$$\Sigma : \langle X, T_n\rangle \to \langle \Sigma(X), \Sigma T_n\rangle \cong \langle \Sigma(X), \Sigma T_n\rangle,$$

which is an isomorphism by(4.13.5.5). □

Thm. (4.14.6.6) [Brown Representability]. Any reduced ES-cohomology theory on $\mathcal{CW}^{\text{pt}}$ is represented by a Ω-prespectrum. ⌟

Proof: ? □

Eilenberg-Maclane Spaces

Def. (4.14.6.7)[Eilenberg-Maclane Spaces]. For $\Lambda \in \mathcal{A}\text{b}$, an **Eilenberg-Maclane space** is defined to be a pointed CW complex $K(\Lambda, n) \in \mathcal{CW}^{\text{pt}}$ s.t. $\pi_k(K(\Lambda, n)) = \begin{cases} \Lambda & , k = n \\ 0 & , \text{otherwise} \end{cases}$. ⌟

Prop. (4.14.6.8) [Eilenberg-Maclane Spaces and Homologies]. For $X \in \mathcal{CW}^{\text{pt}}, \Lambda \in \mathcal{A}\text{b}$, there are isomorphisms

$$\widetilde{H}_p(X; \Lambda) \cong \varinjlim_{p+n} \pi_{p+n}(X \wedge K(\Lambda, n)).$$

⌟

Proof: Cf.[May, P176]. □

Prop. (4.14.6.9) [Eilernberg-Maclane Spaces and Cohomologies]. For $\Lambda \in \mathcal{A}\text{b}, X \in \mathcal{CW}^{\text{pt}}, n \in \mathbb{N}$, $K(\Lambda, n)$ are unique up to weak homotopy, and there are natural isomorphisms

$$\widetilde{H}^n(X; \Lambda) \cong \langle X, K(\Lambda, n)\rangle.$$

⌟

Proof: Given a $K(\Lambda, n)$, if we define $K(\Lambda, m) = \Sigma^{m-n}(K(\Lambda, n))$, then these are all CW complexes by(4.13.3.13), and it defines an ordinary cohomology theory: The dimension axiom follows from the definition of $K(\Lambda, n)$, and it is a reduced ES-cohomology theory by(4.13.5.5) and(4.14.6.10). Thus the asserted isomorphism follows from(4.14.2.3).

This shows in particular that $K(\Lambda, n)$ are unique up to homotopy by Yoneda lemma. □

Cor. (4.14.6.10) [Uniqueness of Eilenberg-Maclane Spaces]. $K(\Lambda, n)$ is unique up to homotopy, and $\Omega(K(\Lambda, n)) \sim K(\Lambda, n-1) \in \mathcal{CW}^{\text{pt}}$. ⌟

Prop. (4.14.6.11) [Eilenberg-Maclane Spaces Exist]. Take $K(\Lambda, n) = \Gamma(B(\Lambda, n))$(4.15.3.7), where Λ is regarded as a discrete subgroup.

Note $K(G, 1)$ is constructed the same as by(4.6.8.1). ⌟

Proof: □

Prop. (4.14.6.12) [Cohomology Operators]. Cohomological operators $\widetilde{H}^p(-; \Lambda) \to \widetilde{H}^{p+n}(-; \Lambda')$ are in bijection with elements in $\widetilde{H}^{p+n}(K(\Lambda, p); \Lambda')$, by(4.14.6.9) and Yoneda lemma. ⌟

Prop. (4.14.6.13) [Examples].

- $K(\mathbb{Z}, 1) = S^1 = U(1)$.
- $K(\mathbb{Z}, 2) = \mathbb{CP}^\infty$.
- $K(\mathbb{Z}/(2), 1) = \mathbb{RP}^\infty$.

⌟

Proof: 1 is clear.

2: This is because by(4.15.1.17), $\mathbb{S}^\infty \to \mathbb{CP}^\infty$ is a locally trivial bundle with fiber S^1, and $\mathbb{S}^\infty$ is contractible by(4.13.3.18) thus by(4.13.6.14), $\pi_2(\mathbb{CP}^\infty) = \mathbb{Z}$ and $\pi_n(\mathbb{CP}^\infty) = 0$ for $n \neq 2$.

3: This is because by(4.15.1.17), $\mathbb{S}^\infty \to \mathbb{CP}^\infty$ is a locally trivial bundle with fiber $\{\pm 1\}$, and $\mathbb{S}^\infty$ is contractible by(4.13.3.18) thus by(4.13.6.14), $\pi_2(\mathbb{CP}^\infty) = \mathbb{Z}/2\mathbb{Z}$ and $\pi_n(\mathbb{CP}^\infty) = 0$ for $n \neq 2$. □

Steenrod Powers

Prop. (4.14.6.14) [Steenrod Powers]. There are stable cohomology operators

$$\mathrm{Sq} : H^*(X, \mathbb{F}_2) \to H^*(X, \mathbb{F}_2) : x \in H^k(X, \mathbb{F}_2) \mapsto \sum_{i \in \mathbb{N}} \mathrm{Sq}^i(x), \quad \mathrm{Sq}^i(x) \in H^{k+i}(X, \mathbb{F}_2)$$

called **Steenrod Powers** that satisfies

- $\mathrm{Sq}(\alpha \cup \beta) = \mathrm{Sq}(\alpha) \cup \mathrm{Sq}(\beta)$.
- $\mathrm{Sq}^i(\alpha) = \alpha^2$ if $i = |\alpha|$, and 0 if $i > |\alpha|$.

For $p \in \mathbf{P}$, the total Steenrod powers P is a similar map from $H^n(X, \mathbb{F}_p) \to H^{n+*}(X, \mathbb{F}_p)$ that $\mathrm{P}^i(\alpha) = \alpha^p$ if $2i = |\alpha|$ and 0 if $2i > \alpha$. ⌟

Proof: Cf.[Hatcher P497].? □

Prop. (4.14.6.15) [Adam Relations]. For $0 < i < 2j \in \mathbb{Z}$,

$$\mathrm{Sq}^i \mathrm{Sq}^j = \sum_{0 \leq k \leq \lfloor \frac{i}{2} \rfloor} \binom{j-k-1}{i-2k} \mathrm{Sq}^{i+j-k} \mathrm{Sq}^k \in \mathrm{End}(H^*(-, \mathbb{F}_2))$$

There are Adam relation calculators in terms of Serre-Cartan basis at`https://math.berkeley.edu/~kruckman/adem/`. ⌟

Proof: □

Cor. (4.14.6.16). The subalgebra of $\mathrm{End}(H^*(-, \mathbb{F}_2)$ generated by $\{\mathrm{Sq}^{\mathbb{Z}}\}$ is generated respectively by elements Sq^{2^k}.

and for $p \in \mathbf{P}$ The subalgebra of $\mathrm{End}(H^*(-, \mathbb{F}_p))$ generated by $\{\mathrm{P}^{\mathbb{Z}}\}$ is generated by elements P^{p^k} and β. ⌟

Proof: ? □

Prop. (4.14.6.17) [$H^*(K(\mathbb{F}_2, p), \mathbb{F}_2)$]. $H^*(K(\mathbb{F}_2, p), \mathbb{F}_2))$ can be calculated, Cf,[May, P185]. ⌟

Proof:

□

7 Stable Homotopy Theory

4.15 Fiber Bundles & K-Theory

Main references are [Ati64], [AGP02] and [M-S74].

Remark (4.15.0.1). Any base space B in this section is assumed to be paracompact. Instead, we may require in the definition of locally trivial bundles s.t. there exists a trivialization that is dominated by a partition of unity on B. ⌟

1 Fiber Bundles

Def. (4.15.1.1) [Fiber Bundles]. $\pi : E \to X \in \mathcal{CG}$ is called a **fiber bundle** with fiber F if every fiber $\pi^{-1}(x)$ is homeomorphic to F. If any $x \in X$ has a nbhd U together with a homeomorphism $\pi^{-1}(U) \cong U \times F$ over U, then it is called a **locally trivial bundle**. And a **numerical locally trivial bundle** is a locally trivial bundle $\pi : E \to X$ s.t. their there is a numerical covering $\{U_i \to X\}$ s.t. there are homeomorphisms $\pi^{-1}(U_i) \cong U_i \times F$ over U_i for each i. ⌟

Prop. (4.15.1.2) [Dold]. If $\pi : E \to X \in \mathcal{CG}$ and there is a numerical covering $\{U_i \to X\}$ s.t. $\pi^{-1}(U_i) \to U_i$ are Hurewicz fibrations, then π is a Hurewicz fibration. ⌟

Proof: Cf.[Tammo tom Dieck, Algebraic Topology]Chap13**?** □

Cor. (4.15.1.3) [Fiber Bundles are Hurewicz Fibrations]. Every numerical locally trivial bundle is a Hurewicz fibration. ⌟

Prop. (4.15.1.4) [Pullback Bundle]. Let $\pi : E \to X$ be a fiber bundle with fiber F and $f : Y \to X$ a map, then the pullback space $f^*E \to Y$ (4.4.1.8) is also a fiber bundle over Y with fiber F, called the **pullback bundle**. ⌟

Prop. (4.15.1.5). If $E \to B, E' \to B'$ are fiber bundles both with compact Hausdorff fibers/or both with discrete fibers/, and $f : E/B \to E'/B'$ is a bundle map that induces isomorphisms on the fibers, then $E \cong f^*E'$ over B. ⌟

Proof: □

Lemma (4.15.1.6). Suppose $\pi : E \to B \times I$ is a fiber bundle whose restriction to $B \times [0, a]$ and $B \times [a, 1]$ are all trivial for some $a \in I$, then $E \to B \times I$ is a trivial bundle. ⌟

Proof: Choose trivializations $\varphi_1 : B \times [0, a] \times B \times F \to \pi^{-1}(B \times [0, a])$, and $\varphi_2 : B \times [a, 1] \times B \times F \to \pi^{-1}(B \times [a, 1])$, then these induces a map

$$B \times \{a\} \times F \xrightarrow{\varphi_1|} \pi^{-1}(B \times \{a\}) \xrightarrow{\varphi_2^{-1}|} B \times \{a\} \times F,$$

of the form $(b, a, v) \mapsto (b, a, g(b)v)$, where $g : B \to \mathrm{Homeo}(F)$ is continuous. Then we get a trivialization

$$B \times I \times F \to E : \varphi(b, t, v) = \begin{cases} \varphi_1(b, t, v) & t \le a \\ \varphi_2(b, t, g(b)v) & t \ge a \end{cases}.$$

□

Lemma (4.15.1.7). Let $E \to B \times I$ be a fiber bundle, then there exists a covering $\{U_i\}$ of B that E is trivial on each $U_i \times I$. ⌟

Proof: For each $b \in B$, we can find a nbhd U_b and a division $0 = s_0 < s_1 < \ldots < s_n = 1$ that E is trivial on each of $U_b \times [s_i, s_{i+1}]$. Then by(4.15.1.6), E is trivial on $U_b \times I$. Then these $\{U_b\}$ is a covering of X that E is trivial on each $U_b \times I$. □

Lemma (4.15.1.8). Let $\pi : E \to B \times I$ be a fiber bundle, where B is a paracompact space, and $r : B \times I \to B \times I$ defined by $r(b, x) = (b, 1)$, then there exists a bundle morphism f over r that induces an isomorphism $r^*E \cong E$ over $B \times I$. ⌟

Proof: By(4.15.1.7), we can choose a covering $\{U_\alpha\}$ of B that is E is trivial over each $U_\alpha \times I$, and let ψ_α be a partition of unity $1 = \sum \psi_i$ that $\mathrm{Supp}(\psi_i) \subset U_i$ and $\{\mathrm{Supp}(\psi_i)\}$ is locally finite. We also define $\mu_\alpha(x) = \frac{\psi_\alpha(x)}{\max\{\psi_\beta(x)\}}$, then μ_α are all continuous and subordinate to $\{U_\alpha\}$, and for each $x \in B, \max\{\mu_\alpha(x)\} = 1$.

Let $\varphi_\alpha : U_i \times I \times F \to \pi^{-1}(U_i \times I)$ be the local trivializations. We define a bundle map $f_\alpha : E/B \times I \to E/B \times I$ by identity outside $\pi^{-1}(U_i \times I)$ and $f_\alpha(\varphi_\alpha(b, t, v)) = \varphi_\alpha(b, \max(\mu_\alpha(x), t), v)$, then f_α is continuous and induces an isomorphism $f_\alpha^* E \cong E$ over $B \times I$. Now choose a well-ordering on α, by local finiteness, for each $v \in E$, there is a nhhd $W_v \times I$ of $\pi(v) \in B \times I$ that $W_v \cap U_\alpha \neq \varnothing$ for only α in a finite set $\{\alpha_1, \ldots, \alpha_m\}$ with $\alpha_1 < \alpha_2 \ldots < \alpha_m$. Then we define a bundle map $f : E \to E$ that $f|_{\pi^{-1}(W_v \times I)} = f_{\alpha_m} \circ \ldots \circ f_{\alpha_1}$. Then this is well-defined, and it is a bundle map over r that induces an isomorphism $f^*E \cong E$. □

Prop. (4.15.1.9) [Homotopy Invariance of Fiber Bundles]. Let $E' \to B'$ be fiber bundles. If $f, g : B \to B'$ are two homotopic maps with B paracompact, then there is a bundle isomorphism $f^*E' \cong g^*E'$. ⌟

Proof: Let $F : B \times I \to B'$ be a homotopy from f to g, and let $i_v : B \to B \times I : i_v(b, x) = (b, v)$ for $v = 0, 1$. Let $r : B \times I \to B \times I$ be the retraction defined by $r(b, x) = (b, 1)$, then by(4.15.1.8), there is an isomorphism of fiber bundles

$$f^*E' \cong (F \circ i_0)^*E' \cong i_0^* F^* E' \cong i_0^* r^* F^* E' \cong i_1^* F^* E' \cong g^* E'.$$

□

Prop. (4.15.1.10) [Cone Bundles]. Let E/X be a fiber bundle with fiber F, then we can construct a new fiber bundle $Cone(E)/X$ with bundle $C(F)$. ⌟

Cor. (4.15.1.11). This is because we can use the transformation characterization to extend maps $U_i \cap U_j \to \mathrm{Aut}(F)$ to maps $U_i \cap U_j \to \mathrm{Aut}(C(F))$. ⌟

Prop. (4.15.1.12) [Hopf Fibration]. There is a locally trivial fiber bundle $S^3 \to S^2$ with fiber S^1, called the **Hopf fibration**. ⌟

Proof: Cf.[AGP02]P129. □

Prop. (4.15.1.13) [Ehresmann]. Let $f : E \to B \in \mathcal{M}\mathrm{ani}_{\mathrm{sm}}$ be a proper submersion, then it is a locally trivial bundle. ⌟

Proof: Cf.[Björn Dundas, A Short Course in Differential Topology].**?** □

Cor. (4.15.1.14). There is a locally trivial bundle $S^{2n-1} \to \mathbb{CP}^n$ with fiber S^1. ⌟

Proof:

□

Cor. (4.15.1.15). There is a locally trivial bundle $\mathbb{RP}^{2n-1} \to \mathbb{CP}^n$ with fiber S^1. ⌟

Proof: □

Prop. (4.15.1.16) [Classifying Space Bundles]. There is a locally trivial bundle $U(n,\mathbb{K}) \to V_n(\mathbb{K}^\infty) \to \mathrm{Gra}(n,\mathbb{K}^\infty)$. for $\mathbb{K} = \mathbb{R}, \mathbb{C}$ or $\mathbb{H}$. ⌟

Proof: □

Cor. (4.15.1.17). There is a locally trivial bundle $\mathbb{S}^\infty \to \mathbb{CP}^\infty$ with fiber S^1. ⌟

Prop. (4.15.1.18). There is a locally trivial bundle $S^n \to \mathbb{RP}^n$ with fiber $\{\pm 1\}$. ⌟

Proof: □

Prop. (4.15.1.19). There is a locally trivial fiber bundle $\mathbb{S}^\infty \to \mathbb{RP}^\infty$ with fiber $\{\pm 1\}$. ⌟

Proof: Cf.[AGP02]P335. □

Covering Space

Def. (4.15.1.20) [Covering Space]. A **covering space** is a fiber bundle $E \to X$ with discrete fibers. ⌟

Prop. (4.15.1.21). if X and Y are Hausdorff spaces, $f : X \to Y$ is a local homeomorphism, X is compact, and Y is connected, then f a covering map. ⌟

Proof: First, f is surjective (using the connectedness), and that for each $y \in Y$, $f^{-1}(y)$ is finite. Because X is compact, there exists a finite open cover of X by $\{U_i\}$ such that $f(U_i)$ is open and $f|_{U_i} : U_i \to f(U_i)$ is a homeomorphism. For $y \in Y$, let $\{x_1, \ldots, x_n\} = f^{-1}(y)$ (the x_i all being different points). Choose pairwise disjoint neighborhoods $U_1, \ldots, U_n$ of $x_1, \ldots, x_n$, respectively (using the Hausdorff property).

By shrinking the U_i further, we may assume that each one is mapped homeomorphically onto some neighborhood V_i of y.

Now let $C = X \setminus (U_1 \cup \cdots \cup U_n)$ and set

$$V = (V_1 \cap \cdots \cap V_n) \setminus f(C)$$

V should be an evenly covered nbhd of y. □

Prop. (4.15.1.22). If $\pi : \tilde{B} \to B$ is a local onto homeomorphism with the property of lifting arcs. Let $\tilde{B}$ be arcwise connected and B simply connected, then π is a homomorphism. ⌟

Proof: only need to prove injective. If p_1 and p_2 map to the same point, then they can be connected, and the image is a loop thus contractable, contradiction. □

Cor. (4.15.1.23). If $\tilde{B}$ is locally arcwise connected and B is locally simply connected, then π is a covering map. ⌟

Proof: Choose the connected components of a simply connected nbhd of a point p and use(4.15.1.22). □

Prop. (4.15.1.24) [Homotopy Lifting Property]. Given a covering space $\pi : \widetilde{X} \to X$, and a homotopy $f_t : Y \to X$, and a map $\widetilde{f_0} : Y \to \widetilde{X}$ lifting X, then there is a unique homotopy $\widetilde{f_t} : Y \to \widetilde{X}$ of $\widetilde{f_0}$ lifting f_t. ⌟

Proof: Let U_α be a covering of X that the We first construct a lift $\widetilde{F} : N \times I \to \widetilde{X}$ for N a nbhd near some point $y_0 \in Y$. Because f is continuous, there is a nbhd N of y_0 and a partition $0 = t_0 < t_1 < \ldots < t_m = 1$ of I that each $N \times [t_i, t_{i+1}]$ is mapped into some U_α. Then we can construct a lifting $\widetilde{F} : N \times I \to \widetilde{X}$ by induction using the local homeomorphism property of covering space.

Next we show the uniqueness in the special case that Y is a point. This can also be done using a partition of I and induction.

Finally we can construct lifting near every point $y \in Y$, and also they coincide on the overlap because of the uniqueness we just proved. So these liftings glue together to give a lifting $\widetilde{f_t} : Y \to \widetilde{X}$. □

Cor. (4.15.1.25). The map $\pi_* : \pi_1(\widetilde{X}, \widetilde{x}_0) \to \pi_1(X, x_0)$ induced by the covering map is injective. And the image of this map consists of homotopy types of loops that based at x_0 whose lift starting at $\widetilde{x}_0$ are also loops. ⌟

Proof: This is because a homotopy of a the image of a loop to trivial loop in $\widetilde{X}$ can be lifted to a homotopy of the loop itself to trivial loop. And this homotopy also fixes the endpoint, because the lifting of a trivial loop must be a trivial loop.

For the second assertion, one direction is easy, for the other, if a loop is a homotopic to the image of a loop of $\widetilde{X}$, then it is itself the image of a loop of $\widetilde{X}$. □

Prop. (4.15.1.26) [Degree of a Covering]. Let $\pi : \widetilde{X} \to X$ be a covering map, then the cardinality of $\pi^{-1}(x)$ is a a locally constant function of x. Thus if X is constant, this cardinality is fixed for any $x \in X$, and it is called the degree of the covering.

The number of sheets of a covering with $\widetilde{X}$ path-connected equals the index of $\pi_*(\pi_1(\widetilde{X}, \widetilde{x}_0))$ in $\pi_1(X, x_0)$. ⌟

Proof: For a loop g in X based at x_0, let $\widetilde{g}$ be its lift to $\widetilde{X}$ starting at $\widetilde{x}_0$. Now if $h \in \pi_*(\pi_1(\widetilde{X}, \widetilde{x}_0))$, then the loop $h \cdot g$ has lift that has the same ending as $\widetilde{g}$. So we get a map from the quotient set $\pi_1(X, x_0)/\pi_*(\pi_1(\widetilde{X}, \widetilde{x}_0))$ to $p^{-1}(x_0)$ mapping $\pi_*(\pi_1(\widetilde{X}, \widetilde{x}_0))[g]$ to $\widetilde{g}(1)$. This map is injective, and it is surjective because $\widetilde{X}$ is path-connected. Then we are done. □

Prop. (4.15.1.27) [Unique Lifting Property]. Let $\pi : (\widetilde{X}, \widetilde{x}_0) \to (X, x_0)$ be a covering space and $f : (Y, y_0) \to (X, x_0)$ be a map with Y path-connected and locally path-connected, then a lift $\widetilde{f} : (Y, y_0) \to (\widetilde{X}, \widetilde{x}_0)$ exists iff $f_*(\pi_1(Y, y_0)) \subset \pi_*(\pi_1(\widetilde{X}, \widetilde{x}))$. And when Y is connected, this lifting is unique.

In particular, a covering space has unique path lifting property. ⌟

Proof: One direction is clear, for the other, to construct a lifting, choose a path γ from y_0 to y, the path $f\gamma$ has a unique lifting $\widetilde{f\gamma}$ starting from $\widetilde{x}_0$. Define $\widetilde{f}(y) = \widetilde{f\gamma}$. This is a well-defined map: if γ' is another path from y_0 to y, then $f\gamma^{-1} f\gamma'$ is a loop that is homotopic to the image of a loop at $\widetilde{x}_0$. Now we can lift this homotopy, and then $f\gamma^{-1} f\gamma'$ is also the image of a loop at $\widetilde{x}_0$, which must be $\widetilde{f\gamma}^{-1}\widetilde{f\gamma'}$ by uniqueness. So $\widetilde{f}$ is well-defined.

It can be verified that $\widetilde{f}$ is continuous.

The uniqueness is clear, because if there are two lifts, the points that they are equal and the points that they are not are both open in Y. □

Prop. (4.15.1.28)[Galois Theory of Covers]. Let X be a path-connected and locally path-connected and semilocally simply-connected space(4.13.4.27), then

- there is a connected and simply-connected covering space $\widetilde{X}$ of X, called a **universal cover** of X.
- Thee fundamental group acts continuously and properly on $\widetilde{X}/X$.
- For any subgroup H of $\pi_1(X, x_0)$, there is a connected covering space $\pi : X_H \to X$ that $\pi_*(\pi_1(X_H, \widetilde{x}_0)) = H$ for a suitably chosen base point $\widetilde{x}_0$. And this covering space is unique up to isomorphism over (X, x_0). Thus by(4.15.1.27), there is an inclusion-preserving bijection between isomorphism classes of covering spaces over X and the the set of conjugacy classes of subgroups of $\pi_1(X, x_0)$.

⌟

Proof: Cf.[Hat02]P64, P67.**?** □

Def. (4.15.1.29) [Normal Covering Spaces]. A **normal covering space** is a covering space $\pi : \widetilde{X} \to X$ that for any $x \in X$ and two elements $\widetilde{x}, \widetilde{x}' \in \pi^{-1}(x)$, there is a covering isomorphism of $\widetilde{X}/X$ taking $\widetilde{x}$ to $\widetilde{x}'$. ⌟

Prop. (4.15.1.30). Let $\pi : (\widetilde{X}, \widetilde{x}_0) \to (X, x_0)$ be a path-connected covering space of a path-connected, locally path-connected space X, and let H be the subgroup $\pi_*(\pi_1(\widetilde{X}, \widetilde{x}_0)) \subset \pi_1(X, x_0)$, then

- The covering space is normal iff H is normal in $\pi_1(X, x_0)$.
- The group $G(\overline{X})$ of covering transformations of $\widetilde{X}$ is isomorphic to $N(H)/H$.

⌟

Proof: 1: Let $\widetilde{x}_1, \widetilde{x}_2 \in \pi^{-1}(x_0)$ and γ a path from $\widetilde{x}_1$ to $\widetilde{x}_2$ corresponding to an element of $\pi_1(X, x_0)$, then H is normal is equivalent to $\pi_*(\pi_1(\widetilde{X}, \widetilde{x}_1)) = \pi_*(\pi_1(\widetilde{X}, \widetilde{x}_2))$. Then the lifting criterion shows there is a covering transformation taking $\widetilde{x}_1$ to $\widetilde{x}_2$. The converse is also true.

2: From the above argument, we can define a map $N(H) \to G(\widetilde{x})$ by mapping a $\gamma \in N(H)$ to a covering transformation mapping $\widetilde{x}_0$ to $\widetilde{x}_1$. And the kernel of this map is exactly those γ lifting to a loop at $\widetilde{x}_0$, which are exactly the elements of H. □

Prop. (4.15.1.31) [Covering Space Action]. If G is a discrete group and $G \times Y \to Y$ is a covering space action(4.12.1.14), then the quotient map $Y \mapsto Y \backslash G$ is a normal covering space. And if Y is path-connected, G is the group of covering transformations. ⌟

Proof: The condition on the action shows it is locally a homeomorphism, thus it is a covering space. And it is a normal covering space because $g_1 g_2^{-1}$ takes any $g_1(x)$ to $g_2(x)$. The group of covering transformations is just G, because the covering transformation on a path-connected space is determined by its action on a single point. □

2 Vector Bundles

Basics

Def. (4.15.2.1) [Vector Bundle]. Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$, a $\mathbb{K}$-**vector bundle** of dimension n over a topological space X is a fiber bundle over X with fiber $\mathbb{K}^n$ that each trivialization φ_α restricts to $\mathbb{K}$-linear isomorphisms on the fibers. The category of vector bundles over X is denoted by $\mathcal{V}\mathrm{ect}_{\mathbb{K}}(X)$.A **vector bundle homomorphism** $E \to F$ is a map of spaces over X that the maps on the fibered are all $\mathbb{K}$-linear.

Then a $\mathbb{K}$-vector bundle of dimension n over X is just an associated $\mathrm{GL}(n,\mathbb{K})$-bundle with fiber $\mathbb{K}^n$ over X. In particular, there is a bijection $\mathcal{V}\mathrm{ect}^n_{\mathbb{K}}(X) \cong \mathscr{P}_{\mathrm{GL}(n,\mathbb{K})}(X)$ by(4.15.3.4). ⌟

Def. (4.15.2.2) [Trivial Vector Bundles]. For any $n \in \mathbb{N}$, the **trivial vector bundle** of rank n is denoted by e^n. ⌟

Prop. (4.15.2.3) [Constructions of Vector Bundles]. Let $T : (\mathcal{V}\mathrm{ect}^f/\mathbb{K})^{\otimes n} \to \mathcal{V}\mathrm{ect}^f/\mathbb{K}$ be a functor that is either covariant or contravariant for each of its factor that $T : \prod_i \mathrm{Hom}(V_i, W_i) \to \mathrm{Hom}(T(V_i), T(W_i))$ is continuous, then we have a functor $T : Vect(X)^n \to Vect(X)$ that is either covariant or contravariant for each of its factor. ⌟

Proof: Cf.[Ati64]P6. □

Cor. (4.15.2.4). In this way, given a vector bundles E, F on X, we can construct

$$E \oplus F, \quad E \otimes F, \quad \mathrm{Hom}(E,F) \cong E^* \otimes F, \quad E^*, \quad T^n E, \quad \wedge^i E.$$

⌟

Prop. (4.15.2.5) [Existence of Hermitian Metric]. There exists a Hermitian(Riemannian) metric on any bundle E over a paracompact space X. In this way, $E^* \cong E(\overline{E})$. ⌟

Proof: Choose a metric on each trivialization open subset and use partition of unity to glue. □

Cor. (4.15.2.6). A vector bundle over a paracompact space can have its transform maps $\in O(n)$ (or $U(n)$). ⌟

Proof: We can choose the metric on it compatible with the given metric. In this way, the transform map is $\in O(n)$ (or $U(n)$). □

Cor. (4.15.2.7) [Semisimplicity of $\mathcal{V}\mathrm{ect}(B)$]. Any exact sequence of vector bundles over a paracompact space B splits. ⌟

Proof: Because we can take the orthogonal complement. □

Cor. (4.15.2.8). If $f : X \to Y$ is a homotopy equivalence, then $f^* : \mathcal{V}\mathrm{ect}(Y) \to \mathcal{V}\mathrm{ect}(X)$ is an isomorphism.

In particular, if X is contractible, then every bundle over X is trivial. ⌟

Def. (4.15.2.9) [Orientations of Vector Bundles]. Let $\pi : E \to X$ be a vector bundle of rank n over a space X and $\mathbb{R} \cong \mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}$, then a **orientation of** E with coefficient R is a functions that assigns a generator u_x of $H^n(E_x, 0, R) \cong R$ for any $x \in X$ s.t. for any $x \in X$, there is a nbhd U of $x \in X$ and an element $u \in H^n(\pi^{-1}N, \pi^{-1}(N)_0, R)$ s.t. u pulls back to u_x via $(E_x, 0) \subset (\pi^{-1}N, \pi^{-1}(N)_0)$ for any $x \in U$. In particular, any vector bundle is $\mathbb{F}_2$-orientable. ⌟

Prop. (4.15.2.10) [Orientation of Complex Vector Bundles]. For $E/X \in \mathcal{V}\mathrm{ect}_{\mathbb{C}}(X)$, the underlying real bundle has a preferred orientation, which is compatible with direct sums.

In particular, the tangent bundle of a complex manifold gives rise to a unique orientation of the underlying real manifold. ⌟

Proof: Let $a_1, \ldots, a_n$ be a complex basis for E, then take the real basis to be $a_1, ia_1, \ldots, a_n, ia_n$. This orientation is stable under $GL(n, \mathbb{C})$ transformation, as $GL(n, \mathbb{C})$ is connected. □

Prop. (4.15.2.11). If E is a complex vector bundle over X, then $E \otimes_{\mathbb{R}} \mathbb{C} \cong E \oplus \overline{E}$ as complex vector bundles. ⌟

Lemma (4.15.2.12). Suppose $\pi : E \to B \times I$ is a fiber bundle whose restriction to $B \times [0, a]$ and $B \times [a, 1]$ are all trivial for some $a \in I$, then $E \to B \times I$ is a trivial bundle. ⌟

Proof: The proof is similar to that of(4.15.1.6) □

Lemma (4.15.2.13). Let $E \to B \times I$ be a fiber bundle, then there exists a covering $\{U_i\}$ of B that E is trivial on each $U_i \times I$. ⌟

Proof: The proof is similar to that of(4.15.1.7) □

Lemma (4.15.2.14). Let $\pi : E \to B \times I$ be a fiber bundle, where B is a paracompact space, and $r : B \times \mathbb{I} \to B \times I$ defined by $r(b, x) = (b, 1)$, then there exists a bundle morphism f over r that induces an isomorphism $r^*E \cong E$ over $B \times \mathbb{I}$. ⌟

Proof: The proof is similar to that of(4.15.1.8) □

Prop. (4.15.2.15) [Homotopy Invariance of Vector Bundles]. Let $E' \to B'$ be a vector bundle. If $f, g : B \to B'$ are two homotopic maps with B paracompact, then there is a bundle isomorphism $f^*E' \cong g^*E'$. ⌟

Proof: The proof is similar to that of(4.15.1.9) □

Bundles of Finite Type

Def. (4.15.2.16) [Bundles of Finite Type]. Let X be a paracompact Hausdorff space, then a **vector bundle of finite type** over X is a vector bundle over X that has a covering by f.m. trivialization maps. The category of k-dimensional vector bundles over X of f.t. is denoted by $\mathcal{V}\mathrm{ect}_k^{\mathrm{ft}}(X)$. Trivially, any vector bundle over a compact space is of f.t.. ⌟

Prop. (4.15.2.17) [Vector Bundles on the Quotient]. Let Y be a closed subspace of X, E a vector bundle over X, then a trivialization $\alpha : E|_Y \cong Y \times V$ defines a bundle E/α over X/Y. The isomorphism class of E/α only depends on the homotopy type of α. ⌟

Proof: To show it is a vector bundle, notice the trivialization α extends to a □

Prop. (4.15.2.18) [Splitting Principle]. For a vector bundle $E \to X$, there is a space $Y \to X$ that p^* is injective on $H^*(-, \mathbb{Z})$ and p^*E splits as a sum of line bundles. This proposition is useful when proving theorems about characteristic classes. ⌟

Proof: It suffice to find a Y that p^*E has a subbundle, then choose its orthogonal part, and use induction. For this, choose $Y = P(E)$, then Y has a tautological bundle, which is a subbundle of p^*E, and Y is fibered over X with fiber $\mathbb{P}^n$, and we want to use Leray-Hirsch, so check the fact $H^*(\mathbb{P}^n)$ is free and generated by the first Chern class, by(4.15.4.16) and(6.7.2.1). And Chern class is functorial, so the powers of Chern class of f^*E will generate the cohomology ring of any stalks. □

Prop. (4.15.2.19). For any bundle E over a compact Hausdorff space X, there is a surjective bundle map $X \otimes \mathbb{R}^n \to E$ for some $m \geq 0$. ⌟

Proof: Choose a finite cover of trivialization of E, then we can glue these maps together via a partition function. □

Cor. (4.15.2.20) [Negation of Bundles]. For any vector bundle E on a compact space X, there is a vector bundle F that $E \oplus F$ is a trivial bundle. ⌟

Proof: Choose a bundle map $\mathbb{R}^n \times X \to E$ that is surjective, then the kernel of this map is a bundle F, such that $E \oplus F \cong \mathbb{R}^n$(By taking a Hermitian metric(4.15.2.5) and taking the orthogonal bundle). □

Cor. (4.15.2.21) [Global Transversal Sections]. For a vector bundle over a compact manifold, there exists a global section transversal to the zero section, in particular, if $\dim E > M$, then it has no zero. ⌟

Proof: Choose a bundle map $\mathbb{R}^n \times X \to E$ that is surjective, and then use parametric transversality theorem(12.1.4.5) to prove there is a section that is transversal. □

Cor. (4.15.2.22) [Vector Fields with Isolated Zeros]. There is a vector field on compact manifold of only isolated zeros. And a vector bundle over a k dimensional curve splits to components of dimension no bigger than k. Determined by its Chern class. ⌟

Prop. (4.15.2.23) [Constructing Vector Bundles]. ⌟

Cor. (4.15.2.24). There is a natural isomorphism $\mathcal{V}\mathrm{ect}_n(S(X)) \cong [X, GL(n, \mathbb{C})]$. ⌟

Proof: Write $\Sigma(X) = C^+(X) \coprod C^-(X)$, and $C^\pm(X)$ are both contractible, thus E are trivial restricted to them(4.15.2.8). Let $\alpha^\pm$ be the trivialization isomorphism, then $\alpha^+ \circ \alpha^-$ is a bundle map of $X \times \mathbb{R}^n$, which is equivalent to a map $\alpha : X \to GL(n, \mathbb{C})$. The homotopy type of α is determined because $C^\pm(X)$ are both contractible, and vise versa. □

Prop. (4.15.2.25) [Vector Bundles as Modules]. Γ induces an equivalence between the category of vector bundles over X and the category of finitely projective modules over $C(X)$. ⌟

Proof: Clearly a bundle induces a module over $C(X)$. And it is a fully faithful functor. Now the image is the subcategory of finite projective modules, because every bundle is a direct summand of a trivial bundle, and a trivial bundle corresponds to a finite free $C(X)$-modules. □

Thom isomorphism

Prop. (4.15.2.26) [Thom Class]. Let $R = \mathbb{Z}$ or $\mathbb{F}_2$ and an R-orientable vector bundle E over base B of rank n.

Then there exists uniquely **Thom class** $u_E \in H^n(E, E \backslash B, R)$ that induce the preferred generator $H^n(E_x, E_x \backslash \{0\}, R)$(4.15.2.9) on every fiber. Then the relative Leray-Hirsch will give an isomorphism

$$\varphi_R : H^i(B, R) \cong H^{i+n}(E, E \backslash B, R) : x \mapsto \pi^*(x) \cup u_E.$$

For $\mathbb{F}_2$ coefficient there exists a Thom class, and for orientable bundle there exists a $\mathbb{Z}$-Thom class. Notice that fiber bundle over a simply connected base is orientable. ⌟

Proof: □

Cor. (4.15.2.27) [Naturality].

- Let $B' \to B$ be a map and E/B be an R-orientable vector bundle, which induces a map $f^* : H^n(E, E_0, R) \to H^n(f^*(E), E_0', R)$. Then $f^* u_E \cong u_{f^*(E)}$.

- The Thom class u_E maps to $u_{E,2}$ under the change of coefficients $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$.

⌟

Prop. (4.15.2.28). Similarly, for a orientable fiber bundle $S^{n-1} \to E \to B$, make it a $D^n \to E' \to B$ bundle, then E' is homotopy equivalent to B so there is a Gysin sequence

$$\to H^{i-n}(B) \xrightarrow{\smile e} H^i(B) \to H^i(E) \to H^{i-n+1}(B) \to$$

Where the Euler class e is chosen to commute with the Thom isomorphism. ⌟

Examples of Vector Bundles

Def. (4.15.2.29) [n-Universal k-Vector Bundle]. Let $K = \mathbb{R}$ or $\mathbb{C}$, endow $\mathbb{K}^n$ with the canonical Hermitian metric, define $E_k(\mathbb{K}^n)$ be the subspace of $\mathrm{Gra}(k, \mathbb{K}^n) \times \mathbb{K}^n$ consisting of pairs (W, v) that $v \in W$. Then this is a vector bundle over the Grassmannian $\mathrm{Gra}(k, \mathbb{K}^n)$(12.11.2.12), called the **n-universal k-vector bundles**, or the **tautological bundles**. ⌟

Proof: We construct localization maps: endow $\mathbb{K}^n$ with the natural metric. For $W_0 \in G_k(\mathbb{K}^n)$, then the subspace U of $G_k(\mathbb{K}^n)$ consisting of W that $W \cap W_0^\perp = \varnothing$ is a nbhd of W_0, and it is naturally homeomorphic to $\mathrm{Hom}(W_0, W_0^\perp)$. There is an isomorphism

$$\pi^{-1}(U) \cong U \times W_0 : (f, (f + \mathrm{id})w_0) \mapsto (f, w_0).$$

□

Prop. (4.15.2.30) [Universal Vector Bundle]. Because by(4.15.3.20) $E_k(\mathbb{K}^\infty)/\,\mathrm{Gra}(k, \mathbb{K}^\infty)$ is the universal bundle, there is a map $i_k : \mathrm{Gra}(k, \mathbb{K}^n) \to \mathrm{Gra}(k+1, \mathbb{K}^n)$ s.t. $i_k^*(E_{k+1}(\mathbb{K}^\infty))$ is the bundle $E_k(\mathbb{K}^\infty) \oplus \mathbb{K}$. Then it can be shown

$$BU(\mathbb{K}) = \mathrm{colim}_k(\mathrm{Gra}(k, \mathbb{K}^\infty) \xrightarrow{i_k} \mathrm{Gra}(k+1, \mathbb{K}^\infty))$$

is a CW complex.

Moreover, there are maps $w_{k,l} : \mathrm{Gra}(k, \mathbb{K}^\infty) \times \mathrm{Gra}(l, \mathbb{K}^\infty) \to \mathrm{Gra}(k+l, \mathbb{K}^\infty)$ that corresponds to the bundle $E_k(\mathbb{K}^\infty) \times E_l(\mathbb{K}^\infty)$, and these maps induces an H-space structure on BU. ⌟

Proof: □

Prop. (4.15.2.31)[Tautological Line Bundles]. For $\mathrm{Gra}(1, \mathbb{R}^{n+1}) \cong \mathbb{RP}^n$, the line bundle $E_1(\mathbb{R}^{n+1})$ is denoted by γ_n^1.

Then the tangent bundle τ_n of $\mathbb{RP}^n$ is isomorphic to $\mathrm{Hom}(\gamma_n^1, \gamma_n^\perp)$, where $\gamma_n^\perp$ is the orthogonal complement of γ_n^1 in $e^{n+1}_{\mathbb{RP}^n}$(with the canonical norm). ⌟

Proof: This is because a tangent vector at $x \in \mathbb{RP}^n$ is equivalent to a homomorphism $[x]$ to $[x]^\perp$.
? How to prove this rigorously. □

Cor. (4.15.2.32). $\tau_n \oplus e^1 \cong (\gamma_n^1)^{n+1}$. ⌟

Proof: By(4.15.2.31), $\tau_n \oplus e^1 \cong \mathrm{Hom}(\gamma_n^1, \gamma_n^1) \oplus \mathrm{Hom}(\gamma_n^1, \gamma_n^\perp) = \mathrm{Hom}(\gamma_n^1, \mathbb{R}^n) = (\gamma_n^1)^{*n}$. Then we are done because γ_n^1 is self-dual because it has a Euclidean metric(4.15.2.5). □

Prop. (4.15.2.33) [Pullback the Universal Bundle]. For $V \in \mathcal{V}\mathrm{ect}/\mathbb{K}$, for any continuous map $\varphi : X \to \mathrm{Gra}(k, V)$, we get a subspace $E_\varphi = \{(x, v) \in X \times V | v \in \varphi(x)\} \subset X \times V$. This is a vector bundle over X, and it is a subbundle of the trivial bundle $X \times V \to X$. In fact, $E_\varphi \cong f^* E_k(V)$(4.15.2.29). ⌟

Cor. (4.15.2.34). Let $f : X' \to X$ and $\varphi : X \to Pr(V)$, then $f^*(E_\varphi) = E_{\varphi \circ f}$. ⌟

Prop. (4.15.2.35) [Infinite Universal k-Vector Bundle]. The n-universal k-vector bundles $E_k(\mathbb{K}^n)$(4.15.2.29) for various n gets together to a bundle $E_k(\mathbb{K}^\infty)$ on $\mathrm{Gra}(k, \mathbb{K}^\infty)$ that the pullback of $E_k(\mathbb{K}^\infty)$ via $i : \mathrm{Gra}(k, \mathbb{K}^n) \to \mathrm{Gra}(k, \mathbb{K}^\infty)$ is $E_k(\mathbb{K}^n)$. ⌟

Def. (4.15.2.36) [Hopf Bundle]. Define a map $\varphi : \mathbb{C}P^n \to G_1(\mathbb{C}^{n+1})$ that $\varphi([z]) = [z]$, then this defines a vector bundle on $\mathbb{C}P^n$ by(4.15.2.33), called the **dual of Hopf bundle**. The **Hopf bundle** is defined to be the dual of the dual of Hopf bundle. ⌟

3 Principal Bundles

Main reference is [Principal Bundles and Classifying Space].

Def. (4.15.3.1) [Principal Bundles]. For $G \in \mathcal{T}\mathrm{op}\,\mathcal{G}\mathrm{rp}$, a **principal G-bundle** is a bundle P with G-fibers that the transition function is right G-map, i.e. left multiplication by some $g_{\alpha\beta}$. a associated bundle of a representation $G \to \mathrm{End}(V)$ is the total space of $P \times V$ module the equivalence $[gg_0, v] = [g, g_0 v]$. The corresponding transition function is just the left action by $g_{\alpha\beta}$.

For $B \in \mathcal{T}\mathrm{op}$, denote $\mathcal{P}_G(B)$ the isomorphism classes of vector bundles on B. ⌟

Prop. (4.15.3.2) [Homogenous Space]. For $G \in \mathcal{L}\mathrm{ie}\mathcal{G}\mathrm{rp}$ and $H \leq G$ is a closed subgroup, then the quotient $H \backslash G$ can be given a structure of a G-homogenous space and $G \to H \backslash G$ is a principal H-bundle. ⌟

Proof: □

Prop. (4.15.3.3). The projection $\mathbb{S}^{2n+1} \to \mathbb{CP}^n$ is a principal $\mathbb{S}^1$-bundle. ⌟

Proof: □

Prop. (4.15.3.4) [Associated Bundles]. If $G \in \mathcal{T}\mathrm{op}\,\mathcal{G}\mathrm{rp}$ and G acts freely on $F \in \mathcal{T}\mathrm{op}$, then an **associated G-bundle with fiber F** is a locally trivial F-bundles with a G-action**?**.

Then the isomorphism classes of associated G-bundles with fiber F over B is in bijection with $\mathcal{P}_G(B)$. ⌟

Proof: **?** □

Classifying Space

Def. (4.15.3.5) [Classifying Spaces]. For $G \in \mathcal{T}\mathrm{op}\,\mathcal{G}\mathrm{rp}$, a **classifying space** of G is a space $B(G) \in \mathcal{T}\mathrm{op}$ together with a principal G-bundle $E(G) \to B(G)$ s.t. $E(G)$ is contractible.

Notice $\pi_{n+1}(BG) = \pi_n(G)$ by(4.13.6.14). ⌟

Thm. (4.15.3.6) [Classifying Spaces and Principal Bundles]. If $G \in \mathcal{T}\mathrm{op}\,\mathcal{G}\mathrm{rp}$ and $E(G) \to B(G)$ is a classifying space for G, then for any $B \in \mathcal{T}\mathrm{op}$ that is paracompact, the pullback induces a bijection

$$[B, B(G)] \cong \mathcal{P}_G(B).$$

In particular, the classifying spaces is uniquely defined up to homotopy, if it exists. ⌟

Proof: ?? □

Prop. (4.15.3.7) [Classifying Spaces Exist]. For $G \in \mathcal{T}\mathrm{op}\,\mathcal{G}\mathrm{rp}$, define

$$E_*(G) \in s\,\mathcal{T}\mathrm{op} : E_n(G) = G^{n+1}$$

$$d_i((g_1,\ldots,g_{n+1})) = \begin{cases} (g_2,\ldots,g_{n+1}) & ,i=0 \\ (g_1,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_{n+1}) & ,1\le i\le n \end{cases}$$

$$s_i((g_1,\ldots,g_n)) = (g_1,\ldots,g_i,e,g_{i+1},\ldots,g_n), \quad 0\le i\le n$$

And

$$B_*(G) \in s\,\mathcal{T}\mathrm{op} : B_n(G) = G^n$$

$$d_i((g_1,\ldots,g_n)) = \begin{cases} (g_2,\ldots,g_n) & ,i=0 \\ (g_1,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_n) & ,1\le i\le n-1 \\ (g_1,\ldots,g_n) & i=n \end{cases}$$

$$s_i((g_1,\ldots,g_{n-1})) = (g_1,\ldots,g_i,e,g_{i+1},\ldots,g_{n-1}), \quad 0\le i\le n.$$

Then there is a map

$$\mathrm{pr} : E_*(G) \to B_*(G) \in s\,\mathcal{T}\mathrm{op} : (g_1,\ldots,g_{n+1}) \in E_n(G) \mapsto (g_1,\ldots,g_n) \in B_n(G).$$

Denote $E(G) = |E_*(G)|, B(G) = |B_*(G)|$, then pr induces a map $\mathrm{pr} : E(G) \to B(G)$. $B(G)$ is called the **classifying space** of G. ⌟

Cor. (4.15.3.8). Any group G is a fundamental group of a topological space. ⌟

Prop. (4.15.3.9). Situation as in(4.15.3.7), there is a right action of G on $E_*(G)$ on the last coordinates, which induces an action of G on $E(G)$, and $B(G) \cong E(G)/G$. Then if (G,e) is well-pointed, $E(G) \to B(G)$ is a locally trivial bundle with fiber G, and $E(G)$ is contractible. In particular, $G \cong \Omega(BG)$, by(4.13.6.20). ⌟

Proof: ?. Cf.[Milnor, Construction of Universal Fiber Bundles, I, II]. □

Cor. (4.15.3.10). For $G, G' \in \mathcal{T}\mathrm{op}\,\mathcal{G}\mathrm{rp}$,

$$E(G\times G') \cong E(G)\times E(G'), \quad B(G\times G') \cong B(G)\times B(G').$$

⌟

Cor. (4.15.3.11). If G is commutative, then $G\times G \to G$ is a homomorphism that makes $B(G)$ a commutative topological group. Then we can define for any $n\in\mathbb{N}$,

$$B(G,n) = B^{\circ n}(G).$$

⌟

Prop. (4.15.3.12). $[X, BG] \cong G$-bundles on X. And BG is Abelian if G is Abelian. Thus the classifying space BG is unique up to homotopy equivalence because they all represent the functor from the CW homotopy category to the set of G-bundles on it. ⌟

Proof: Cf.[Principal Bundles and Classifying Space P13]. □

Prop. (4.15.3.13) [Examples of Classifying Spaces].

- $B(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{S}^\infty/(\mathbb{Z}/n) = (\mathbb{C}^\infty\backslash\{0\})/(\mathbb{R}^+ \times \mu_n)$(4.13.3.17). In particular, $B(\mathbb{Z}/2) \cong \mathbb{RP}^\infty$(4.13.3.19).
- $BSU(2,\mathbb{R}) = \mathbb{HP}^\infty$.
- $B(\mathbb{Z}^g) = \mathbb{T}^g$ because $\mathbb{R} \to \mathbb{T}^1$ is a universal cover, this can be seen observing only has to satisfy the sum of inner angle is π.
- $BO(n), BU(n), BSp(n)$ are respectively the infinite Grassmannians $\mathrm{Gra}(n,\mathbb{R}^\infty), \mathrm{Gra}(n,\mathbb{C}^\infty), \mathrm{Gra}(n,\mathbb{H}^\infty)$, because there is a locally trivial fiber bundle(4.15.1.16) $U(n,\mathbb{K}) \to V_n(\mathbb{K}^\infty) \to \mathrm{Gra}(n,\mathbb{K}^\infty)$, and $V_n(\mathbb{K}^\infty)$ is contractible(4.13.3.18). In particular, $B(\mathbb{Z}/2) = \mathbb{RP}^\infty$ and $BS^1 = \mathbb{CP}^\infty$.

⌟

Proof: □

Def. (4.15.3.14) [Admissible Subgroups]. A subgroup of a topological group G is called **admissible** if $G \to G/H$ is a principal H-bundle. In particular, this is the case for $G \in \mathcal{L}\mathrm{ie}\mathcal{G}\mathrm{rp}$ and $H \leq G$ closed, by(4.15.3.2). ⌟

Prop. (4.15.3.15). If H is an admissible subgroup of G, then there is a homotopy fiber sequence $G/H \to BH \to BG$. ⌟

Proof: Cf.[Principal Bundles and Classifying Space P22]. □

Cor. (4.15.3.16). There are homotopy equivalences $\Omega BK \cong K$ and $B\Omega K \cong K$. ⌟

Prop. (4.15.3.17). If H is an admissible normal subgroup of G, then there is a homotopy fiber sequence $BH \to BG \to B(G/H)$. ⌟

Proof: □

Cor. (4.15.3.18).

- there are fiber bundles $\mathbb{S}^0 \to BSO(n) \to BO(n)$ and similarly for $BSU(n)$ and $BSp(n)$.
- there are fiber bundles $\mathbb{S}^n \to BO(n) \to BO(n+1)$.
- there are fiber bundles $U(n)/T^n \to (\mathbb{CP}^\infty)^n \to BU(n)$, where $U(n)/T^n$ is the variety of complete flags in $\mathbb{C}^n$.
- for a discrete group $H \subset G$, $BH \to BG$ is a covering map.
- there are fiber bundles $BSO(n) \to BO(n) \to \mathbb{RP}^\infty$ and similarly for $\mathbb{C}$ and $\mathbb{H}$.
- there are fiber bundles $\mathbb{RP}^\infty \to B\,\mathrm{Spin}(n) \to BSO(n)$.

⌟

Proof: These are all classifying spaces of Lie groups. □

Prop. (4.15.3.19) [Classifying Line Bundles]. Note that $K(\mathbb{Z},2) = \mathbb{CP}^\infty = B(K(\mathbb{Z},1)) = BU(1)$(4.15.3.13), thus we have a bijection $H^2(X,\mathbb{Z}) \cong [X,K(\mathbb{Z},2)] \cong \mathcal{V}\mathrm{ect}^1_{\mathbb{C}}(X)$. Similarly, we have a bijection $H^1(X,\mathbb{Z}/2\mathbb{Z}) \cong \mathcal{V}\mathrm{ect}^1_{\mathbb{R}}(X)$. ⌟

Classifying Spaces

Prop. (4.15.3.20)[Universal Real Bundle]. Let X be paracompact, then there is a natural bijection

$$[X, \mathrm{Gra}(k, \mathbb{K}^\infty)] \to \mathcal{V}\mathrm{ect}^k_{\mathbb{K}}(X) : f \mapsto f^* E_k(\mathbb{K}^\infty).$$(4.15.3.13)(4.15.2.35)

⌟

Proof: Because E is of f.t., we can find a f.d. vector space W with a metric and a vector bundle epimorphism $\varphi : X \times W \to E$ via partition of unity. Then we can take the map $\varphi : X \to G_k(W) : x \mapsto \ker(\varphi_x)^\perp$. Then $f^* E_k(\mathbb{K}^\infty) \cong E$ via restriction of φ. The last assertion follows from the definition of $E_k(\mathbb{K}^\infty)$(4.15.2.35) and(4.15.2.15).

Cf.[AGP02]P284.? □

Cor. (4.15.3.21). By(4.14.6.13), there are isomorphisms

$$\mathcal{V}\mathrm{ect}^{\mathbb{R}}_1(X) \cong [X, \mathrm{Gra}(1, \mathbb{R}^\infty)] = [X, K(\mathbb{Z}/(2), 1)] = H^1(X, \mathbb{F}_2).$$

$$\mathcal{V}\mathrm{ect}^{\mathbb{C}}_1(X) \cong [X, \mathrm{Gra}(1, \mathbb{C}^\infty)] = [X, K(\mathbb{Z}, 2)] = H^2(X, \mathbb{Z}).$$

⌟

Cohomology of Classifying Spaces

Prop. (4.15.3.22). $H_*(\mathbb{B}G, \mathbb{Z}) \cong H_*(\Lambda, \mathbb{Z})$ and $H^*(\mathbb{B}G, \mathbb{Z}) \cong H^*(G, \mathbb{Z})$. ⌟

Proof: Because EG is weakly contractible, $S_*(EG)$ is a free $\mathbb{Z}[G]$-module resolution of $\mathbb{Z}$ and $S_*(EG)_G$ is identified with $S_*(BG)$. The rest is easy. □

Def. (4.15.3.23) [Whitney Sums]. ⌟

Prop. (4.15.3.24). The diagonal map $O(1)^n \to O(n)$ induces a map

$$\omega : (\mathbb{RP}^\infty)^n \cong (\mathbb{B}O(1))^n \to \mathbb{B}O(n).$$

The conjugation by permutation matrices preserves $O(1)^n$, thus induces a covariant action on this map. The action on $\mathbb{B}O(n)$ is identity?, and the action on $(\mathbb{B}O(1))^n$ is by permutation.

Then it induces a map

$$H^*(\mathbb{B}O(n)) \to H^*((\mathbb{B}O(1))^n)^{S_n} \cong \mathbb{F}_2[\sigma_1, \sigma_2, \ldots, \sigma_n]$$

where σ_i are the elementary symmetric functions. This is injective and thus surjective when tensoring any field, thus it is a bijection?.

Denote the inverse image of σ_i by w_i, then

$$H^*(\mathbb{B}O(n)) \cong \mathbb{F}_2[w_1, \ldots, w_n], \quad |w_i| = i$$

and these elements satisfy

- $c_0 = 1$.
- $i_1^*(c_1)$ is the canonical generator of $H^2(\mathbb{B}U(1))$.
- $i_n^*(w_i) = c_i$.

- $p^*(w_i) = \sum_{j=0}^{i} w_j \otimes w_{i-j}$.

⌟

Proof: Cf.[Cohomology of Classifying Space Toda P82]. □

Prop. (4.15.3.25)[$H^*(\mathbb{B}SO(n), \mathbb{F}_2)$]**.** $\mathrm{pr} : \mathbb{B}SO(n) \to \mathbb{B}O(n)$ is the universal covering with fiber $\mathbb{Z}/(2)$, and

$$H^*(\mathbb{B}SO(n), \mathbb{F}_2) \cong \mathbb{F}_2[\mathrm{pr}^* \omega_2, \ldots, \mathrm{pr}^* \omega_n].$$

⌟

Proof:

□

Prop. (4.15.3.26). The diagonal map $U(1)^n \to U(n)$ induces a map

$$\omega : (\mathbb{CP}^\infty)^n \cong (\mathbb{B}U(1))^n \to \mathbb{B}U(n).$$

The conjugation by permutation matrices preserves $U(1)^n$, thus induces a covariant action on this map. The action on $\mathbb{B}U(n)$ is identity?, and the action on $(\mathbb{B}U(1))^n$ is by permutation.

Then it induces a map

$$H^*(\mathbb{B}U(n)) \to H^*((\mathbb{B}U(1))^n)^{\mathcal{S}_n} \cong \mathbb{Z}[\sigma_1, \sigma_2, \ldots, \sigma_n]$$

where σ_i are the elementary symmetric functions. This is injective and thus surjective when tensoring any field, thus it is a bijection?.

Denote the inverse image of σ_i by c_i, then

$$H^*(\mathbb{B}U(n)) \cong \mathbb{Z}[c_1, \ldots, c_n], \quad |c_i| = 2i$$

and these elements satisfy

- $c_0 = 1$.
- $i_1^*(c_1)$ is the canonical generator of $H^2(\mathbb{B}U(1))$.
- $i_n^*(c_i) = c_i$.
- $p^*(c_i) = \sum_{j=0}^{i} c_j \otimes c_{i-j}$.

⌟

Proof: Cf.[Cohomology of Classifying Space Toda P81]. □

Prop. (4.15.3.27).

$$H^*(BO(2n), \mathbb{Z}[\frac{1}{2}]) \cong H^*(BO(2n+1), \mathbb{Z}[\frac{1}{2}]) \cong H^*(BSO(2n+1), \mathbb{Z}[\frac{1}{2}]) = \mathbb{Z}[\frac{1}{2}][p_1, p_2, \ldots, p_n], \quad |p_i| = 4i$$

$$H^*(BSO(2n), \mathbb{Z}[\frac{1}{2}]) = \mathbb{Z}[\frac{1}{2}][p_1, p_2, \ldots, p_n, e], e^2 = p_n, \quad |p_i| = 4i$$

Cf.[Cohomology of Classifying Space Toda P81]. ⌟

Prop. (4.15.3.28)[Complexifications]. As $\mathbb{B}SO(n)$ is the set of oriented real n-planes in $\mathbb{R}^\infty$, $BU(n)$ is the set of complex n-planes in $\mathbb{C}^\infty$, regarding a complex n-plane as an oriented real $2n$-plane induces a map

$$r : \mathbb{B}U(n) \to \mathbb{B}SO(2n).$$

And complexification of a real plane induces a map

$$\mathsf{c} : \mathbb{B}O(n) \to \mathbb{B}U(n).$$

Then

$$p_k = (-1)^k \mathsf{c}^*(c_{2k}) \in H^{4k}(\mathbb{B}O(n)), \quad \mathsf{c}^*(c_k) = w_k^2 \in H^{2k}(\mathbb{B}O(n), \mathbb{F}_2), \quad p_k = w_{2k}^2 \in H^{4k}(\mathbb{B}O(n), \mathbb{F}_2)$$

$$r^*(w_{2k}) = c_k \in H^{2k}(\mathbb{B}U(n), \mathbb{F}_2), \quad r^*(e) = c_n \in \mathbb{H}^{2n}(BU(n)).$$

$$Bk^*(p_k) = \sum_{i+j=k} (-1)^i c_i c_j, \quad .$$

Cf.[Cohomology of Classifying Space Toda P81]. ⌟

4 Characteristic Classes

References are [Cohomology of Classifying Space, Toda], [May99] and [M-S74].

Def. (4.15.4.1) [Characteristic Classes]. For an ES-cohomology theory E^*, $p \in \mathbb{Z}, n \in \mathbb{N}$, a **characteristic class** functor of degree p for n-dimensional $\mathbb{K}$-bundles is a natural assignment $c : \mathcal{V}\mathrm{ect}^n_{\mathbb{K}}(X) \to E^p(X)$ for any $X \in \mathcal{T}\mathrm{op}$ paracompact that is functorial w.r.t. pullbacks.

By(4.15.3.20), there is a bijection between characteristic class functors of degree p with elements in $E^p(BO(n))$. ⌟

Stiefel-Whitney Classes

Def. (4.15.4.2) [Stiefel-Whitney Classes]. A **Stiefel-Whitney class** functor w for real bundles is a total characteristic class functor for real bundles for the ordinary cohomology theory with $\mathbb{F}_2$ coefficients $H^*(-, \mathbb{F}_2)$ that satisfies:

- $w(E) = 1 + w_1(E) + \ldots + w_n(E) \in H^*(X, \mathbb{F}_2), \quad |w_i| = i, n = \mathrm{rank}(E).$
- $f^*(w(E)) = w(f^*(E)).$
- $w(E \oplus F) = w(E)w(F).$
- On the tautological bundle γ_1^1 over $\mathbb{RP}^1$, $w(\gamma_1^1) = 1 + w_1(\gamma_1^1)$ and $w_1(\gamma_1^1)$ is the unique non-trivial element in $H^1(\mathbb{RP}^1, \mathbb{F}_2)$.

⌟

Prop. (4.15.4.3)[Existence and Uniqueness of Stiefel-Whitney Classes]. There exists uniquely a Stiefel-Whitney class functor, and they can be defined using the Thom isomorphism

$$\varphi_E : H^i(B; \mathbb{F}_2) \cong H^{i+n}(E, E \backslash B; \mathbb{F}_2)\text{(4.15.2.26)}$$

as

$$w(E) = \varphi_E^{-1} \operatorname{Sq}(\varphi_E(1)) \in H^*(B; \mathbb{F}_2) = \varphi^{-1} \operatorname{Sq}(u_E).$$

⌟

Proof: Cf.[May, P191] and [Milnor, P92].**?** □

Prop. (4.15.4.4). For $B \in \mathcal{T}\mathrm{op}$ paracompact, $E, E' \in \mathcal{V}\mathrm{ect}_{\mathbb{R}}(B)$, then

- If E is trivial, $w(E) = 1$.
- If $E \oplus E'$ is trivial, then

$$w(E') = w(E)^{-1} = 1 + w_1 + (w_1^2 + w_2) + (w_1^3 + w_3) + (w_1^4 + w_1^2 w_2 + w_2^2 + w_4) + \dots.$$

- Let γ_n^1 be the tautological line bundle over $\mathbb{RP}^n$(4.15.2.31), then $w(\gamma_n^1) = 1 + a$.
- Let ξ, η be vector bundles on M, N, then

$$w(\xi \times \eta) = \pi_1^* w(\xi) \cup \pi_2^* w(\eta) = w(\xi) \times w(\eta)$$

in $H^*(M \times N, \mathbb{F}_2)$.

⌟

Proof: 1: A trivial bundle is the pullback of a bundle over pt, thus $w(f^*(E)) = w^*(e(E)) = 1$.

2 is trivial.

3: This is because $E_1(\mathbb{R})/\mathbb{RP}^1 \to E_1(\mathbb{R}^n)/\mathbb{RP}^n$ is a bundle map, thus $w_1(E_1(\mathbb{R}^n))$ pulls back to $w_1(E_1(\mathbb{R})) \neq 0$, thus $w_1(E_1(\mathbb{R}^n)) = a$.

4: This follows from the definition that $\xi \times \eta = \pi_1^* \xi \oplus \pi_2^* \eta$ and Künneth formula(4.14.2.13). □

Cor. (4.15.4.5) [Tangent and Normal Bundles]. Let M be a submanifold of a smooth manifold N, let $\mathcal{T}_M, \mathcal{T}_N$ be the tangent bundles and ν the normal bundle, then

$$w(\mathcal{N}_{M/N}) = w(\mathcal{T}_N) w(\mathcal{T}_M)^{-1}$$

⌟

Proof: This follows form the smooth nbhd theorem**?**. □

Prop. (4.15.4.6) [Wu Formula]. For $E \in \mathcal{V}\mathrm{ect}_B$,

$$\mathrm{Sq}^i(w_j) = \sum_{t=0}^{i} \binom{j+t-i-1}{t} w_{i-t} w_{i+t}$$

⌟

Proof: Use splitting principal. □

Def. (4.15.4.7) [Characteristic Classes of Smooth Manifolds]. For $M \in \mathcal{M}\mathrm{ani}_{\mathrm{sm}}$, denote $w(M) = w(TM)$. ⌟

Prop. (4.15.4.8) [Wu Formula]. For $M \in \mathcal{M}\mathrm{ani}^d_{\mathrm{sm,cpct}}$, define the **Wu class** $v = \sum v_i \in H^*(M, \mathbb{F}_2)$ s.t.

$$\langle \nu(M) \cup x, [M]_2 \rangle = \langle \mathrm{Sq}(x), [M]_2 \rangle$$

for any $x \in H^*(M, \mathbb{F}_2)$. In particular, $\nu_k(M)_k \cup x = \mathrm{Sq}^k(x)$ for any $x \in H^{d-k}(M, \mathbb{F}_2)$. Notice such a class exists by Poincaré duality.

Then the Stiefel-Whitney class of M is given by the Wu class:

$$w(M) = \mathrm{Sq}(\nu(M))\text{(4.14.6.14)}.$$

⌟

Proof: Cf.[Milnor, P132]. □

Cor. (4.15.4.9) [Homotopy Invariance of Stiefel-Whitney Classes of Manifolds]. The Stiefel-Whitney classes only depends on the homotopy type of M, and pullbacks of Stiefel-Whitney classes along smooth maps between smooth manifolds only depends on the homotopy type of the map. ⌟

Def. (4.15.4.10) [Stiefel-Whitney Numbers]. Let M be a closed smooth manifold of dimension n, then for each tuple $(i_1, \ldots, i_k)$ with $i_1 + \ldots + i_k = n$, define the **Stiefel-Whitney number**

$$w_{i_1,\ldots,i_k}(M) = (w_{i_1}(TM) \cup \ldots \cup w_{i_k}(TM), [M]) \in \mathbb{Z}/2\mathbb{Z}.$$

⌟

Euler Classes

Def. (4.15.4.11) [Euler Classes]. Axioms for **Euler classes** for orientable real bundles E/B:

- $e(e^1) = 0$.
- For any map $f : B' \to B$, $f^*(e(E)) = e(f^*(E))$.
- $e(E \oplus F) = e(E)e(F)$.
- for the opposite orientation $-E$, $e(-E) = -e(E)$.

⌟

Prop. (4.15.4.12) [Existence of Euler Classes]. For any oriented $E/B \in \mathcal{V}\mathrm{ect}_{\mathbb{R}}(B)$, let $e(E)$ be defined as the image of the Thom class(4.15.2.26) under the maps

$$\varphi_E^{-1} : H^n(E, E_0, \mathbb{Z}) \to H^n(E, \mathbb{Z}) \cong H^n(B, \mathbb{Z}).$$

or equivalently, $e(E) = \varphi^{-1}(u_E \cup u_E)$ where u_E is the Thom class and $\varphi_{\mathbb{Z}}$ is the Thom isomorphism(4.15.2.26). then it is the desired Euler class. ⌟

Proof: **?**

1: If E has a non-zero section $s : B \to E_0$, then $B \xrightarrow{s} E_0 \subset E \to B$ is identity, thus

$$H^n(B) \xrightarrow{\pi^*} H^n(E) \to H^n(E_0) \xrightarrow{s^*} H^n(B)$$

is the identity. But $H^n(B) \xrightarrow{\pi^*} H^n(E) \to H^n(E_0)$ equals the restriction of u_E to E_0, which is 0.

2: This $e(E)$ is compatible with base change by(4.15.2.27) and the definition.

3: For products, Cf.[Milnor, P100].

4: If the orientation is reversed, then $u_{-E} = -u_E$. □

Cor. (4.15.4.13).

- For a trivial line bundle, $e(E) = 0$.
- For an odd dimensional vector space E/B, $2e(E) = 0$.

⌟

Proof: 1: A trivial bundle is the pullback of a bundle over pt, thus $e(f^*(E)) = f^*(e(E))$ is trivial.

2: This is because their is an orientation preserving isomorphism $(-1) : E/B \cong (-E)/B$ that is isomorphism on the base, so $e(-E) = e(E)$. □

Cor. (4.15.4.14) [Euler classes and Whitney Classes]. For a vector bundle E/B of rank n, the natural map $H^n(B,\mathbb{Z}) \to H^n(B,\mathbb{Z}/2\mathbb{Z})$ maps the Euler class $e(E)$ to the top Whitney class $w_n(E)$. ⌟

Proof: $e(E) = \varphi^{-1}(u_E \times u_E)$, which maps to $\varphi_2^{-1}(u_{E,2} \cup u_{E,2}) = \varphi_2^{-1}(Sq^n(u_{E,2})) = w_n(E)$ by(4.15.2.27). □

Prop. (4.15.4.15) [Euler Class and Euler Characteristic]. For $M \in \mathcal{M}\mathrm{ani}_{\mathrm{cpct,sm,orntd}}$, then

$$\langle e(\mathcal{T}_M), [M]\rangle = \chi(M).$$

⌟

Proof: **?** □

Chern Classes

Def. (4.15.4.16) [Chern Classes]. Axioms for **Chern classes** for complex bundles:

- $c(E) = 1 + c_1(E) + \ldots + c_n(E) \in H^*(X,\mathbb{Z}), \quad |c_i| = 2i, n = \deg(E)$.
- $f^*(c(E)) = c(f^*(E))$.
- $c(E \oplus F) = c(E)c(F)$.
- For the tautological bundle η over $\mathbb{CP}^\infty$, $c_1(\eta)$ corresponds to the element id $\in [\mathbb{CP}^\infty, \mathbb{CP}^\infty] \cong H^2(\mathbb{CP}^\infty)$.

⌟

Prop. (4.15.4.17). There exists uniquely a natural transformation $c : Vect_{\mathbb{C}}(X) \to H^*(X,\mathbb{Z})$ satisfying these axioms. (For this, it suffice to calculate the cohomology ring of $BGL_n(\mathbb{C})$, Cf.[Cohomology of Classifying Space Toda]). ⌟

Cor. (4.15.4.18). For a trivial bundle $E = \underline{\mathbb{C}}$, $c_i(E) = 0$ for $i > 0$, because E is a pullback from a bundle on pt.

In particular, for any complex vector bundle E, $c(E \oplus \underline{\mathbb{C}}) = c(E)$. ⌟

Prop. (4.15.4.19) [First Chern Class Map]. A complex line bundle can be seen as an element of $H^1(X, \underline{\mathbb{C}}^*)$, by(6.3.2.14), by the exact sequence

$$0 \to \underline{\mathbb{Z}} \to \underline{\mathbb{C}} \xrightarrow{exp(2\pi i -)} \underline{\mathbb{C}^*} \to 0$$

($\mathbb{C}$ is sheaf of smooth functions from X to $\mathbb{C}$)which gives a map $H^1(X,\mathbb{C}^*) \to H^2(X,\mathbb{Z})$, called the **first Chern class map**. It is called so because it gives the first Chern class of this complex line bundle. It is also an isomorphism because $\mathbb{C}$ is fine sheaf so acyclic. ⌟

Proof: Only have to prove they are equal in $H^2(X,\mathbb{C})$. We choose a totally convex covering U_i of X by(12.3.3.21), then it is a fine cover, so by(6.3.2.15) the Čech cohomology and sheaf cohomology equal.

Use the Chern-Weil map definition of the Chern class, a connection on a line bundle satisfies $\nabla e_\alpha = \omega_\alpha e_\alpha$, and if $e_\beta = e_\alpha g_{\alpha\beta}$, then $\omega_\beta = g_{\alpha\beta}^{-1}\omega_\alpha g_{\alpha\beta} + g_{\alpha\beta}^{-1} dg_{\alpha\beta} = \omega_\alpha + d(\log g_{\alpha\beta})$. So $\Omega_\alpha = d\omega_\alpha$ locally, and the first Chern class is giving by Ω_α in $H^2(X,\mathbb{C})$.

Then we need to understand the deRham isomorphism. For the exact sequence $0 \to \underline{\mathbb{C}} \to \mathcal{A}^0 \to \mathcal{A}^1 \to \ldots$, it has a splitting: $0 \to \underline{\mathbb{C}} \to \mathcal{K}^1 \to 0$ and $0 \to \mathcal{K}^1 \to 0 \to \mathcal{A}^1 \to \mathcal{K}^2 \to 0$, this gives

$$0 \to H^1(X, \mathcal{K}^1) \xrightarrow{\delta} H^2(X, \underline{\mathbb{C}}) \to 0, \quad \mathcal{A}^1(X) \to \mathcal{K}^2(X) \xrightarrow{\delta} H^1(X, \mathcal{K}^1) \to 0.$$

because $\mathcal{A}^k$ are fine sheaves. The composite of them is just the de Rham isomorphism(Here we are identifying $H^2(X, \underline{\mathbb{C}})$ to $H^2(X, \mathbb{C})$ by(6.3.5.9)). Tracking the lifting, we notice Ω is mapped to the cocycle $\{\log g_{\alpha\beta} + \log g_{\beta\gamma} - \log g_{\alpha-\beta}\}$, which is exactly the image of the first Chern class map. □

Cor. (4.15.4.20). Complex line bundles are characterized by the first Chern class up to smooth isomorphism, because $H^1(X, \mathbb{C}^*) \to H^2(X, \mathbb{Z})$ is an isomorphism. ⌟

Pontryagin Classes

Def. (4.15.4.21) [Pontryagin Classes]. The Pontryagin classes are defined as $p_k(E) = (-1)^k c_{2k}(E_{\mathbb{C}}) \in \mathrm{H}^{4k}(X, \mathbb{Z})$. ⌟

Def. (4.15.4.22) [Pontryagin Number]. Let M be a closed manifold of dimension $4n$, then for each tuple $I = (i_1, \ldots, i_k)$ with $i_1 + \ldots + i_k = n$, define the **Pontryagin numbers**

$$p_I(M) = (p_{i_1}(TM) \cup \ldots \cup p_{i_k}(TM), [M]) \in \mathbb{Z}.$$

⌟

Prop. (4.15.4.23) [Pontryagin Number of Product Manifolds]. Let M, N be closed submanifolds of dimension $4m, 4n$ resp., then for any tuple $I = (i_1, \ldots, i_k)$ with $i_1 + \ldots + i_k = m + n$,

$$p_I(M \times N) = \sum_{I_1, I_2 | I_1 \coprod I_2 = I} p_{I_1}(M) p_{I_2}(N)$$

where the summation is over all partitions I_1, I_2 of m, n resp.. ⌟

Proof: Cf.[Milnor, P193]. □

Combinatorial Pontryagin Classes

See [Milnor]Chap20.

Calculations and Applications

Prop. (4.15.4.24). $w(\mathbb{RP}^n) = (1 + a)^{n+1}$. In particular, $w(\mathbb{RP}^n) = 1$ iff $n = 2^k - 1$ for some k. ⌟

Proof: This follows from(4.15.2.32). □

Cor. (4.15.4.25). Let $n = 2^k - 1 - r$, where $r \leq 2^{k-1} - 1$, then $\mathbb{RP}^n$ can be immersed into $\mathbb{R}^{n+d}$ iff $d \geq r$. ⌟

Proof: By(4.15.4.5), the normal bundle ν satisfies $w(\nu) = (1+a)^r$, and $r < n$, thus $d = \mathrm{rank}(\nu) \geq r$. □

Cor. (4.15.4.26). If $n + 1 = 2^r m$, then there doesn't exist 2^r-linearly independent vector fields on $\mathbb{RP}^n$. ⌟

Proof: This is because if their is, then $w(\mathbb{RP}^n)$ has degree$\leq n-2^r = 2^r(m-1)-1$, but in fact it equals $(1+a^{2^r})^m$ has leading term $a^{2^r(m-1)}$. □

Remark (4.15.4.27). By considering irreducibility, we can prove stronger results, like $\tau_{\mathbb{RP}^4}$ doesn't contain a subbundle of rank2. ⌟

Prop. (4.15.4.28) [Non-Vanishing Vectors]. $\mathbb{RP}^n$ admits a non-vanishing vector field iff n is odd. ⌟

Proof: If $n = 2k+1$, consider the non-vanishing vector field on $\mathbb{S}^{2k+1} : (x_1,\ldots,x_{2k+2}) \mapsto (x_2,-x_1,x_4,-x_3,\ldots,x_{2k+2},-x_{2k+1})$. Then This descends to a non-vanishing vector field on $\mathbb{RP}^{2k+1}$. Conversely, if $n=2k$, by(4.15.4.26), there doesn't exists a non-vanishing vector field on $\mathbb{RP}^{2k}$. □

5 K-Theory

Def. (4.15.5.1) [Topological K-Groups]. For $X \in \mathcal{T}\mathrm{op}_{\mathrm{cpct}}$, the **K-group** $K(X)$ is defined to be $K_0(\mathcal{V}\mathrm{ect}(X))$(10.1.2.6), which is a ring under sum and tensor. Two vector bundles E,F are called **stably equivalent** if $[E]=[F]$.

There is a degree map $\deg K(X)\to\mathbb{Z}$, and the kernel is denoted by $\widetilde{K}(X)$. There is a canonical splitting $K(X)\cong\widetilde{K}(X)\oplus\mathbb{Z}$. ⌟

Prop. (4.15.5.2). A continuous map $f:X\to Y$ induces a group morphism $f^*:K(Y)\to K(X)$. By(4.15.1.9), this map only depends on $f\in[X,Y]$. ⌟

Prop. (4.15.5.3). By(4.15.2.20), over a compact Hausdorff space, E,F is stably equivalent iff $E\oplus\mathbb{R}^n\cong F\oplus\mathbb{R}^n$ for some n. ⌟

Thm. (4.15.5.4) [Periodicity Theorem]. Let L be a line bundle over X, then as a $K(X)$-algebra, $K(P(L\oplus 1))$ is generated by $[H]$, and is subject to the single relation $([H]-[1])([L][H]-[1])=0$. ⌟

Proof: Cf.[K theory, Atiyah, P46]. □

Cor. (4.15.5.5). $K(S^2)$ is generated by $[H]$ as a $K(\mathrm{pt})$-module, and is subject to the single relation $([H]-[1])^2=0$. ⌟

Cor. (4.15.5.6). There is an isomorphism $\mu: K(X)\otimes K(S^2)\to K(X\times S^2)$, where $\mu(a\otimes b)=(\pi_1^*a)(\pi_2^*b)$. ⌟

Def. (4.15.5.7) [Setup for Proof of Periodicity Theorem]. Given a line bundle E over X, we can associate a projective bundle $P(E)$ that $P(E)_x = P(E_x)$. Now denote P^0 the subspace of $P(E)$ consisting of all vectors of length≤ 1 and P_∞ the subspace consisting of all vectors of length≥ 1 together with the infinity section. There are projections $\pi_0: P_0\to X$ and $\pi_\infty: P_\infty\to X$, which are homotopy equivalences.

Now by(4.15.2.8), ⌟

6 Adam Operators

7 Cobordism

Def. (4.15.7.1) [Bordism Groups]. If X is a topological space, define the **bordism group** $\Omega_n(X)$ to be the set of pairs (M,f) where M is a closed smooth manifold of dimension n and $f:M\to X$ is a continuous map, under the equivalence relation that $(M_0, f_0) \sim (M_1, f_1)$ iff there is an $n+1$ manifold N and a map $F : N \to X$ that $\partial F = f_1 \coprod f_2$. This is a vector space over $\mathbb{F}_2$.

Let $\Omega_n = \Omega_n(\mathrm{pt})$, then for any m, n, there is a map $\Omega_m \times \Omega_n \to \Omega_{m+n} : (M, N) \mapsto M \times N$, so Ω_* is a graded commutative ring. ⌟

Prop. (4.15.7.2) [Thom]. If $N \in \mathcal{M}\mathrm{ani}^{n+1}_{\mathrm{sm,cpct},\partial}$ and $\partial(N) = M$, then all the Stiefel-Whitney numbers of M vanish.

Conversely, if $M \in \mathcal{M}\mathrm{ani}^{n}_{\mathrm{sm,cpct}}$ with all Stiefel-Whitney numbers 0, then it is the boundary of a compact smooth manifold with boundary. ⌟

Proof: Let $[N] \in H_{n+1}(N, M)$ be the fundamental homology class of the pair, then $\partial([N]) = [M]$. Let τ_N, M be the tangent bundle of N, M, then $\tau_N|_M = \tau_M \oplus \mathbb{R}^1$, because there is an outward pointing normal bundle. Thus the Stiefel-Whitney classes of M comes from restriction of that of N. Now the composite $H^n(N) \to H^n(M) \xrightarrow{\delta} H^n(N, M)$ is 0, so $\delta(w_{i_1,\ldots,i_k}(M)) = 0$. thus

$$\langle w_{i_1,\ldots,i_k}(M), [M]\rangle = \langle \delta(w_{i_1,\ldots,i_k}(M)), [N]\rangle = 0.$$

Conversely, Cf.[Stong, Notes on Cobordism Theory].? □

Prop. (4.15.7.3). For $m \in \mathbb{Z}_+$, $\mathbb{RP}^{2m-1}$ is a boundary and $\mathbb{RP}^{2m}$ is not a boundary. ⌟

Proof: Consider the fiber bundle $S^1 \to \mathbb{RP}^{2n-1} \to \mathbb{CP}^n$, its cone bundle is $D^1 \to M^n \to \mathbb{CP}^{2n-1}$, which has boundary $\mathbb{RP}^{2n-1}$.

$\mathbb{RP}^{2m}$ is not a boundary by(4.15.7.2) and the fact its top Stiefel-Whitney class is non-zero. □

Thm. (4.15.7.4) [Thom].

$$\Omega_* = \mathbb{F}_2[t_2, t_4, t_5, \ldots,]$$

is a graded polynomial algebra where there's one generator $t_n \in \Omega_n$ for each $n \neq 2^k - 1$.

Also $\Omega_*(X) = H_*(X, \Omega_*) \cong H_*(X, \mathbb{F}_2) \otimes_{\mathbb{F}_2} \Omega_*$. ⌟

Proof:

□

Cor. (4.15.7.5). A map $f : X \to Y$ induces a map $f_* : \Omega_n(X) \to \Omega_n(Y)$. This map only depends on the homotopy type of f. ⌟

Oriented Cobordism

Def. (4.15.7.6)[Oriented Bordism Groups]. When X is an orientable manifold, define the **oriented bordism group** $\Omega^{so}_n(X)$ to be the set of pairs (M, f) where M is an oriented smooth manifold of dimension n and $f : M \to X$ is a continuous map preserving orientation, under the equivalence relation that $(M_0, f_0) \sim (M_1, f_1)$ iff there is an $n+1$ manifold N and a map $F : N \to X$ that $\partial F = (-f_1) \coprod f_2$.

Let $\Omega^{so}_n = \Omega^{so}_n(\mathrm{pt})$, then for any m, n, there is a map $\Omega^{so}_m \times \Omega^{so}_n \to \Omega^{so}_{m+n} : (M, N) \mapsto M \times N$, and $M \times N \cong (-1)^{mn} N \times M$, so Ω^{so}_* is a graded anti-commutative ring. ⌟

Prop. (4.15.7.7). The relation of (oriented) bordism is truly an equivalence class. It suffices to show transitivity, and this is because we can piece together two manifold with boundaries by collar neighborhood theorem(12.1.1.2). ⌟

Prop. (4.15.7.8). If $N \in \mathcal{M}\mathrm{ani}^{n+1}_{\mathrm{sm,cpct,orntd},\partial}$ and $\partial(N) = M$, then all the Pontryagin numbers of M vanish. ⌟

Proof: Let $[N] \in H_{n+1}(N, M)$ be the fundamental homology class of the pair, then $\partial([N]) = [M]$. Let τ_N, M be the tangent bundle of N, M, then $\tau_N|_M = \tau_M \oplus \mathbb{R}^1$, because there is an outward pointing normal bundle. Thus the Stiefel-Whitney classes of M comes from restriction of that of N. Now the composite $H^n(N) \to H^n(M) \xrightarrow{\delta} H^n(N, M)$ is 0, so $\delta(w_{i_1,\ldots,i_k}(M)) = 0$. thus

$$\langle w_{i_1,\ldots,i_k}(M), [M]\rangle = \langle \delta(w_{i_1,\ldots,i_k}(M)), [N]\rangle = 0.$$

□

Prop. (4.15.7.9) [Mayer-Vitories]. Let $X = U \cup V$ where U, V are open subsets of X, **?** ⌟

Thm. (4.15.7.10) [Thom].

$$\Omega^{so}_* \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}[u_1, \ldots, u_n, \ldots],$$

where $u_i \in \Omega^{so}_{4i}$ and is represented by $[\mathbb{CP}^{2i}]$. Moreover,

- $\Omega^{so}_0 = \mathbb{Z}$.
- $\Omega^{so}_1 = 0$.
- $\Omega^{so}_2 = 0$.
- $\Omega^{so}_3 = 0$.
- $\Omega^{so}_4 = \mathbb{Z}$, generated by $\mathbb{CP}^2$.
- $\Omega^{so}_5 = \mathbb{Z}/2\mathbb{Z}$, generated by Y^5.
- $\Omega^{so}_6 = 0$.
- $\Omega^{so}_7 = 0$.
- $\Omega^{so}_8 = \mathbb{Z} \oplus \mathbb{Z}$, generated by $\mathbb{CP}^4$ and $\mathrm{CP}^2 \times \mathbb{CP}^2$.
- $\Omega^{so}_9 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, generated by Y^9 and $Y^5 \times \mathbb{CP}^2$.
- $\Omega^{so}_{10} = \mathbb{Z}/2\mathbb{Z}$, generated by $Y^5 \times Y^5$.
- $\Omega^{so}_{11} = \mathbb{Z}/2\mathbb{Z}$, generated by Y^{11}.
- $\Omega^{so}_n \neq 0$ for $n \geq 8$.

⌟

Proof: Cf.[Milnor, P203].

By (4.15.7.8), for any partition I of k, there is a map $\Omega_{4k} \to \mathbb{Z} : M \mapsto p_I(M)$. These maps can be used to show that the products $\{\mathbb{CP}^{2i_1} \times \mathbb{CP}^{2i_r} | \sum i_r = k\}$ are linearly independent in Ω_{4k} by(4.15.4.23). □

Prop. (4.15.7.11) [Index and Oriented Cobordism]. If $k \in \mathbb{N}, W \in \mathcal{M}\mathrm{ani}^{4k+1}_{\mathrm{cntd,orntd,cpct}}$, then the index $I(M) = 0$. ⌟

Proof: This follows from the fact the image of $H^{2k}(W) \xrightarrow{i^*} H^{2k}(M)$ is a half-dimensional subspace(4.14.3.18) that the intersection product is trivial:

$$\langle i^*\alpha \cup i^*\beta, \partial[W]\rangle = \langle \alpha \cup \beta, i_*\partial[W]\rangle = 0.$$

Then it is by linear algebra**?** that the signature of this pairing is 0. □

Def. (4.15.7.12) [Stably Framed Manifold]. A **stably framed manifold** is a smooth manifold M of dimension n together with an isomorphism $TM \oplus \mathbb{R}^N \cong \mathbb{R}^{N+n}$ for some N. ⌟

Def. (4.15.7.13) [Framed Bordism Groups]. Because $T(\partial N) \oplus \mathbb{R} \cong TN|_{\partial N}$, we have the notion of a stably framed bordism $\Omega_n^{fr}(X)$. Denote $\Omega_n^{fr} = \Omega_n^{fr}(\mathrm{pt})$. ⌟

Prop. (4.15.7.14). $S^3 \cong SU(2)$ is naturally framed, and this generates $\Omega_3^{fr} \cong \mathbb{Z}/24$. ⌟

Thm. (4.15.7.15) [Pontryagin]. $\Omega_n^{fr} \cong \pi_{n+N}(S^N)$. ⌟

8 Applications

Prop. (4.15.8.1). A simply connected manifold is orientable. (Use the orientable double cover). ⌟

4.16 Stable Homotopy Theory

Main references are [Higher Algebra, Lurie].

5 Commutative Algebras

5.1 Commutative Algebra I

Main References are [A-M69], [Mat80], [Sta]Chap10, [Commutative Algebra with a View Towards Algebraic Geometry] and [Wei94]Chap4.

Commutative rings are studied in this subsection.

Notation (5.1.0.1).

- All rings and algebras in this section is assumed to be commutative.

⌟

1 Basics

Def. (5.1.1.1) [Integral Monoids]. An **integral monoid** is a monoid $M \in \mathcal{CM}\mathrm{on}^{0,1}$ s.t. for any $a, b \in M$, $ab = 0$ implies $a = 0$ or $b = 0$. ⌟

Def. (5.1.1.2) [Ideals]. For $R \in \mathcal{CM}\mathrm{on}^{0,1}$, an **ideal** of R is a subgroup $I \leq R$ that is a left ideal. The category of ideals of R is denoted by $\mathrm{Ideal}(R)$. ⌟

Prop. (5.1.1.3) [Quotients]. For $R \in \mathcal{CR}\mathrm{ing}, I \in \mathrm{Ideal}(R)$, there is a **quotient ring** $R/I \in \mathcal{CR}\mathrm{ing}_R$ with the universal property: any $f : R \to R' \in \mathcal{CR}\mathrm{ing}$ that vanishes on I factors through R/I. ⌟

Proof: □

Prop. (5.1.1.4). The quotient map induces an order-preserving bijection of ideals of A/I and ideals of A containing I. ⌟

Prop. (5.1.1.5) [Prime Avoidance]. Let $R \in \mathcal{CR}\mathrm{ing}, I \in \mathrm{Ideal}(R)$, and $\mathfrak{p}_i$ are f.m. prime ideals that $I \not\subseteq \mathfrak{p}_i$ for any i, then $I \not\subseteq \cup\mathfrak{p}_i$. ⌟

Proof: Use induction on the number of primes n. For $n = 1$ this is trivial. For $n > 2$, let $z_i \in I \backslash \cup_{j \neq i} P_j$. Now consider $z = z_1 \cdot z_{n-1} + z_n$. If $z \in P_i$ for some $i < n$, then $z_n \in P_i$, contradiction. If $z \in P_n$, then some $z_i, i < n$ is in P_n because P_n is a prime ideal, contradiction. □

Prop. (5.1.1.6) [Existence of a Maximal Ideal]. Any non-zero commutative ring has a maximal ideal. ⌟

Proof: Use Zorn's lemma, the union of a chain of ideals is an ideal. □

Cor. (5.1.1.7). Any non-trivial ideal is contained in a maximal ideal. ⌟

Proof: If $I \subset A$ is a non-trivial ideal, then A/I is a non-zero ring, thus A/I has a maximal ideal, which corresponds to a maximal ideal of A containing I(5.1.1.4). □

Prop. (5.1.1.8). If $r(I)$ and $r(J)$ are coprime, then I, J are coprime. ⌟

Proof: As $a+b=1$, and $a^m \in I, b^n \in J$, $1=(a+b)^{m+n} \in I+J$. □

Def. (5.1.1.9) [Local Ring]. A **local ring** is a commutative ring R that has only one maximal ideal. Equivalently, there is a prime ideal $\mathfrak{m}$ that any element in $R\backslash\mathfrak{m}$ is invertible. ⌟

Proof: If $\mathfrak{m}$ is the maximal ideal, then for any $x \in R$, if (x) is not all of R, then x is contained in a maximal ideal by(5.1.1.6), which can only be $\mathfrak{m}$. Conversely, if there is a prime ideal $\mathfrak{m}$ that any element in $R\backslash\mathfrak{m}$ is invertible, then clearly every non-trivial ideal is included in $\mathfrak{m}$. □

Prop. (5.1.1.10). Any quotient of a local ring is also a local ring. ⌟

Def. (5.1.1.11) [Local Ring Map]. A map between two local rings are called **local ring map** iff it maps non-invertible elements to non-invertible elements, equivalently, $f^{-1}(\mathfrak{m}_S)=\mathfrak{m}_R$. ⌟

Def. (5.1.1.12) [Ideal of Definition]. In a Noetherian local ring $(R,\mathfrak{m})$, an ideal $I \subset R$ is called an **ideal of definition** if $\sqrt{I}=\mathfrak{m}$. ⌟

Prop. (5.1.1.13)[Ideals of Products and Filters]. If $F_i, i \in I$ is a collection of fields, then the prime ideals in the ring $\prod F_i$ is in bijection with the ultrafilters on I, where the ultrafilter $\mathcal{F}$ corresponds to the ideal $p_{\mathcal{F}}=\{(a_i)|\text{the set of coordinates that } a_i=0 \text{ is in } \mathcal{F}\}$. And in the same way, ideals of $\prod F_i$ corresponds to the filters on I. ⌟

Proof: Clearly $p_{\mathcal{F}}$ is an ideal, and if $\mathcal{F}$ is an ultrafilter, let $Z(a)$ be the coordinates that a is zero on, and notice $Z(ab)=Z(a)\cup Z(b)$, then $ab \in p$ iff $a \in p$ or $b \in p$, by(2.2.10.7), so it is a prime ideal.

Conversely, notice that any two a, b with $Z(a)=Z(b)$ differs by a unit, so $\mathcal{F}_p=\{Z(a)|z \in p\}$ is easily checked to be a filter. And if p is a prime, then for any $A \subset I$, let $a, b \in \prod F_i$ be that $Z(a)=A, Z(b)=I-A$, then $ab=0 \in p$, so $a \in p$ or $b \in p$. □

Def. (5.1.1.14)[Torsion-Free Modules]. Let $S \subset A$ be a set in a commutative ring, then an A-module M is called S**-torsion-free** if for any $\{x \in M|Sx=0\}=0$. ⌟

Prop. (5.1.1.15)[Maximal Torsion-Free Quotient]. Let $S \subset A$ be a set, the functor from the category of torsion-free A-modules to the category of A-modules has a left adjoint, called the **maximal** S**-torsion-free quotient**. ⌟

Proof: A quotient of M is determined by the kernel. It suffices to prove if $M/N_1, M/N_2$ are both S-torsion-free, then $M/N_1\cap N_2$ is also S-torsion-free: This is easy. □

Prop. (5.1.1.16). Let A be a ring and B a finite A-algebra. if $A \to B$ is epimorphism in the category of rings, then $A \to B$ is surjective. ⌟

Proof: Notice that $h^B \to h^A$ is injective iff $h^B \times_{h^A} h^B \cong h^B$, or equivalently, $B \times_A B \to B$ is an isomorphism. Now we can localize A at maximal ideals, thus we can assume A is local, with maximal ideal $\mathfrak{m}$ and residue field k. And then use Nakayama lemma, it suffices to show that $k \to B/\mathfrak{m}=C$ is surjective. But $C \times_k C \cong C$, so $\dim_k C=1$ or 0, which means $k \to C$ is surjective. □

Def. (5.1.1.17) [Locally Nilpotent]. A **locally nilpotent ideal** is an ideal consisting of nilpotent elements. ⌟

Prop. (5.1.1.18). If I is a locally nilpotent ideal of A, then $1+I \to 1+I : x \mapsto x^n$ is an isomorphism. ⌟

Proof: The converse is given by $x \mapsto (1+x)^{1/n} = 1 + \binom{1/n}{1}x + \binom{1/n}{2}x^2 + \ldots$. □

Cor. (5.1.1.19). If I is a locally nilpotent ideal of A, then a unit in A is an n-th power iff it is an n-th power in A/I. ⌟

Proof: If $a =\equiv b^n \mod I$, then b is also a unit, and $ab^{-n} = c^n$ for some n by(5.1.1.18), thus a is a n-th power. □

Tensor Product, Limits and Colimits

Remark (5.1.1.20) [Tensor Product]. Tensor product is defined in(3.2.4.13). Notice that in case the rings are all commutative, there are no need to distinguish between left and right modules. ⌟

Def. (5.1.1.21) [Tensor Algebras]. For a module M over a commutative ring R, we define the

- **tensor algebra** operator from $\mathcal{M}\mathrm{od}_R$ to graded algebras over R that is left adjoint to the forgetful functor. It can be defined as follows:

$$T(M) = \bigoplus_{n\geq 0} \otimes^n M$$

  as the module, and the algebra structure determined by the canonical map $\otimes^m M \times \otimes^n M \to \otimes^{m+n} M$.
- **exterior product** $\wedge^k M$ as the module with the universal property that $\mathrm{Hom}_B(\wedge^k M, N)$ is the set of all morphisms $M^n \to N$ that vanishes on all elements that have two equal coordinates.
- **exterior algebra** operator $\wedge$ from $\mathcal{M}\mathrm{od}_R$ to the category of strict graded commutative algebras over R that is left adjoint to the forgetful functor. It can be defined as follows: $\wedge(M) = T(M)/(x\otimes x)$, where $x \in M$, or equivalently $\wedge(M) = \bigoplus_{k\geq 0} \wedge^k(M)$.
- **symmetric algebra** operator S from $\mathcal{M}\mathrm{od}_R$ to $\mathcal{CR}\mathrm{ing}_R$ that is left adjoint to the forgetful functor. It can be defined as follows: $\wedge(M) = T(M)/(x\otimes y - y\otimes x)$ where $x, y \in M$.

⌟

Cor. (5.1.1.22). The construction of $T(M), \wedge M$ and $\mathrm{Sym}(M)$ commutes with all colimits, because they are all left adjoints. ⌟

Prop. (5.1.1.23) [Tensor Product and Quotient]. Let R be a commutative ring and I, J be ideals of R, then $R/I \otimes_R R/J \cong R/(I+J)$. ⌟

Proof: This follows from the universal property of quotient and tensoring. □

Prop. (5.1.1.24). There is a pullback square

$$\begin{array}{ccc} R/I\cap J & \longrightarrow & R/I \\ \downarrow & & \downarrow \\ R/J & \longrightarrow & R/(I+J) \end{array}$$

⌟

Proof: The pullback is just the elements in $R/I \times R/J$ that mapsto the same element in $R/(I+J)$. If $(x+I, y+J)$ maps to the same element $z+I+J$, then $x = y+i+j$, so $x - i = y + j$, and the pullback lies in the image of $\Delta : R \mapsto R/I \times R/J$. Now the kernel is just $I \cap J$. □

Prop. (5.1.1.25)[Filtered Colimits of Modules are Exact]. If $R \in \mathcal{R}\text{ing}$ and $\mathcal{I}$ be an index category that each connected components of $\mathcal{I}$ is filtered, then taking colimits over $\mathcal{I}$ is exact in the category $\mathcal{M}\text{od}_R$. ⌟

Proof: It is clearly right exact. To check left exactness, Cf.[Sta]04B0.**?** □

Cor. (5.1.1.26) [Filtered Colimits of Abelian Groups are Exact]. Filtered colimits are exact in $\mathcal{A}\text{b}$. ⌟

Prop. (5.1.1.27). Let k be a field and A, B be k-algebras and let $\mathfrak{b} \subset A \otimes_k B$ be an ideal. Then among the ideals $\mathfrak{a} \subset A$ that $\mathfrak{b} \subset \mathfrak{a} \otimes_k B$, there exists a smallest one. ⌟

Proof: Choose a k-basis of B, then the smallest ideal $\mathfrak{a}$ is just the ideal generated by all the A-coefficients of elements of $\mathfrak{b}$. □

Localization

Def. (5.1.1.28) [Localization as Filtered Colimit]. Let A be a commutative ring and S be a multiplicatively closed subset of A containing 1 and not containing 0, the localization $S^{-1}A$ is defined to be a ring over A that any ring map $A \to B$ that maps elements of S to units factors through $S^{-1}A$.

$S^{-1}A$ can be constructed as

$$\varinjlim_{s \in S} A$$

where the ordering is defined to be $s < t$ if $t = sr$ for some $r \in S$, and if $t = sr$, there is a map from A_s to A_t defined by multiplying by r. This is easily seen to be a filtered colimit. There is easily seen to be the localization. ⌟

Prop. (5.1.1.29) [Localization is exact]. S^{-1} is an exact functor from $\mathcal{M}\text{od}_R$ to $\mathcal{M}\text{od}_R$. Because it is a filtered colimit(4.8.3.28)(5.1.1.25). ⌟

Cor. (5.1.1.30). $(R/I)_{\bar{P}} \cong R_P/IR_P$, in particular, $k(R/P) \cong R_P/PR_P$. ⌟

Def. (5.1.1.31) [Total Ring of Fractions]. For any ring R, the set of non-zerodivisors in R is a multiplicatively closed set S, and the localization $Frac(R) = S^{-1}R$ is called the **total ring of fractions** of R. ⌟

Prop. (5.1.1.32) [Localization Along an Ideal]. Let I be an ideal of A, then the localization of A along I is the ring $\widetilde{A}$ that $\operatorname{Spec}\widetilde{A}$ is the localization of $\operatorname{Spec} A$ along $V(I)$ as defined in(4.12.4.20)(because $\operatorname{Spec} A$ is spectral, by(4.12.4.13)).

Equivalently, it can be defined as $\widetilde{A} = S^{-1}A$, where $S = A\backslash(\cup_{\mathfrak{p}\in V(I)}\mathfrak{p})$. (It can be checked that S is multiplicatively closed).

Notice then $I \subset \operatorname{rad}\widetilde{A}$.

For $f \in A$, we call the localization of A along f the **f-localization** of A. In fact, it is the universal A-algebra that $f \in \operatorname{rad}\widetilde{A}$. ⌟

Prop. (5.1.1.33). Let R be a commutative ring, $f_1, \ldots, f_n \in R$, and M an R-module, then $M \to \oplus_i M_{f_i}$ is injective iff $M \to \oplus_i M : m \mapsto (mf_1, \ldots, mf_n)$ is injective. ⌟

Proof: Cf.[Sta]0565. □

Prop. (5.1.1.34). For any ring A, $A \to \prod A_{\mathfrak{m}}$ is injective, where $\mathfrak{m}$ are maximal ideals of A.

For a domain A, $A = \bigcap A_{\mathfrak{m}}$ inside the fraction field of A, where $\mathfrak{m}$ are maximal ideals of A. ⌟

Proof: if $g \in \mathrm{Frac}(A)$ is in the RHS, then $I = \{x \in A | xg \in A\}$ is an ideal of A not contained in any maximal ideal, thus $I = 1$(5.1.1.7), and thus $g \in A$. □

Lemma (5.1.1.35). Let R be a ring and $\mathfrak{p}$ be a prime, then there exists an $f \in R, f \notin \mathfrak{p}$ that $R_f \subset R_{\mathfrak{p}}$, if any of the following holds:

- R is a domain.
- R is Noetherian.
- R is reduced and has f.m. irreducible components.

⌟

Proof: Cf.[Sta]0BX1. □

Def. (5.1.1.36) [Identifying Local Rings]. A ring map $A \to B$ is said to **identify local rings** if for every prime $\mathfrak{q} \subset B$, the map $A_{\varphi^{-1}(\mathfrak{q})} \to B_{\mathfrak{q}}$ is an isomorphism. ⌟

Prop. (5.1.1.37). The property of identifying local rings is stable under base change and composition. (This is immediate from(5.1.1.38)). ⌟

Prop. (5.1.1.38) [Tensor Product and Localization]. For a ring map $R \to S$, let $q \subset \mathrm{Spec}\, S$, $p = q \cap R$, then $(M \otimes_R S)_q = M_p \otimes_{R_p} S_q$ for any R-module M. ⌟

Proof: $(M \otimes_R S)_q = M \otimes_R S_q = M \otimes_R R_p \otimes_{R_p} S_q = M_p \otimes_{R_p} S_q$. □

Noetherian

Def. (5.1.1.39) [Noetherian Module]. Let R be a commutative ring and M an R-module, then M is called **Noetherian** iff every ascending chain of submodules stablizes.

R is called a **Noetherian ring** iff R is Noetherian over itself. ⌟

Prop. (5.1.1.40). Let $R \in \mathcal{CR}\mathrm{ing}$ and $0 \to M_1 \to M \to M_2$ be an exact sequence in $\mathcal{M}\mathrm{od}_R$, then M is Noetherian iff M_1, M_2 are both Noetherian. ⌟

Prop. (5.1.1.41)[Hilbert Basis Theorem, Hilbert1888]. Let A be a Noetherian ring, then quotient ring, f.g. module, f.g. algebra, localization and power series of A are Noetherian. Hence graded algebra of a Noetherian ring A by an ideal I is Noetherian. Products of Noetherian rings are Noetherian. ⌟

Proof: Only need to prove $A[X]$ and $A[[X]]$, localization and others are quotients of these. For an ascending chain of ideal I_j of $A[X]$, we consider the coefficients ideal $I_{i,j}$ of X^i of I_j, then there are only f.m. different $I_{i,j}$s, so we have I_j stabilize as well.

Similarly for $A[[X]]$, we prove any ideal I is f.g. Consider the lowest terms coefficient ideal at degree i, then it is ascending and stabilize, then a set of generators as a whole generate I. □

Remark (5.1.1.42). The subring of a Noetherian ring is NOT necessarily Noetherian, by the example of $k[X_1, \ldots, X_n, \ldots] \subset k(X_1, \ldots, X_n, \ldots)$. ⌟

Prop. (5.1.1.43). When A is Noetherian and is quipped with I-adic topology, then I is f.g., and there is a surjective ring map $A[[X]] \to A^\wedge$, mapping to the generators of I, hence the completion is Noetherian. (It is surjective can be seen by the Cauchy sequence construction of completion). ⌟

Prop. (5.1.1.44). If $R \to R'$ is ring map of f.t., then if $S \in \mathcal{CR}\mathrm{ing}\,/R$ and S is Noetherian, then $S \otimes_R R'$ is Noetherian, because $S \times_R R'$ is of f.t. over S, and use(5.1.1.41). ⌟

Cor. (5.1.1.45). For $k \in \texttt{Field}$, $S \in \mathcal{CR}\text{ing}/k$, then for any f.g. field extension K/k, $S \otimes_k K$ is Noetherian. (Because there is a f.g. algebra B over k that K is the localization of B, and use(5.1.1.41)). ⌟

Prop. (5.1.1.46). If R is Noetherian and M is a f.g. R-module, then there is a filtration $\{M_i\}$ of M that the quotients are all isomorphic to $R_{\mathfrak{p}_i}$ where $\mathfrak{p}_i$ are primes. ⌟

Proof: M is generated by x_i, so $(x_1) \cong R/I_i$, and so we modulo x_i, then the result follows by induction. So we may assume $M = R/I$. We use Noetherian condition to choose a maximal element J that is a counterexample, then J is not a prime, so there are $a, b \notin J$ that $ab \in J$. Then we have a filtration $0 \subset aR/(J \cap aR) \subset R/J$. Notice $R/(J + bR) \to aR/(J \cap aR) \to 0$, and the second quotient is $R/(J + aR)$, so they all can be factorized. □

Prop. (5.1.1.47). A Noetherian ring has only f.m. minimal prime ideals. ⌟

Proof: This is a consequence of(6.4.1.20)(6.4.1.21) and(4.12.3.4). □

Prop. (5.1.1.48) [Cohen]. If $R \in \mathcal{CR}\text{ing}$ and every prime ideal is f.g., then R is Noetherian. ⌟

Proof: Suppose P is not Noetherian. Firstly the set of non-finitely generated ideals has the chain property: if I_i is a chain of non-f.g. ideals of R, then $I = \cup_{i\in\Phi} I_i$ is non-f.g., otherwise there are $(f_i) = I$, but $\{f_i\} \in I_h$ for some h, thus I_h is f.g.. Then we use the Zorn's lemma to find a maximal non-f.g. ideal I. We show that I is a prime ideal:

$I \neq R$ because $R = (1)$. So if $a, b \in R\backslash I$ that $ab \in I$, then $I + (a)$ and $I + (b)$ is f.g. by $p_i + r_i a$, by maximality, and let $K = (P : a)$, then $I \subset I + (b) \subset K$, thus K is f.g., so does aK.

Now I claim $I = (p_1) + \ldots + (p_n) + aK$: one direction is clear, and if $r \in I \subset I + (a)$, then $r = \sum c_i(p_i + r_i a)$, thus $(\sum c_i r_i)a = r - \sum c_i p_i \in I$, thus $\sum c_i r_i \in K$, thus $r = \sum c_i p_i + (\sum c_i r_i)a \in (p_1) + \ldots + (p_n) + aK$.

So now I is f.g., contradiction, which shows I is a prime, but this contradicts the hypothesis. □

Prop. (5.1.1.49) [Modules over Noetherian Ring are Noetherian]. Let R be a Noetherian ring, then any submodule of a finite module M over R is finite. Thus any module over R is a Noetherian module(5.1.1.39). In particular, any module over R is of f.p. ⌟

Proof: it suffices to prove the first assertion: we use induction on the minimal number of generators of M: if it is generated by 1 element, then $M \cong R/I$ for some ideal I, thus $N \subset M$ is isomorphic to some J/I, so it is finite because J is finite. If the minimal number of generators of M is greater than 1, then there exists an exact sequence

$$0 \to M' \to M \to M'' \to 0$$

where M', M'' has fewer number of generators. Now there is also an exact sequence

$$0 \to N \cap M' \to N \to \overline{N} \to 0,$$

and the minimal number of generators of N is smaller than the sum of that of M' and M'', thus it is also finite. □

Prop. (5.1.1.50) [Artin-Tate]. Let R be a Noetherian ring and S a f.g. R-algebra. If $T \subset S$ is an R-subalgebra that S is a finite module over T, then T is f.g. over R. ⌟

Proof: Cf.[Sta]00IS. □

Prop. (5.1.1.51) [Krull-Akizuki]. If R is a Noetherian domain of dimension 1 with fraction field K, L/K a finite extension of fields, then for any ring A s.t. $R \subset A \subset L$, A is Noetherian. ⌟

Proof: Cf.[Sta]00PG. □

2 Lengths

Def. (5.1.2.1) [Lengths]. The **length** of a R-module M is the supremum of lengths of chains of submodules of M, denoted by $\mathrm{length}_R(M)$. ⌟

Prop. (5.1.2.2). Length is an additive function on $\mathcal{M}\mathrm{od}_R$. ⌟

Proof: Cf.[Sta]00IV. □

Prop. (5.1.2.3). If $\mathrm{length}_R(M) < \infty$, then any maximal chain of submodules has the same length. ⌟

Proof: Let $l(M)$ be the minimal length of a maximal chain, then if $M \subsetneq N$, then firstly $l(M) < l(N)$, because a maximal chain of M restricts to a maximal chain of N, and if the length is the same, then each term is in M, so $N \subset N$, contradiction. Now any chain has length $l(M)$, because if there is a chain M_i, then $l(M_0) < l(M_1) < \ldots < l(M)$. □

Prop. (5.1.2.4). Let $R \in \mathcal{CR}\mathrm{ing}$ and S a multiplicative set of R, then $\mathrm{length}_R(M) \geq \mathrm{length}_{S^{-1}R}(S^{-1}M)$. ⌟

Proof: This is because any $S^{-1}R$-submodule of $S^{-1}M$ is of the form $S^{-1}N$ where N is a R-submodule of M. □

Prop. (5.1.2.5). If R is a ring with a maximal ideal $\mathfrak{m}$, M is an R-module that $\mathfrak{m}M = 0$, then $\mathrm{length}_R(M) = \dim_{k(\mathfrak{m})}(M)$. ⌟

Prop. (5.1.2.6) [Length over a Local Ring]. Let $(R, \mathfrak{m})$ be a local ring, and $M \in \mathcal{M}\mathrm{od}_R$ is of finite length, then $\mathfrak{m}^n M = 0$ for some $n \in \mathbb{N}$.

Conversely, if $\mathfrak{m}$ is f.g. and M is a finite R-module, and $\mathfrak{m}^n M = 0$ for some $n \in \mathbb{N}$, then $\mathrm{length}_R(M) < \infty$. ⌟

Proof: M is clearly a finite module over R. Take $n = \mathrm{length}_R(M)$. If $f_1, \ldots, f_n \in \mathfrak{m}$ and $x \in M$ s.t. $f_1 \ldots f_n x \neq 0$, then by Nakayama the submodules

$$0 \subset (f_1 \ldots f_n)x \subset (f_2 \ldots f_n)x \subset (f_n)x \subset M$$

are all different, so $\mathrm{length}_R(M) \geq n$, contradiction.

For the converse, use additivity on the filtration $0 = \mathfrak{m}^m M \subset \mathfrak{m}^{n-1} M \subset \ldots \subset M$, where each quotient is finite over R and annihilated by $\mathfrak{m}$, so we conclude by(5.1.2.5). □

Prop. (5.1.2.7). If $(A, \mathfrak{m})$ is a local ring and B is a ring over A with f.m. maximal ideals $\mathfrak{m}_i$ s.t. each $\mathfrak{m}_i$ is over $\mathfrak{m}$ and $k(\mathfrak{m}_i)/k(\mathfrak{m})$ is finite, then there for any $M \in \mathcal{M}\mathrm{od}_B$ with $\mathrm{length}_B M < \infty$,

$$\mathrm{length}_A M = \sum_i [k(\mathfrak{m}_i) : k(\mathfrak{m})] \,\mathrm{length}_{B_{\mathfrak{m}_i}} M_{\mathfrak{m}_i}.$$

⌟

Prop. (5.1.2.8). Let $A \to B$ be a flat local maps of local rings, then for any $M \in \mathcal{M}\mathrm{od}_A$,

$$\mathrm{length}_A(M)\,\mathrm{length}_B(B/\mathfrak{m}_A B) = \mathrm{length}_B(M \otimes_A B).$$

⌟

Proof: Cf.[Sta]02M1.? □

Cor. (5.1.2.9). Let $A \to B \to C$ be local maps of local rings, C/B is flat, and $\mathfrak{m}_A$ the maximal ring of A, then

$$\text{length}_B(B/\mathfrak{m}_A B)\,\text{length}_C(\mathfrak{m}_B C) = \text{length}_C(C/\mathfrak{m}_B C).$$

⌟

Prop. (5.1.2.10) [Order of Vanishing]. If R is a semi-local Noetherian domain of dimension 1 and a, b are not zero-divisors, then $f(a) = \text{length}(R/(a))$ satisfies $f(a) + f(b) = f(ab) < \infty$.

So this $R \subset K$ and has fraction field K, then f extends to an additive function on K^*, denoted by $\text{ord}_R(f)$. ⌟

Proof: It is finite by[Sta]00PF. It is additive because length is additive(5.1.2.1) and $0 \to R/(a) \to R(ab) \to R(b) \to 0$. □

3 Artinian Ring

Def. (5.1.3.1) [Artinian Rings]. A ring A is called **Artinian** if any descending chain of ideals of A stablizes.

For example, a f.g. k-algebra that is a finite k-module is an Artinian ring. ⌟

Lemma (5.1.3.2). Let A be an Artinian ring, then A has f.m. maximal ideals. ⌟

Proof: Consider $\mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \ldots \supset$, then it is a descending chain, by Chinese remainder theorem. So it has f.m. maximal ideals. □

Lemma (5.1.3.3). If A is an Artinian ring, then the Jacobson radical is nilpotent. ⌟

Proof: Consider the Jacobson radical I, $I^n = I^{n+1}$ for some n, let $J = \text{Ann}(I^n)$, it suffices to show $J = A$. If not, choose a minimal J' that contains J but not J(exists by Artinian property), then $J' = J + Ax$, and $IJ' \subset J$ by Nakayama, so $xI^{n+1} \subset JI^n = 0$, so $x \in J$, contradiction. □

Prop. (5.1.3.4) [Characterization of Artinian Rings]. The following are equivalent:

1. A is Artinian.
2. A is Noetherian of dimension 0.
3. $\text{length}_A A < \infty$.
4. A is a finite product of local Artinian rings.
5. A is Noetherian, Jacobson(5.2.6.4), and has f.m. maximal ideals.

⌟

Proof: $1 \iff 3$: if $\text{length}_A A < \infty$, then A is clearly Artinian. Conversely, if A is Artinian, then by(5.1.3.2)(5.1.3.3)(5.2.6.7) A a finite product of its localization of maximal ideals, so we may assume A is local with maximal ideal $\mathfrak{m}$. Then $\mathfrak{m}^n = 0$ for some n by(5.1.3.3), and $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ has length the same as their dimension as a $A/\mathfrak{m}$ vector space, by(5.1.2.5), which is finite because A is Artinian, so $\text{length}_A A < \infty$.

$1 + 3 \to 5$: A has f.m. maximal ideals by(5.1.3.2). It is Jacobson by(5.1.3.3). $\text{length}_A A < \infty$ clearly implies A is Noetherian.

$5 \to 2$: By(5.2.6.7).

$2 \to 5$: all prime ideals are maximal, so $\text{Spec}\, A$ is discrete, so A has f.m. maximal ideals, and it is clearly Jacobson.

$5 \to 3$: By(5.2.6.7), R is a product of its local rings, and the local rings are all Noetherian and Jacobson(5.2.6.6), so by Nakayama, they have finite lengths. So also R has finite length.

$5 \to 4$: By lemma(5.2.6.7) below, A is a product of its localization, and its localizations also satisfies 5, and by $5 \to 3 \to 1$, they both have descending conditions.

$4 \to 5$: An Artinian ring is Noetherian and Jacobson by $1 + 3 \to 5$, then so does their product. □

Cor. (5.1.3.5) [Reduced Artinian Ring]. A reduced local Artinian ring is a field. In particular, A reduced Artinian ring is a product of fields. ⌟

Proof: An Artinian local ring A is Jacobson(5.1.3.4) so the maximal ideal $\mathfrak{m} = 0$ as A is reduced. □

Prop. (5.1.3.6). For an Artinian local ring A, the following are equivalent:

1. A is a PID.
2. the maximal ideal $\mathfrak{m}$ is principal.
3. $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.

⌟

Proof: It suffices to prove $3 \to 1$: If $\mathfrak{m} = \mathfrak{m}^2$, then $\mathfrak{m} = 0$ by Nakayama, so A is a field. If $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$, then $\mathfrak{m}$ is principle by Nakayama. And $\mathfrak{m}$ is nilpotent by(5.1.3.4), so for any ideal a there is a minimal n that $a \subset \mathfrak{m}^n$. Now choose $y \in a - \mathfrak{m}^{n+1}$, then $y = ux^r$, and $u \notin (x)$, so u is a unit, thus $x^r \in a$, meaning $a = \mathfrak{m}^n$ hence principal. □

4 Local Properties

Def. (5.1.4.1) [Local properties]. A property P of rings or modules over a ring is called **local property** iff X has P iff X_{f_i} all has P for a covering $(f_1, \ldots, f_n) = 1$.

A property of morphisms of rings is called **local on the target** iff $R \to S$ has P iff $R_{f_i} \to S_{f_i}$ has P for a covering $(f_1, \ldots, f_n) = 1$ in R. ⌟

Prop. (5.1.4.2) [Stalkwise Properties]. For a commutative ring R, a property P is called stalkwise if A satisfies P iff all $A_\mathfrak{m}$ satisfies P where $\mathfrak{m}$ are maximal ideals, and iff all $A_\mathfrak{p}$ satisfies P where $\mathfrak{p}$ are prime ideals of A.

1. Trivial is stalkwise for modules over R. Hence so does injectivity and surjectivity because localization is exact.
2. Torsion-free is stalkwise for modules over R if R is integral.
3. Flatness for modules over R.
4. Flatness for rings over R on the source.
5. Formal unramifiedness for rings over R, both on the target and source.
6. (universally)catenary is stalkwise.
7. reducedness is stalkwise.
8. Integral+integrally closed is stalkwise.
9. normal is stalkwise.
10. regular is stalkwise.

⌟

Proof:

1. It suffice to prove an element is trivial on every localization then it is 0. For this, consider the annihilator $\mathrm{Ann}(x)$, it is not contained in any maximal ideal so it contains 1.
2. if $xf = 0$ but $f \neq 0$, then $x \in Ann(f) \neq (1)$, so $Ann(f) \subset \mathfrak{m}$ maximal, so f is torsion in $M_{\mathfrak{m}}$ over $R_{\mathfrak{m}}$. Conversely, if f is torsion in $R_{\mathfrak{m}}$, then it is clearly torsion over R.
3. We use the definition(5.4.1.2). Notice $(IM)_{\mathfrak{p}} = I_{\mathfrak{p}}M_{\mathfrak{q}}$ and every ideal of $R_{\mathfrak{p}}$ is of the form $I_{\mathfrak{p}}$. Then use the fact injective is stalkwise(5.1.4.2).
4. We use the definition(5.4.1.2). Notice $(I \otimes_R S)_{\mathfrak{q}} = I_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} S_{\mathfrak{q}}$ for all primes $\mathfrak{q}$ of S and $\mathfrak{p} = \mathfrak{q} \cap R$. And every ideal of $R_{\mathfrak{p}}$ is of the form $I_{\mathfrak{p}}$. Then use the fact injective is stalkwise(5.1.4.2)
5. Because formally unramified is equivalent to $\Omega_{R/S} = 0$(5.4.6.1), so we get the result by functorial properties of $\Omega_{S/R}$(5.4.3.6) and triviality is stalkwise(5.1.4.2).
6. For any two prime ideals $\mathfrak{p} \subset \mathfrak{q}$, we can choose a maximal ideal containing them.
7. use(5.1.1.34).
8. If A is integrally closed, then clearly any localization of A is integrally closed. Conversely, if $r \in K(A)$ is integral over A but $r \notin A$, let $I = \{s \in A | rs \in A\}$, then $I \neq A$, so $I \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, then $r \notin A_{\mathfrak{m}}$, so $A_{\mathfrak{m}}$ is not integrally closed, contradiction.
9. By definition.
10. By definition.

□

Remark (5.1.4.3). Our main technique of proving local properties are using affine communication theorem(6.4.1.2). ⌟

Prop. (5.1.4.4) [Local Properties]. For a fixed ring R,

1. Every property that is stalkwise is a local property.(5.1.4.2) The properties listed below should be not stalkwise.
2. Every property that satisfies faithfully flat descent is a local property. The properties listed below should not satisfy faithfully flat descent.
3. Noetherian.
4. F.t. ring maps on the source.
5. F.p. ring maps on the source.
6. N-1 and N-2 and universally Japanese for rings.
7. Nagata for rings.

⌟

Proof:

1.
2.
3. If A is Noetherian, then A_{f_i} are Noetherian by(5.1.1.41). Conversely, if A_{f_i} are all Noetherian and $I_1 \subset I_2 \subset \ldots$ is an ascending chain of ideals of A, consider $A \to \prod A_{f_i}$ faithfully flat, thus

$I_1 \otimes_A (\prod A_{f_i}) \subset I_2 \otimes_A (\prod A_{f_i}) \subset \ldots$ is an ascending chain of $\prod A_{f_i}$. Now $\prod A_{f_i}$ are Noetherian by(5.1.1.41), so this chain stabilizes. But this ring map is faithfully flat, so the original chain must also stablizes.

4. Let $(g_1, \ldots, g_n) = 1$, choose $\sum h_i g_i = 1$, and let $x_{ij} = y_{ij}/g_i^{n_{ij}}$ generates S_{g_i}. Now let S' be the sub-R-algebra of S generated by y_{ij}, g_i, h_j. Then $(S')_{f_i} \to S_{f_i}$ is surjective for any i, so $S' \to S$ is also surjective, by(5.1.4.2). Then $S' = S$, and S is f.g. over R.
5. Cf.[Sta]00EP.
6. If A is N-1, then A_{f_i} are N-1 because taking integral closure commutes with localization. The same for N-2. Conversely, if all A_{f_i} are N-1 or N-2, so is A because finiteness is local(5.1.4.4). The universal Japanese case follows from the N-2 case.
7. This follows from the localness of Noetherian and N-2(5.1.4.4).

□

5 Miscellaneous

Fitting Ideals

Def. (5.1.5.1)[Fitting Ideals]. Let $R \in \mathcal{CR}\mathrm{ing}$ and M be a finite R-module, then for any presentation

$$\oplus_{j \in J} R \to R^{\oplus n} \to M \to 0$$

given by a $n \times J$ matrix A, the ideal generated by the $(n-k) \times (n-k)$ matrices of A is independent of the presentation chosen, called the k-th **Fitting ideal of** A, denoted by $\mathrm{Fit}_k(M)$. ⌟

6 Rings and Categories

Quotient by Equivalence Relations

Prop. (5.1.6.1) [Quotients by Equivalence Relations]. Let $u_0, u_1 : A_0 \to A_1$ be an equivalence in the dual category of $\mathcal{CR}\mathrm{ing}_{R_0}$(4.1.1.23). If u_0 is locally free of constant rank r, then a quotient $u : A \to A_0$ exists, and u is locally free of constant rank r. ⌟

Proof: Cf.[Mil17b]P592. □

Morita Equivalence

Basic References are [Morita Equivalence] and [Fuller Rings and Categories of Modules].

Def. (5.1.6.2). Two ring R, S are called **Morita equivalent** if the category of mod-R is equivalent to the category of mod-S. ⌟

Prop. (5.1.6.3). For an Abelian category $\mathcal{A}$ satisfying AB3 (i.e arbitrary sum exists), An object P of $\mathcal{A}$ is a **progenerator** if the functor $h' : X \mapsto \mathrm{Hom}_{\mathcal{A}}(P, X)$ is exact and and strict: $h'(X) = 0$ implies $X = 0$. Then h' determines an equivalence from $\mathcal{A}$ to mod-R, where $R = \mathrm{Hom}_{\mathcal{A}}(P, P)$.

Similarly, if $\mathcal{A}$ is an Abelian Noetherian category and P is a progenerator, then R is Noetherian and $\mathcal{A}$ is equivalent to the category of finitely generated R-categories. ⌟

Proof: Essentially surjective: construct using direct limit and cokernel.

Notice that $h'(X) \cong h'(X') \to X \cong X'$ by strictness and A4 axiom. So let $X = \mathrm{Coker}(P^{\oplus I}, P^{\oplus J})$,

$$\begin{aligned}\mathrm{Hom}(h'(X), h'(Y)) &= \mathrm{Hom}(\mathrm{Coker}(h'(P^{\oplus J}), h'(P^{\oplus I})), h'(Y)) \\ &= \ker(\mathrm{Hom}(h'(P^{\oplus J}), h'(Y)) \to \mathrm{Hom}(h'(P^{\oplus I}), h'(Y))) \\ &= \ker(h'(Y^{\Pi I}) \to h'(Y^{\Pi J})) \\ &= \mathrm{Hom}(X, Y)\end{aligned}$$

□

Prop. (5.1.6.4). In the case when A is the category mod-R, P is a generator $\iff$ $h' : X \mapsto \mathrm{Hom}_R(P, X)$ is faithful $\iff$ every M is a quotient of direct sums of P. And a **progenerator** is a f.g. projective generator. ⌟

Prop. (5.1.6.5). Let P be a (A, B)-bimodule, iff P is a progenerator as a right B module, then it is a progenerator as a left A module. ⌟

Prop. (5.1.6.6). Let P be a progenrator as a ⌟

Prop. (5.1.6.7) [Morita]. The following are equivalent:

- categories A-mod and B-mod are equivalent.
- categories mod-A and mod-B are equivalent.
- There exist a finitely generated progenerator P of mod-A that $B \cong \mathrm{End}_A P$.

⌟

Proof: $2 \to 3$:A is a progenerator in mod-A, thus when $A \sim B$, F : mod-$A \to$ mod-B, $A \cong \mathrm{End}_A A = \mathrm{End}_B F(A)$, and $F(A)$ is a left A module as well as a progenerator of B. Thus there is a (A, B)-bimodule P that $A \cong \mathrm{End}_B P$, and a (B, A)-bimodule Q that $B \cong \mathrm{End}_A Q$. □

Prop. (5.1.6.8). There can be defined another Morita invariance that $R \sim S$ iff there are (R, S)-bimodule P and (S, R)-bimodule Q that $P \otimes_S Q \cong R$ as a (R, R)-bimodule and $Q \otimes_R P \cong S$ as a (S, S)-bimodule. This will immediately generate equivalence between R-mod and S-mod as well as equivalence between mod-R and mod-S by tensoring. And P and Q are projective modules respectively, because equivalence is a kind of adjoint. ⌟

Prop. (5.1.6.9). Let D be a division ring over k of finite degree and $A = M_r(D)$. Let $S = D^r$ with A acting by left multiplication and D acting by right multiplication, then there S is a simple A-module, and every A-module is a direct sum of copies of S. This means that $S \otimes_D -$ induces an equivalence from $\mathcal{M}\mathrm{od}_D$ to $\mathcal{M}\mathrm{od}_A$. ⌟

Prop. (5.1.6.10) [Properties Preserved under Morita Invariance]. Cf.[Rings and Categories of Modules P54]. ⌟

7 Spectra

Lemma (5.1.7.1). In $\mathrm{Spec}\, A$, a subset U is retrocompact iff it is quasi-compact iff it is a finite union of standard opens $D(f_i)$. In particular, any constructible subset of $\mathrm{Spec}\, A$ is a finite union of morphisms of the form $D(f_i) \cap V(g_1, \ldots, g_m)$. ⌟

Proof: Retrocompact is quasi-compact because $\operatorname{Spec} A$ is quasi-compact. A quasi-compact subset is equivalent to a finite union of $D(f_i)$. Now for any quasi-compact subset $V = \cup_j D(g_j)$, $U \cap V = \cup_{ij} D(f_i g_j)$ is also quasi-compact, so $\cup_i D(f_i)$ is retrocompact. □

Lemma (5.1.7.2). Let R be a ring, then

- the image of any standard open subsets of $\operatorname{Spec} R[X]$ is qc open in $\operatorname{Spec} R$.
- for $g, f \in R[X]$ with g monic, the image of $D(f) \cap V(g)$ is qc open in $\operatorname{Spec} R$.

⌟

Proof: 1: For any prime $\mathfrak{p}$ of R, the primes mapping to $\mathfrak{p}$ has a minimal one, $\mathfrak{p}[X]$, so $\mathfrak{p}$ is in the image of $\operatorname{Spec} R[X] \to \operatorname{Spec} R$ iff $f \in \mathfrak{p}[X]$, which means the image is $D(a_0, a_1, \ldots, a_n)$, where $f = a_0 + a_1 X + \ldots + a_n X^n$.

2: $R[X]/g$ is finite free over R, let $P(T) = T^d + r_{d-1} T^{d-1} + \ldots + r_0$ be the characteristic polynomial of f acting on $R[X]/g$ by left multiplication, then $\mathfrak{p} \in V(r_0, \ldots, r_{d-1})$ iff f acts nilpotently on $R[X]/g \otimes_R k(\mathfrak{p})$, which is equivalent to $\mathfrak{p}$ being in the image of $D(f) \cap V(g)$(by base change to $k(\mathfrak{p})$ argument). □

Lemma (5.1.7.3) [Affine Chevalley]. The Spec map of a f.p. ring map maps constructible sets to constructible sets. ⌟

Proof: Suppose $S = R[X_1, \ldots, X_n](f_1, \ldots, f_m)$, then it suffices to show for the case $S = R/(f_1, \ldots, f_m)$ and $S = R[X]$.

If $S = R/(f_1, \ldots, f_m) = R/I$, it suffices to show the image of $D(\overline{g}) \cap V(\overline{h}_1, \ldots, \overline{h}_m)$ is retrocompact in $\operatorname{Spec} R$: in fact its image is just $D(g) \cap V(h_1, \ldots, h_m) \cap V(I)$, where g, h_i are any inverse images in R.

For the second case, we first prove some localizing result: If $S = R_f$, then the compact open subsets of $\operatorname{Spec} S$ are compact open subsets of $\operatorname{Spec} R$, so $\operatorname{Spec} S \to \operatorname{Spec} R$ maps constructible sets to constructible sets. Now for any $c \in R$, $\operatorname{Spec} R = \operatorname{Spec} R/c \coprod \operatorname{Spec} R_c$, so to prove the proposition for R, it suffices to prove for R_c and R/c.

Let $D(f) \cap V(g_1, \ldots, g_n) \subset \operatorname{Spec} R[X]$, where f, g_i are polynomials, We can use induction on the degree series $\deg(g_1) \le \deg(g_2) \le \ldots \le \deg(g_n)$. If the leading coefficient of g_1 is invertible, then we can use reduction to R/c and R_c to either reduces the degree of g_1 or reduce to the case it is invertible. If it is invertible, then we can use Euclidean division. Eventually, it can be reduced to the case $D(f) \cap V(g)$ where g is monic, or $D(f)$. This is proved in the above lemma(5.1.7.2). □

Lemma (5.1.7.4). For a Noetherian local ring $(A, \mathfrak{m})$, $\operatorname{Spec} A - \mathfrak{m}$ is affine iff $\dim A \le 1$. ⌟

Proof: if $\dim A = 0$, this is true, if $\dim A = 1$, let $f \in m$ not in any other minimal primes of A, then $\operatorname{Spec} A - m = \operatorname{Spec} A_f$.

Conversely, Cf.[[Sta]0BCR]. □

Idempotents

Prop. (5.1.7.5) [Clopen Subsets]. The clopen subsets of $\operatorname{Spec} A$ corresponds to idempotents in A. ⌟

Proof: This is all equivalent to the fact that there exists $e + f = 1, ef = 0$:

If $A = U \coprod V$, then both U, V are closed hence qc, so $\operatorname{Spec} A = \cup V(f_i) \coprod \cup V(g_j)$, then $f_i g_j$ is nilpotent by(5.2.6.2). Denote $I = (f_i), J = (g_j)$, then $(IJ)^N = 0$ and $I + J = A$, there are $1 = x + y$, $x \in I^N, y \in J^N$.

For uniqueness, if $e_1 \ne e_2$, then $0 \ne e_1 - e_2 = e_1(e_2 + f_2) - e_2(e_1 + f_1) = e_1 f_2 - e_2 f_1$, so may assume $e_1 f_2 \ne 0$, and it is not nilpotent, so there is a $e_1 f_2 \subset \mathfrak{p}$, which is a contradiction. □

Cor. (5.1.7.6). A local ring has no non-trivial idempotents, and then an idempotent is defined by the maximal ideals that it vanishes. ⌟

Cor. (5.1.7.7). If I is an ideal of R that $I = I^2$, and I is f.g., then $V(I)$ is open and closed in $\operatorname{Spec} R$, and $V(I) = R_e$ for some idempotent e. ⌟

Proof: By Nakayama, there is a a $f = 1 - e$ with $e \in I$ that $fI = 0$. So $e - e^2 = 0$ and $f^2 = f$. $V(I) = D(f) = D(e)$. □

Lemma (5.1.7.8). If I is a locally nilpotent ideal, then $R \to R/I$ induces a bijection on idempotents. ⌟

Proof: Because $R \to R/I$ induces a homeomorphism on the spectra, and clopen subsets of the spectrum corresponds to the idempotents(5.1.7.5). □

Lemma (5.1.7.9). Let R be a ring and $T \subset \operatorname{Spec} R$ is a set. Then the following are equivalent:

- T is closed and is a union of connected components of $\operatorname{Spec} R$.
- T is an intersection of clopen subsets.
- $T = V(I)$ where I is generated by idempotents.

⌟

Proof: 1 and 2 are equivalent by(4.12.4.3), and $2 \to 3 \to 1$ are easy. □

Prop. (5.1.7.10). Let R be a ring, then any connected component of $\operatorname{Spec} R$ is of the form $V(I)$, where I is an ideal generated by idempotents that any idempotent of R maps to either 0 or 1 in R/I. ⌟

Proof: By(4.12.4.2) and(4.12.4.13), a connected component of $\operatorname{Spec} R$ is an intersection of clopen subsets, so it is of the form $V(I)$ where I is generated by idempotents. The last assertion is equivalent to $V(I)$ being connected. □

Going-up and down

Def. (5.1.7.11) [Going-up and Going Down]. Going-up and down for topological spaces is defined in(4.12.3.7). A ring map $R \to S$ is said to satisfy the going-up property iff its Spec map does, equivalently, for any prime ideal $\mathfrak{q} \subset S$ and prime ideal $\mathfrak{p} \subset \mathfrak{q} \cap R$, there exists a prime ideal $\mathfrak{q}' \subset \mathfrak{q}$ that $\mathfrak{q}' \cap R = \mathfrak{p}$.

It is said to satisfy the going-down property iff its Spec map does, equivalently, for any prime ideal $\mathfrak{q} \subset S$ and prime ideal $\mathfrak{q} \cap R \subset \mathfrak{p}$, there exists a prime ideal $\mathfrak{q} \subset \mathfrak{q}'$ that $\mathfrak{q}' \cap R = \mathfrak{p}$. ⌟

Prop. (5.1.7.12). Going-up and Going-down are stable under composition, trivially. ⌟

Prop. (5.1.7.13) [Integral Map satisfies Going-Up]. Integral ring map satisfies going-up(5.2.1.5). Flat ring map satisfies going-down(5.4.1.19). ⌟

Lemma (5.1.7.14). If the image of the Spec map of a ring map is closed under specialization, then this image is closed. ⌟

Proof: Let it be $R \to S$, let I be the kernel, then the image is contained in $V(I)$, so we may replace R be R/I, then $R \subset S$. Now we show the image contains all the minimal primes of R: for a minimal prime $\mathfrak{p}$, $A_\mathfrak{p} \subset B_\mathfrak{p}$, thus $B_\mathfrak{p}$ is not-empty, and thus has a maximal ideal, whose intersection with $A_\mathfrak{p}$ can only be $\mathfrak{p}$ by hypothesis, thus $\mathfrak{p}$ is in the image of Spec. Then the image is all of $\operatorname{Spec} R$ by hypothesis, thus closed. □

Cor. (5.1.7.15) [Going-up and Spec Closed]. Going-up is equivalent to Spec map closed. ⌟

Proof: If going-up holds, then Spec map is closed by(5.1.7.14). Conversely, a closed map satisfies going-up, by(4.12.3.8). □

Prop. (5.1.7.16). If $R \to S$ is a ring map that satisfies going-up, and $P \subset S$ is a maximal ideal, then $P \cap R$ is also a maximal ideal. ⌟

Prop. (5.1.7.17) [Krull]. If $A \subset B$ is an integral extension of integral domains, and A is normal, then going-down holds. ⌟

Proof: Let L_1, K be the fraction fields of B, A resp., and let L be the normal extension of K contained in L_1, C the integral closure of A in L. Let $P \in \operatorname{Spec} B$ and $\mathfrak{p} = P \cap A$, $\mathfrak{p}' \subset \mathfrak{p}$. Take a prime ideal $Q' \in \operatorname{Spec} C$ lying over p, and by going-up applied to $A \subset C$(5.1.7.13), there is a prime ideal Q_1 lying over $\mathfrak{p}$ that $Q' \subset Q_1$. Take $Q \in \operatorname{Spec} C$ lying over P, then by(5.3.5.12) there is a $\sigma \in G_{L/K}$ that $\sigma(Q_1) = Q$. Set $P' = \sigma(Q') \cap B$, then $P' \subset P$ is a prime of B lying over $\mathfrak{p}'$, so going-down holds for $A \subset B$. □

Prop. (5.1.7.18) [Going-down and Spec Open]. If Spec map is open, then going-down holds. ⌟

Proof: □

Minimal Primes and Irreducible Components

Prop. (5.1.7.19) [Minimal Primes Exists]. Every nonzero ring contains a minimal prime ideal. ⌟

Proof: Firstly prime ideal exists, by(5.1.1.6), and we use Zorn's lemma to find a minimal prime ideal: it suffices to show the intersection of a chain of prime ideals is a prime ideal, this is not hard. □

Lemma (5.1.7.20). If $\mathfrak{p}$ is a minimal prime of R, then $\mathfrak{p}R_{\mathfrak{p}}$ is locally nilpotent by(5.2.6.1). In particular, if R is reduced, then $R_{\mathfrak{p}}$ is a field. ⌟

Prop. (5.1.7.21) [Zerodivisors in a Reduced Ring]. Let R be a reduced ring, then

- $R \to \prod_{\mathfrak{p} \text{ minimal}} R_{\mathfrak{p}}$ is an embedding into a product of fields.
- $\cup_{\mathfrak{p} \text{ minimal}} \mathfrak{p}$ is the set of zerodivisors of R.

⌟

Proof: 1: By(5.1.7.20), $R_{\mathfrak{p}}$ are fields. In particular, the kernel of $R \to R_{\mathfrak{p}}$ is $\mathfrak{p}$. Then the kernel of the map $R \to \prod_{\mathfrak{p} \text{ minimal}} R_{\mathfrak{p}}$ is $\cap_{\mathfrak{p} \text{ minimal}} \mathfrak{p} = 0$ by(5.2.6.1).

2: If $xy = 0$ and $x \neq 0$, then $x \notin \mathfrak{p}$ for some minimal prime $\mathfrak{p}$ by(5.2.6.1), thus $y \in \mathfrak{p}$. Conversely, if $y \in \mathfrak{p}$ for some minimal prime p, then y is mapped to $0 \in R_{\mathfrak{p}}$, which means there are some $x \notin \mathfrak{p}$ that $xy = 0$. □

Prop. (5.1.7.22). If R is a ring with f.m. minimal primes $\mathfrak{q}_i$ and $\cup_i \mathfrak{q}_i$ is the set of zerodivisors of R, then the ring of fractions of R(5.1.1.31) is equal to $\prod_i R_{\mathfrak{q}_i}$. ⌟

Proof: Cf.[Sta]02LX. □

Prop. (5.1.7.23) [Irreducible Components of Spectrum]. The irreducible closed subsets of $\operatorname{Spec} R$ are exactly the sets of the form $V(\mathfrak{p})$ for some prime $\mathfrak{p} \subset R$. The irreducible components of $\operatorname{Spec} R$ are exactly the sets of the form $V(\mathfrak{p}_i)$ for some minimal prime $\mathfrak{p}_i$. ⌟

Prop. (5.1.7.24). If R be a ring and $\mathfrak{p}$ a minimal prime of R. If $W \subset \operatorname{Spec} R$ is a quasi-compact open subset of $\operatorname{Spec} R$ not containing $\mathfrak{p}$, then there exists some $f \in R$ that $\mathfrak{p} \subset D(f)$ and $D(f) \cap W = \varnothing$. ⌟

Proof: W is of the form $\cup_{i=1}^r D(f_i)$. As $\mathfrak{p} \notin D(f_i)$, $f_i \in \mathfrak{p}$ for each i. Then(5.1.7.20) says f_i are nilpotent in $R_\mathfrak{p}$, so there is some $g \in R$ that gf_i are nilpotent in R for any i, which means g satisfies the requirement. □

Prop. (5.1.7.25). For $R \subset S$, all the minimal primes of R are in the image of the Spec map of a minimal prime of S. ⌟

Proof: Localize w.r.t. to the minimal prime $\mathfrak{p}$, then it is a local ring with only one prime. And $S_\mathfrak{p}$ is nonzero because localization is exact, so it has a maximal ideal $\mathfrak{q}$. Now we choose a minimal prime of S contained in $\mathfrak{q}$, then it is also mapped to $\mathfrak{p}$. □

Universal Homeomorphism

Cf.[Sta]10.45 and [Sta]28.44.

Prop. (5.1.7.26). If $\varphi : R \to S$ is a ring map and p is a prime number that satisfies:

- S is generated over R by elements x that there is n that $x^{p^n} \in \varphi(R)$ and $p^n x \in \varphi(x)$.
- $\ker(\varphi)$ is locally nilpotent.

then $\operatorname{Spec} S \to \operatorname{Spec} R$ is a homeomorphism, and any base change of φ satisfies the above conditions, so it is a universal homeomorphism.

In particular, this applies to any base change of a field extension k'/k that is purely inseparable, because it is f.f. hence injective. ⌟

Proof: Cf.[Sta]0BRA. □

5.2 Commutative Algebra II

References are [Sta].

Notation (5.2.0.1).

- Use notations as in3.2.

⌟

1 Integral Extensions

Def. (5.2.1.1)[Totally Integrally Closed]. For two rings $A \to B$, $f \in B$ is called **almost integral**(or totally integral when almost mathematics is performed:)) over A if $f^{\mathbb{N}}$ lies in a f.g. A-module of B. It is clear that the elements of totally integral elements of B is a subring. And A is called **totally integrally closed** in B iff any $f \in B$ totally integral over A is in A. ⌟

Prop. (5.2.1.2). For a ring map $\varphi : A \to B$, an element x is integral over A iff x is contained in a finite A-module in B. In particular, the elements of B that are integral over A is a ring containing $\varphi(A)$. ⌟

Proof: If x is integral, then $\varphi(A)[x]$ is finite. If $\varphi(A)[x]$ is finite, then there is a set of generators of polynomials in x. Then for m large, $x^m = \sum a_i f_i(x)$, so x is integral over A. □

Prop. (5.2.1.3) [Integral Extension of Field]. For $A \subset B$, if B is integral over A, then A is a field iff B is a field. ⌟

Proof: If A is a field, $y^{-1} = -a_n^{-1}(y^{n-1} + \ldots + a_{n-1}) \in B$. If B is a field, $x^{-1} = -(b_1 + b_2 x + \ldots + b_m x^{m-1}) \in A$. □

Cor. (5.2.1.4). If B is integral over A, then a prime $\mathfrak{p} \subset B$ is maximal iff $\mathfrak{p} \cap A$ is maximal. ⌟

Proof: Look at the integral extension $A/(\mathfrak{p} \cap A) \to B/\mathfrak{p}$. □

Prop. (5.2.1.5) [Going-Up]. Let $A \to B$ integral. Then:

1. There is no inclusion relation between prime ideals of B lying over a fixed prime ideal of A.
2. if $A \subset B$, then thee Spec map is surjective. In particular, for any $\mathfrak{p} \subset A$, $\mathfrak{p}B \cap A = \mathfrak{p}$.
3. The going-up holds. In particular, the Spec map of an integral ring map is closed, by(5.1.7.15).

⌟

Proof:

1. If $p \cap A = p' \cap A = q$, Localize at q, then p, p' are both maximal ideals of B_q by(5.2.1.4), they cannot contain each other.
2. For any prime $\mathfrak{p}$ of A, since $A_\mathfrak{p} \subset B_\mathfrak{p}$, $B_\mathfrak{p} \neq 0$, so it has a maximal ideal(5.1.1.6), and use(5.2.1.4).
3. for any prime ideal $\mathfrak{q}$ of B and $\mathfrak{p} = \mathfrak{q} \cap A$, replace $A \to B$ by $A/\mathfrak{p} \subset B/\mathfrak{q}$, then we can use2.

□

2 Graded Rings

Cf.[Matsumura Ch11].

Def. (5.2.2.1) [Graded Rings]. A **graded ring** is a ring $A = \bigoplus_{n\in\mathbb{Z}} A_n$ that $A_m A_n \subset A_{m+n}$. A **graded module** over a graded ring A is a module $M = \bigoplus_{n\in\mathbb{Z}} M_n$ that $A_m M_n \subset M_{m+n}$.

Notice that often we mean $\mathbb{Z}^{\geq 0}$-graded rings when we say graded rings. For a $\mathbb{Z}^{\geq 0}$-graded ring A, the subset $A_+ = \bigoplus_{n=1}^{\infty} A_n$ is an ideal of A, called the **irrelevant ideal**. ⌟

Def. (5.2.2.2) [Twisted Modules]. Let A be a graded ring and M a graded A-module, denote $M(n)$ the graded A-module s.t. $M(n)_m = M_{m+n}$. ⌟

Lemma (5.2.2.3). Let $A = \bigoplus_0^\infty A_n$ be a graded ring, then a set of homogenous elements $f_i \in A_+$ generate A as an algebra over A_0 iff they generate A_+ as an ideal of A. ⌟

Proof: If f_i generate A as algebra over A_0, then every element of A_+ is a polynomial in f_i with constant coefficients in A_0, thus f_i generates A_+ as an ideal. Conversely, if f_i generate A_+ as a ideal, then for any homogenous element f we can use induction on the degree of f to show that f is a polynomial in f_i. □

Prop. (5.2.2.4) [Noetherian Graded Rings]. A graded ring $A = \bigoplus_{n=0}^\infty A_n$ is Noetherian iff A_0 is Noetherian and A_+ is f.g. as an ideal of A. ⌟

Proof: If A is Noetherian, then clearly A_+ is f.g. and $A_0 = A/A_+$ is Noetherian. Now if A_+ is f.g. as an ideal of A, then it is generated by f.m. homogenous elements f_i, so we see f_i generates A as an algebra over A_0, which means A is a quotient of a polynomial ring over A_0, thus Noetherian by(5.1.1.41). □

Def. (5.2.2.5) [Homogenous Ideals]. Let $A_\bullet$ be a graded ring, then a **homogenous ideal** $I_\bullet$ of $A_\bullet$ is a ring that is generated by homogenous elements. ⌟

Prop. (5.2.2.6) [Equivalent definition of Homogenous Ideals]. Let $S_\bullet$ be a graded ring, then

- an ideal I of $S_\bullet$ is homogenous iff it contains the degree n part of each of its element for any n.
- The set of homogenous ideals of $S_\bullet$ is stable under sum, product, intersection and radical.
- A non-trivial homogenous ideal I of $S_\bullet$ is a prime ideal iff for any homogenous elements a, b, if $ab \in I$, then $a \in I$ or $b \in I$.

⌟

Proof: 1: If I contains the degree n part of each of its element for any n, then clearly it is generated by homogenous elements. Conversely, if it is generated by homogenous elements, then any element $f = \sum a_i f_i$, where f_i is homogenous. Then we can see $[f]_n = \sum [a_i]_{n-\deg f_i} f_i$ is also in I.

2: Use 1 and the definition. For radicals, we show $\sqrt{I}$ contains all its homogenous parts: if $f \in \sqrt{I}$, then $f^n \in I$ for some n, then we see that the minimal degree part $[f]_m$ of f also satisfies $[f]_m^n \in I$, because I contains the homogenous parts of each of its elements. Then we can use induction to show that all the homogenous parts of f is in $\sqrt{I}$.

3: One direction is trivial, for the other, if $a = \sum a_i, b = \sum b_i$ satisfies $ab \in I$, and $a \notin I, b \notin I$, and a_i, b_j homogenous. Let i_0, j_0 be the minimal numbers that $a_{i_0} \notin I$, $b_{j_0} \notin I$, then $a_{i_0} b_{j_0}$ is not in I, contradicting the fact I is homogenous. □

Prop. (5.2.2.7). Let $R \to S$ be a homomorphism of graded rings, then the integral closure of R in S is a homogenous ideal of S. ⌟

Proof: consider the base change $\varphi : R \otimes_{R_0} R_0[t, t^{-1}] \to S \otimes_{S_0} S_0[t, t^{-1}]$, where $\deg(t) = 0$, and the integral closure is denoted by A. Then there is an automorphism of φ: $s \mapsto t^{\deg s} s$. This automorphism thus preserves the integral closure. if $s = s_n + s_{n+1} + \ldots + s_m \in S$ is integral over R, to show each s_i are integral over S. We may assume $n > 0$ because s_0 is clearly integral over R_0. Now we use induction on m. If $m > n$, consider $t^n s_n + \ldots + t^m s_m$ is also in A, we see $(t^m - t^i)s_i \in A$ by induction hypothesis.

Notice $S \subset S[t, t^{-1}]/(t^m - t^i - 1) = S[t]/(t^m - t^i - 1)$ is injective, and the image of $(t^m - t^i)s_i$ is s_i, which is integral over $R[t]/(t^m - t^i - 1)$, and this ring is finite over R, so s_i is also integral over R. □

Prop. (5.2.2.8). Let A be a graded ring that is f.g. over A_0 and M be a f.g. graded A-module, then each M_n is a finite S_0-module. ⌟

Def. (5.2.2.9) [Reductions of Graded Rings]. Let S be a graded ring and $d \geq 1$, define $S^{(d)}$ the graded ring $\oplus_{n \geq 0} S_{nd}$. And for a graded S-module M, define $M^{(d)} = \oplus_{n \in \mathbb{Z}} M_{nd}$. ⌟

Prop. (5.2.2.10). If S is a graded ring that is f.g. over S_0, then for d sufficiently divisible, $S^{(d)}$ is generated by the degree 1 part over S_0. ⌟

Proof: Let S be generated by homogenous elements $f_1, \ldots, f_r$. Let $M = lcm(\deg(f_1), \ldots, \deg(f_r))$, then for any $f \in S_{Nm}$ and $N \geq r$, by pigeonhole principle, there are some i s.t. $f_i^{M/\deg(f_i)} | f$. Thus any monomials of degree nrM is a product of polynomials of degree rM. So $d = rM$ satisfies the hypothesis. □

Topology Defined by Ideals

Def. (5.2.2.11) [Filtrations on Graded Modules]. Let A be a ring, M a graded A-module, and $\mathfrak{a}$ be an ideal of A, an **$\mathfrak{a}$-filtration** of M is a descending sequence of submodules $M = M_0 \supset M_1 \supset \ldots$ that $\mathfrak{a} M_n \subset M_{n+1}$. It is called a **stable filtration** iff there is an N that $\mathfrak{a} M_n = M_{n+1}$ for $n \geq N$.

For an ideal $\mathfrak{a} \subset A$, there can be associated a graded ring $A^* = \oplus \mathfrak{a}^n$, and an $\mathfrak{a}$-filtration M can be associated a graded module over $A^* : M^* = \oplus M_n$. When A is Noetherian, then so is A^*, because it is a quotient of a polynomial ring over A(5.1.1.41). ⌟

Lemma (5.2.2.12). If A is a Noetherian ring and M is a f.g. A-module that has a $\mathfrak{a}$-filtration M_n, then M^* is f.g. over A^* iff M_n is a stable filtration. ⌟

Proof: As every M_n is finite over A, if it is stable, then M^* is generated over A^* by all the generator of $M_n, n \leq N$, so it is f.g.. Conversely, if it is f.g., then it is clear that M_n is a stable filtration. □

Prop. (5.2.2.13) [Artin-Rees]. For A Noetherian and I an ideal, let $N \subset M$ be finite A-modules, then if M_n is a stable filtration of M, then $M_n \cap N$ is a stable filtration of N.

In particular, let $M_n = I^n M$, then $I^n M \cap N = I^{n-r}(I^r M \cap N)$, hence the I-adic topology on M induce the I-adic topology on N. ⌟

Proof: This is immediate from the lemma above, as N^* is an A^*-submodule of M^*, and A^* is Noetherian(5.2.2.11). □

Cor. (5.2.2.14) [Krull's Intersection Theorem]. Notation as in(5.2.2.13), let $N = \bigcap^{\infty} I^n M$, then the I-adic topology on N is trivial, by Artin-Rees, thus $IN = N$. So Nakayama tells us there is an element $a \in 1 + I$ that $aN = 0$. Thus if $I \subset \text{rad}(A)$ or A is an integral domain, $N = 0$. This can be used to use induction to prove some theorem.

In particular, for any prime ideal $\mathfrak{p}$ containing I, use the above on $R_{\mathfrak{p}}$ shows $N_{\mathfrak{p}} = 0$. But also N is f.g., so there exists an element $g \notin \mathfrak{p}$ that $N_g = 0$. ⌟

Cor. (5.2.2.15) [Krull]. For A Noetherian, if $I \subset \text{rad}(A)$ or A is a domain, then $\bigcap^\infty I^n = 0$. ⌟

Prop. (5.2.2.16). Notice for any ring A and a non-zero-divisor f, if $I = \cap_n f^n A$, then $fI = I$, needless of the Noetherian property. ⌟

Proof: If $x \in I$, $x = fy$, because $x \in f^n A$, $fy = f^n t$ for some t, so $y = f^{n-1} t$, so $f \in I$. Thus $I = fI$. □

Def. (5.2.2.17) [Hilbert-Serre]. Let A be a Noetherian graded ring with A_0 Artinian that A_+ is generated by A_1. For a f.g. graded A-module $M = \oplus M_n$, we have $l(M_n)$ is a numerical polynomial of n(2.6.3.13) for n sufficiently large, called the **Hilbert Polynomial**. Its degree is the dimension of $\text{Supp}\, M \subset \text{Proj}(A)$. ⌟

Proof: We prove by induction on the minimal number of generators of A_1(it is finite by(5.2.2.4)). If it is 0, then $M_n = 0$ for n large and the result holds. Now choose $x \in S_1$ as one of the minimal set of generators, then the induction hypothesis applies to $S/(x)$.

Firstly, if x acts nilpotently on M, then we do induction on the minimal number r that $x^r M = 0$. If $r = 1$, then M is a module over $S/(x)$ and the assertion holds. If $r > 1$, then we can find an exact sequence $0 \to M' \to M \to M'' \to 0$ that M', M'' has smaller r, then we have the desired result, because l is additive.

Next, if x doesn't act nilpotently on M, let $M' \subset M$ is the largest submodule that x acts nilpotently, then there is an exact sequence $0 \to M' \to M \to M/M' \to 0$. So we can assume multiplication by x is injective on M.

Let $\overline{M} = M/xM$, then for any d, there are exact sequences

$$0 \to M_d \xrightarrow{x} M_{d+1} \to \overline{M}_{d+1}.$$

so $l(M_{d+1}) - l(M_d) = l(\overline{M}_{d+1})$. Then we finish by(2.6.3.14). □

Cor. (5.2.2.18). Let k be a field, $I \subset k[X_1, \ldots, X_n]$ be a non-zero graded ideal, and $M = k[X_1, \ldots, X_n]/I$, then the numerical polynomial $n \mapsto \dim_k(M_n)$ has degree $< d - 1$. ⌟

Proof: The numerical polynomial associated to $k[X_1, \ldots, X_n]$ is $n \mapsto \binom{n-1+d}{d-1}$, and for any non-zero homogenous element $f \in I$ of degree e, $f \cdot k[X_1, \ldots, X_n]_{d-e} \subset I_d$, thus $\dim_k(M_n) < \binom{n-1+d}{d-1} - \binom{n-e-1+d}{d-1}$, which means the numerical polynomial has degree$< d - 1$. □

Prop. (5.2.2.19) [Hilbert Polynomial and Dimension]. For a Noetherian local ring A, the Hilbert polynomial of a f.g. module M w.r.t $\mathfrak{m}$ has degree $\dim M$. And $\dim M$ is the smallest integer r s.t. there exists $x_1, \ldots, x_r$ that $l(M/x_1 M + \ldots, x_r M) < \infty$. ⌟

Proof: Cf.[Mat P76]. □

3 Completions

This subsubsection should be combined with the derived completion.

Prop. (5.2.3.1). Let the topology on a A-module be defined by countable filtration of submodules, then iff M is complete, then M/N is complete in the quotient topology. ⌟

Proof: Write $x_{i+1} - x_i = y_i + z_i$ with $y_n \in M_n$ and $z_n \in N$, then the image of the limit of $\sum y_i$ is the limit of $\overline{x_i}$. □

Def. (5.2.3.2) [Completeness]. Let I be an ideal of R, the **I-adic completion** of a R-module is a functor $\varphi : M \mapsto \widehat{M} = \lim M/I^n M$. An R-module is called **I-adically complete** if the natural map $M \to \widehat{M}$ is an isomorphism.

This is compatible with the general notion of completion of a topological Abelian groups(11.2.1.5). ⌟

Prop. (5.2.3.3). Let R be a ring and $I \subset R$ be an ideal, $\varphi : M \to N$ be a map of R-modules. Then

- If $M/IM \to N/IN$ is surjective, then $\widehat{M} \to \widehat{N}$ is surjective. In particular, this holds for $M \to N$ surjective.
- If $0 \to K \to M \to N \to 0$ is exact and N is flat, then $0 \to \widehat{K} \to \widehat{M} \to \widehat{N} \to 0$ is exact.
- $M \otimes_R \widehat{R} \to \widehat{M}$ is surjective for any finite R-module M.

⌟

Proof: Cf.[Sta]0315. □

Prop. (5.2.3.4). Let I be a f.g. ideal of A and M an A-algebra, then $\widehat{M}$ is I-adically complete and $I^n\widehat{M} = \ker(\widehat{M} \to M/I^n M) = (I^n M)^\wedge$. ⌟

Proof: Because I is f.g., so does I^n. If $I^n = (f_1, \ldots, f_r)$. Applying(5.2.3.3) to $(f_1, \ldots, f_r) : M^r \to I^n M$ shows

$$\widehat{M}^r \to (I^n M)^\wedge = \varprojlim_{m \geq n} I^n M/I^m M = \ker(\widehat{M} \to M/I^n M)$$

but the image is clearly $I^n\widehat{M}$, so $\widehat{M}/I^n\widehat{M} \cong M/I^n M$. Taking inverse limit yields $(M^\wedge)^\wedge = M^\wedge$. □

Cor. (5.2.3.5) [Completion is Complete]. Let I be a f.g. ideal of A and (M_n) an inverse system of A-modules that $I^n M_n = 0$, then $M = \lim M_n$ is I-adically complete. ⌟

Proof: We have maps $M \to M/I^n \to M_n$, taking limit, we get $M \to \widehat{M} \to M$, so M is a direct summand of $\widehat{M}$. Since $\widehat{M}$ is I-adically complete by(5.2.3.4), so does M. □

Prop. (5.2.3.6). If I is a f.g. ideal of A and (M_n) is an inverse system of A-modules that $M_n = M_{n+1}/I^n M_{n+1}$, then $M = \lim M_n$ is I-adically complete and $M/I^n M = M_n$. ⌟

Proof: $\widehat{M}$ is I-adically complete by(5.2.3.5), and $M \to M_n$ are all surjective because the transition maps are surjective. Consider the inverse system $N_n = \ker(M \to M_n)$. Since $M_n = M_{n+1}/I^n M_{n+1}$, the map $N_{n+1} + I^n M \to N_n$ is surjective, and thus $N_{n+1}/(N_{n+1} \cap I^{n+1} M) \to N_n/(N_n \cap I^n M)$ is surjective.

Taking the inverse limit of the exact sequences

$$0 \to N_n/(N_n \cap I^n M) \to M/I^n M \to M_n \to 0,$$

we get an exact sequence

$$0 \to \varprojlim N_n/(N_n \cap I^n M) \to \widehat{M} \to M.$$

As M is I-adically complete, $\widehat{M} = M$, thus $\varprojlim N_n/(N_n \cap I^n M) = 0$, thus $N_n/(N_n \cap I^n M) = 0$ for any n as n the transition maps are surjective. Then $M/I^n M = M_n$, as desired. □

Cor. (5.2.3.7) [Spectrum Map of Completions]. $\operatorname{Spec} R^\wedge \to \operatorname{Spec} R$ has image $\operatorname{Spec} R/I \subset \operatorname{Spec} R$. This follows from(5.2.3.18) and $R/I \cong R^\wedge/I$. ⌟

Prop. (5.2.3.8). If I is an ideal of R and $0 \to M \to N \to Q \to 0$ is an exact sequence that Q is annihilated by a power of I, then completion produces an exact sequence

$$0 \to \widehat{M} \to \hat{N} \to Q \to 0$$

⌟

Proof: If $I^c Q = 0$, then $Q/I^n Q = Q$ cor $n \geq c$, and $I^n M \subset M \cap I^n N \subset I^{n-c} M$ because of this. Then $\widehat{M} = \varprojlim M/(M \cap I^n N)$ by(4.1.1.41), and we apply(5.9.3.2) to the inverse system of exact sequences

$$0 \to M/(M \cap I^n N) \to N/I^n N \to Q \to 0$$

to conclude. □

Cor. (5.2.3.9). If A is a ring with a nonzero-divisor t and there is an exact sequence $0 \to M \to N \to Q \to 0$ of A-modules that $IQ = 0$, then M is I-adically complete iff N is I-adically complete. ⌟

Proof: Use snake lemma. □

Cor. (5.2.3.10). Take $I = (f)$ and $M = N = R$, then we see that if t is a nonzero-divisor in R then t is a nonzero-divisor in $\widehat{R}$. ⌟

Prop. (5.2.3.11). The completion of a submodule $N \subset M$ is the closure of $\varphi(N)$ (By direct construction). The completion of M/N is M^*/N^* because it is right exact. ⌟

Cor. (5.2.3.12). If N is open in M then $M/N \cong M^*/N^*$ because M/N is discrete hence complete. ⌟

Prop. (5.2.3.13). When A is Noetherian and M is finite A-module, then the natural map $M \otimes_A A^* \to M^*$ is an isomorphism (use M is finite presentation and tensor & completion is right exact), and five lemma. ⌟

Cor. (5.2.3.14). When A is Noetherian, $A \to A^\wedge$ is flat (because flatness is check for finite module).

And when A is complete Hausdorff, any finite module M is complete Hausdorff and hence any its submodule is complete thus closed in it. Hence the the completion of a submodule $N \subset M$ is $\varphi(N)A^*$ in $M^* = MA^*$. In fact this implies complete Hausdorff adic-ring is Zariski. ⌟

Remark (5.2.3.15). WARNING: If A is not Noetherian, in general $A \to A^\wedge$ is not flat, Cf.[Sta]0AL8. ⌟

Lemma (5.2.3.16). Let A be a ring and $I = (f_1, \ldots, f_r)$ be a f.g. ideal. If $M \to \varprojlim M/f_i^n M$ is surjective for each i, then $M \to \varprojlim M/I^n M$ is also surjective. ⌟

Proof: Note that $\varprojlim M/I^n M = \varprojlim M/(f_1^n, \ldots, f_r^n)M$, as $I^{rn} \subset (f_1^n, \ldots, f_r^n) \subset I^n$, and elements in $\varprojlim M/(f_1^n, \ldots, f_r^n)M$ can be written as an infinite sum $\xi = \sum_n \sum_i f_i^n x_{n,i}$. There is an element x_i mapping to $\sum_n f_i^n x_{n,i}$ for any i, thus $\sum_i x_i$ maps to ξ. □

Lemma (5.2.3.17). Let A be a ring and $I \subset J$ be ideals, if M is J-adically complete and I is f.g., then M is I-adically complete. ⌟

Proof: It is clearly I-adically Hausdorff, and for completeness, by(5.2.3.16) it suffices to show for $I = (f)$: Let $x_n \in M$ with $x_n - x_{n+1} \in f^n M$, then $\{x_n\}$ is J-adically Cauchy, thus there is an element x that $x - x_n \in J^n$, and we can replace x_n by $x_n - x$ to assume $x_n \in J^n$. Now we prove $x_n \in (f^n)$: assume $x_n - x_{n+1} = f^n z_n$, then

$$x_n = f^n(z_n + f z_{n+1} + \ldots).$$

This equation is true because it is J-adically Cauchy. □

Properties of Complete Rings

Prop. (5.2.3.18). If A is I-adically complete, then $I \subset \operatorname{rad} A$. ⌟

Prop. (5.2.3.19). Let A be a ring with a non-zero-divisor t, then any limit of t-adically complete algebras is t-adically complete. ⌟

Proof: Check the definition directly. □

Prop. (5.2.3.20) [Zariski Rings]. A Noetherian I-adic ring is called **Zariski ring** if it satisfies the following equivalent conditions:

- Every finite module is Hausdorff in the I-adic topology.
- Every submodule in a finite module is closed in the I-adic topology.
- Every ideal is closed.
- $I \subset \operatorname{rad} A$.
- $A^\wedge/A$ is f.f.

Hence every complete Hausdorff ring is Zariski. ⌟

Proof: $1 \to 2$: Apply it to the submodule M/N.
$3 \to 4$: If $I \not\subset m$, then $I^n + m = A$, thus $\overline{M} = A$, contradiction.
$4 \to 1$: by intersection theorem(5.2.2.14).
$4 \to 5$: for any maximal ideal m, $I \subset m$ so it is open, thus $A^*/mA^* = A/m \neq 0$ by(5.2.3.12) thus f.f. by(5.4.1.5).
$5 \to 1$:by(5.4.1.21), for any m maximal, there is a maximal ideal m' lying over m, so $IA^* \subset m^*$ by(5.2.3.14), thus $I \subset m$, hence $I \subset \operatorname{rad} A$. □

Cor. (5.2.3.21). In a Zariski ring A, maximal ideals are open, thus $A/m \cong A^*/mA^*$ by(5.2.3.12), thus $\operatorname{Spec} A^* \to \operatorname{Spec} A$ is bijection on closed pt. ⌟

Prop. (5.2.3.22) [Cohen Structure Theorem]. If A is a complete local ring containing a field k that the residue field is separably generated over k, then there is a field K containing k that is a Cohen ring, i.e. complete local ring with a prime number as a uniformizer, that has the same residue field as A. ⌟

Proof: □

Lemma (5.2.3.23) [Complete Interchanging Lemma]. If R is a commutative ring, $x, y \in R$, if x is not a zero-divisor in R and R is x-adically complete, and y is not a zero-divisor in R/x and R/x is y-adically complete, then the same is true with x, y interchanged. ⌟

Proof: ? □

4 Dimension

Def. (5.2.4.1) [Dimensions and Heights]. For a A-module M, $\dim(M)$ is defined as $\dim(A/\mathrm{Ann}(M))$.

The **height** of an ideal I in A is defined as the infimum of heights of the prime ideals over I.

The **dimension** of a ring R is defined to be the supremum of heights of prime ideals of R. ⌟

Prop. (5.2.4.2). For any ring A $\dim A = \sup \dim A_{\mathfrak{p}}$. ⌟

Def. (5.2.4.3) [Catenary Rings]. $A \in \mathcal{CA}\mathrm{lg}$ is called **catenary** if for any pair of primes $\mathfrak{p} \subset \mathfrak{q} \subset A$, any maximal chain of primes $\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_e = \mathfrak{q}$ has the same length. A Noetherian ring is called **universally catenary** if all f.g. algebras over it are catenary. ⌟

Prop. (5.2.4.4). $A \in \mathcal{CA}\mathrm{lg}$ is catenary iff $\mathrm{Spec}\, A$ is a catenary space(4.12.3.34). ⌟

Prop. (5.2.4.5). Any quotient ring and localization of a (universally)catenary ring is catenary. Any quotient of a Noetherian universally catenary ring is universally catenary. Catenary and universally catenary are stalkwise properties(5.1.4.2). ⌟

Prop. (5.2.4.6). If $(A, \mathfrak{m})$ is a Noetherian local ring, then A is catenary iff $\mathfrak{p} \to \dim(A/\mathfrak{p})$ is a dimension function on $\mathrm{Spec}\, A$. ⌟

Proof: This follows from(4.12.4.13)(4.12.3.39) and(4.12.3.37). □

Example (5.2.4.7) [Universally Catenary Rings]. The following are same examples of universally catenary Rings:

- A f.g. algebra over a universally catenary ring.
- A Noetherian C.M. rings.
- 1-dimensional Noetherian domains,
- Fields.

⌟

Proof: Cf.[Sta]00NM.? □

Def. (5.2.4.8) [Hilbert Polynomials]. Let $(A, \mathfrak{m})$ be a Noetherian local ring, I an ideal of definition, then ⌟

Dimension of Noetherian Local Rings

Prop. (5.2.4.9). For a Noetherian local ring R, the following three numbers are equal:

- $\dim R$.
- $d(R)$.
- the minimal number of elements needed to generate an ideal of definition of R(5.1.1.12).

A **system of parameters** is d elements $g_1, \ldots, g_d$ that generate an ideal of definition of R, where $d = \dim R$. ⌟

Proof: Cf.[Sta]00KQ.? □

Cor. (5.2.4.10). The dimension of a Noetherian local ring is finite, by item3. Thus the codimension of a subscheme in a Noetherian scheme is finite. ⌟

Cor. (5.2.4.11). If A is a Noetherian local ring with maximal ideal $\mathfrak{m}$, then $\dim A \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$. ⌟

Proof: By Nakayama, if $x_1, \ldots, x_d \in \mathfrak{m}$ generate $\mathfrak{m}/\mathfrak{m}^2$, then $(x_1, \ldots, x_d) = \mathfrak{m}$. □

Dimension and Ring Extensions

Prop. (5.2.4.12) [Dimension and Going-Up(Down)]. If $A \to B$ is a ring map that Spec map is surjective and $A \to B$ satisfies either going-up or going-down, then $\dim B \geq \dim A$. ⌟

Proof: The hypothesis implies any chain of primes in A can lifted to a chain of primes in B. □

Prop. (5.2.4.13) [Dimensions and Noetherian Ring Extensions]. Let $A \to B$ be a map between Noetherian rings, P a prime ideal of B, $\mathfrak{p} = P \cap A$, then:

- $\mathrm{ht}(P) \leq \mathrm{ht}(\mathfrak{p}) + \mathrm{ht}(P/pB)$,in other words $\dim(B_P) \leq \dim(A_p) + \dim(B_P/\mathfrak{p}B_P)$.
- equality holds if going-down holds. For example, if it is flat(5.1.7.13).

⌟

Proof: 1: Localize at p and P, we may assume A, B are local rings with maximal ideals $\mathfrak{p}$ and P, then use the characterization(5.2.4.9) of dimension, if $x_1, \ldots, x_d$ generate an ideal of definition of $A_\mathfrak{p}$ and $y_1, \ldots, y_e$ generate an ideal of definition of $B_P/\mathfrak{p}B_P$, then $x_1, \ldots, x_d, y_1, \ldots, y_e$ generate an ideal of definition of B_P.

2: If going down holds, for any chain of primes in B_P containing $\mathfrak{p}B_P$, we can lift the chain of primes in $A_\mathfrak{p}$ to a chain of primes in B_P to get a longer chain, thus we get the other direction of inequality.

□

Prop. (5.2.4.14) [Dimension of Integral Extensions]. Let $A \to B$ be an integral ring map, then:

1. Spec maps closed points to closed points, and $\dim(A) \geq \dim(B)$, which equality if $A \subset B$.
2. If A, B is Noetherian, $\mathrm{ht}(P) \leq \mathrm{ht}(P \cap A)$
3. If A, B is Noetherian and going down holds, then $\mathrm{ht}(J) = \mathrm{ht}(J \cap A)$ for any ideal $J \subset B$.

⌟

Proof: 1:By(5.2.1.5), there is no inclusion relation between prime over a fixed prime, so $\dim(B) \leq \dim(A)$. On the other hand, if $A \subset B$, then Spec map is surjective going-up holds(5.2.1.5), so $\dim(B) \geq \dim(A)$(5.2.4.12).

2: Follows from (5.2.4.13)(1) since $\mathrm{ht}(P/(P \cap A)B) = 0$ by(5.2.1.5).

3: In this case, $\mathrm{ht}(P) = \mathrm{ht}(P \cap A)$ holds by(5.2.4.13)(2), then use the surjectiveness of Spec for the integral extension $A/J \cap A \subset B/J$(5.2.1.5). □

Cor. (5.2.4.15). if $A \to B$ is integral and faithfully flat, then $\dim A = \dim B$. ⌟

Proof: This follows from(5.2.4.14) and(5.4.1.28). □

Prop. (5.2.4.16) [Dimension and Completion]. For a local ring A, $\dim A = \dim \widehat{A}$. ⌟

Proof: □

Noetherian Normalization

Prop. (5.2.4.17). For a Noetherian ring A, $\dim A[X] = \dim A + 1$. ⌟

Proof: Let $\mathfrak{p}$ be a prime ideal of A and let $\mathfrak{q}$ be a prime ideal of $A[X]$ maximal among primes lying over $\mathfrak{p}$, then $\mathrm{ht}(\mathfrak{q}/\mathfrak{p}A[X]) = 1$. In fact, by localizing, we can assume $\mathfrak{p}$ is a maximal ideal, then $A[x]/\mathfrak{p}A[x]$ is a polynomial ring over a field thus a PID and $\mathrm{ht}(\mathfrak{q}/\mathfrak{p}A[X]) = 1$. Thus $\mathrm{ht}(\mathfrak{q}) = \mathrm{ht}(\mathfrak{p}) + 1$ by(5.2.4.13). Now we are done, because $\mathrm{Spec}\, A[X] \to \mathrm{Spec}\, A$ is surjective. □

Prop. (5.2.4.18) [Krull's Height Theorem]. In a Noetherian domain R, the height of an ideal generated by n elements is at most n. ⌟

Proof: Let $\mathfrak{p}$ be a minimal ideal containing $(f_1,\ldots,f_n)$, then it suffices to show $\dim(R_\mathfrak{p})\leq n$ In this case, $(f_1,\ldots,f_n)$ is an ideal of definition of $R_\mathfrak{p}$, thus we can use(5.2.4.9). □

Prop. (5.2.4.19) [Number of Generators]. To show an ideal $I\subset A$ cannot be generated by smaller than n element, choose a maximal ideal $\mathfrak{m}$, then show that $\dim_{A/\mathfrak{m}} I/\mathfrak{m}I\geq n$. ⌟

Cor. (5.2.4.20).

- (x,z) is not principal in $k[x,y,z]$.
- $(wz-xy)$ is not principal in $k[x,y,z]$.
- (xy,yz,xz) is not generated by two elements in $k[x,y,z]$.

⌟

Lemma (5.2.4.21). Let $A=k[X_1,\ldots,X_n]$ be a polynomial ring over a field k, and I is an ideal of A of height r, then we can choose $Y_1,\ldots,Y_n\in A$ that A is integral over $k[Y_1,\ldots,Y_n]$ and $I\cap k[Y_1,\ldots,Y_n]=(Y_1,\ldots,Y_r)$. ⌟

Proof: We use induction on r. $r=0$ is easy. For $r=1$, let $f(X)$ be any non-zero polynomial in I, then we can assign suitable integral weights $d_1=1,d_2,\ldots,d_n$ to X_i that monomials of f have different weights. Put $Y_i=X_i-X_1^{d_i}$ for $i\geq 2$, and

$$Y_1=f(X)=f(X_1,Y_2+X_1^{d_2},\ldots,Y_n+X_1^{d_n})=a_1X_1^N+g(X_1,Y_2,\ldots,Y_n)$$

where g has degree in X_1 lower that N. Then X_1 is integral over $k[Y_1,\ldots,Y_n]$, and hence $X_i=Y_1+X_1^{d_i}$ is also integral over $k[Y]$.

Now (Y_1) is a prime ideal in $k[Y]$ of height 1 and $(Y_1)\in I\cap k[Y]$. Also notice $I\cap k[Y]$ has height 1 by(5.2.4.14)(Because going-down holds by(5.1.7.17)), so $(Y_1)=I\cap k[Y]$.

For $r\geq 2$, let $J\subset I$ be an ideal with height $r-1$, let J be an ideal of $k[X]$ contained in I that $\mathrm{ht}(J)=r-1$.(This is possible by choosing f_i out of all minimal primes containing $(f_1,\ldots,f_{r-1})$ and use Krull's Height Theorem). By induction hypothesis, there exists $Z_1,\ldots,Z_n$ that $k[X]$ is integral over $k[Z]$, and $J\cap k[Z]=(Z_1,\ldots,Z_{r-1})$. Now $\mathrm{ht}(I\cap k[Z])=r$ by the same argument above, thus there exist $f\in I\cap k[Z]\backslash(Z_1,\ldots,Z_{r-1})$, and do the same for $r=1$ again, we can find the desired Y_i that $Y_k=Z_k$ for $k\leq r-1$. □

Prop. (5.2.4.22) [Noetherian Normalization Theorem]. If A is a f.g. algebra over a field. then there are r alg. independent elements y_i that A is integral over $k[y_i]$. ⌟

Proof: Let $A=k[X_1,\ldots,X_n]/I$ and $\mathrm{height}(I)=n-r$, then by the lemma we can choose $Y_1,\ldots,Y_n$ that $k[X_1,\ldots,X_n]$ is integral over $k[Y_1,\ldots,Y_n]$(so $Y_1,\ldots,Y_n$ are algebraically independent) and $I\cap k[Y_1,\ldots,Y_n]=(Y_{r+1},\ldots,Y_n)$. Now we can just choose $y_i=Y_i$ for $i\leq r$. □

Cor. (5.2.4.23) [Dimension and Transcendental Degree]. If A is a f.g. integral ring over a field k, then $\dim A=\mathrm{tr}.\deg_k A$. ⌟

Proof: This is because integral extensions of integral Noetherian rings have the same dimensions(5.2.4.14) and their fraction fields have the same transcendental degrees. □

Cor. (5.2.4.24). Let A,B be f.g. algebras over a field k, then $\dim(A\otimes_k B)=\dim A+\dim B$. ⌟

Cor. (5.2.4.25) [Dimension and Field Base Change]. Let K/k be a field extension and S a f.g. algebra over k, then $\dim S = \dim S \otimes_k K$. ⌟

Proof: By Noetherian normalization, there exists a finite injective map $k[d_1, \ldots, d_n] \to S$ where $n = \dim S$. Then there exists a finite injective map $K[d_1, \ldots, d_n] \to S_K$, so $\dim S \otimes_k K = n$, by(5.2.4.14) and(5.2.4.17). □

Prop. (5.2.4.26) [Codimensions and Field Base Change]. Let K/k be a field extension and S a f.g. k-algebra. Let $\mathfrak{q}$ be a prime of S and q_K be a prime of S_K lying over $\mathfrak{q}$, then

$$\dim(S_K \otimes_S k(\mathfrak{q}))_{\mathfrak{q}_K} = \dim(S_K)_{\mathfrak{q}_K} - \dim S_{\mathfrak{q}} = \operatorname{tr.deg}_k k(\mathfrak{q}) - \operatorname{tr.deg}_K k(\mathfrak{q}_K).$$

Moreover, for any $\mathfrak{q}$, we can choose q_K so that this number is 0. ⌟

Proof: Cf.[Sta]0CWE. □

Local Dimension over Fields

Prop. (5.2.4.27) [Local Dimension]. Let Let S be an algebra f.g. over a field k, $X = \operatorname{Spec} S$ and $x \in X$, then the following three numbers are equal:

- the local dimension(4.12.3.25) $\dim_x(X)$.
- $\max \dim(Z)$ where Z runs through irreducible components of X passing through x.
- $\min \dim(S_{\mathfrak{m}})$, where $\mathfrak{m}$ are maximal ideals containing $\mathfrak{p}_x$.

⌟

Proof: Cf.[Sta]00OT. □

Lemma (5.2.4.28). Let k be a field and S a f.g. k-algebra, $X = \operatorname{Spec} S$, $x \in X$, then

$$\dim_x(X) = \dim S_{\mathfrak{p}} + \operatorname{tr.deg}_k k(\mathfrak{p}).$$

⌟

Proof: Cf.[Sta]00P1. □

Cor. (5.2.4.29). Let $S' \to S$ be a surjection of f.g. algebras over a field k, $\mathfrak{p}$ a prime ideal of S and $\mathfrak{p}'$ its inverse image in S', corresponding to x, x' in $X = \operatorname{Spec} S, X' = \operatorname{Spec} S'$ resp., then

$$\dim_{x'}(X') - \dim_x(X) = \operatorname{ht}(\mathfrak{p}') - \operatorname{ht}(\mathfrak{p}).$$

⌟

Def. (5.2.4.30) [Relative Dimension]. Let $R \to S$ be a ring map of f.t., and $\mathfrak{q} \subset S$ be a prime over $\mathfrak{p} \subset R$, then we define the **relative dimension** of S/R at $\mathfrak{q}$ to be $\dim_{\mathfrak{q}}(\operatorname{Spec} S)_{\mathfrak{p}}$. The supremum of all these numbers over $\mathfrak{q} \subset \operatorname{Spec} S$ is called the relative dimension of S/R, denoted by $\dim(S/R)$. ⌟

Lemma (5.2.4.31) [Local Dimension and Field Extension]. Let K/k be a field extension, S be a f.g. k-algebra, and $X = \operatorname{Spec} S$. Now if $\mathfrak{p}_K$ is an element of S_K lying over $\mathfrak{p} \subset S$, then $\dim_{\mathfrak{p}}(S) = \dim_{\mathfrak{p}_K}(S_K)$. ⌟

Proof: The proof is by reduction to polynomial ring. Let $S = k[X_1, \ldots, X_n]/I$, let $\mathfrak{p}'_K, \mathfrak{p}'$ be primes of $k[X_1, \ldots, X_n]$ and $K[X_1, \ldots, X_n]$ that is the image of x and x_K, then there is a commutative diagram

$$\begin{array}{ccc} K[X_1, \ldots, X_n]_{\mathfrak{q}'_K} & \longrightarrow & (S_K)_{\mathfrak{q}_K} \\ \downarrow & & \downarrow \\ k[X_1, \ldots, X_n]_{\mathfrak{q}'} & \longrightarrow & S_{\mathfrak{q}} \end{array}.$$

The vertical arrows are flat because they are local morphisms of flat maps, and their fibers are the same, so by(6.6.3.17), $\mathrm{ht}(\mathfrak{q}'_K) - \mathrm{ht}(\mathfrak{q}') = \mathrm{ht}(\mathfrak{q}_K) - \mathrm{ht}(\mathfrak{q})$. Also use(5.2.4.29) on the horizontal maps, then we get the desired assertion. □

Prop. (5.2.4.32) [Semicontinuity of Dimensions]. Let $f : R \to S$ be a ring map of f.t., then the map $\mathfrak{q} \mapsto \dim_{\mathfrak{q}}(S/R)$ is a upper-semicontinuous function on $\mathrm{Spec}(S)$.

Moreover, if f is of f.p., then the set $\{\mathfrak{q} | \dim_{\mathfrak{q}}(S/R) \le n\}$ is quasi-compact open in $\mathrm{Spec}(S)$. ⌟

Proof: Cf.[Sta]00QH, 00QJ. □

5 Support and Associated Primes

Def. (5.2.5.1) [Support of a Module]. The **support** $\mathrm{Supp}(M)$ of a module M is the set of all p that $M_p \ne 0$. When M is f.g., $\mathrm{Supp}(M) = V(\mathrm{Ann}(M))$.

⌟

Prop. (5.2.5.2) [Support is Non-Empty]. The support of a nonzero module is not empty, because triviality is stalkwise by(5.1.4.2). ⌟

Prop. (5.2.5.3). If $0 \to N \to M \to Q \to 0$, then we have $\mathrm{Supp}(M) = \mathrm{Supp}(N) \cup \mathrm{Supp}(Q)$, this is because localization is exact. ⌟

Cor. (5.2.5.4). ⌟

Prop. (5.2.5.5). Let $(R, \mathfrak{m})$ be a Noetherian local ring and M a finite R-module, $f \in \mathfrak{m}$, then

$$\dim \mathrm{Supp}(M) - 1 \le \dim(\mathrm{Supp}(M/fM)) \le \dim(\mathrm{Supp}(M))$$

⌟

Proof: Cf.[Sta]0B52. □

Prop. (5.2.5.6). Let $0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$ be a filtration of M that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ where $\mathfrak{p}_i$ are primes, by(5.1.1.46), then $\mathrm{Supp}(M) = \cup_i V(\mathfrak{p}_i)$.

In particular, the minimal primes in $\{\mathfrak{p}_i\}$ are the same as the minimal primes of $\mathrm{Supp}(M)$. Moreover, the multiplicity of a prime $\mathfrak{p}_i$ equals $\mathrm{length}_{R_\mathfrak{p}} M_\mathfrak{p}$. ⌟

Proof: Cf.[Sta]00L7. □

Prop. (5.2.5.7). Let $(R, \mathfrak{m})$ be a Noetherian local ring and M a non-zero finite R-module, then $\mathrm{Supp}(M) = V(\mathfrak{m})$ iff $\mathrm{length}_R(M) < \infty$. ⌟

Proof: Cf.[Sta]00L5.? □

Prop. (5.2.5.8). Let A be Noetherian and I be an ideal, then $I^n M = 0$ for some n iff $\mathrm{Supp}(M) \subset V(I)$. ⌟

Proof: If $I^n M = 0$, then if $I \not\subset P$, then $M_P = 0$. Conversely, we have a filtration of M, and by(5.2.5.3) we have all the P_i include I, so I^n annihilate M. □

Prop. (5.2.5.9). If R is a ring and M is a f.p. R-module, then $\mathrm{Supp}(M)$ is a closed subset of $\mathrm{Spec}\, R$ whose complement is quasi-compact. ⌟

Proof: Let $R^m \to R^n \to M \to 0$, then the support of M is just the the locus that some minor of the linear map from $R^m \to R^n$ doesn't vanish. Then its complement is quasi-compact. □

Prop. (5.2.5.10). Let $(R, \mathfrak{m})$ be a Noetherian local ring and M is a finite R-module, then $d(M) = \dim(\mathrm{Supp}(M))$. ⌟

Proof: Cf.[Sta]00L8. □

Prop. (5.2.5.11). Let R be a Noetherian ring and $0 \to M' \to M \to M'' \to 0$ be an exact sequence of finite R-modules, then $\dim \mathrm{Supp}(M) = \max(\dim \mathrm{Supp}(M'), \dim \mathrm{Supp}(M''))$. ⌟

Proof: Cf.[Sta]0B51. □

Associated Primes of a Module

Def. (5.2.5.12) [Associated Primes of a Module]. The **weakly associated primes** $\mathrm{Ass}(M)$ of an A-module M is the set of minimal primes of $A/\mathrm{Ann}(m)$ for some $m \in M$.

The **associated primes** $\mathrm{Ass}(M)$ is the set of primes $\{p = \mathrm{Ann}(m)\}$ where $m \in M$. ⌟

Prop. (5.2.5.13). $Ass_R(M) \subset WeakAss_R(M)$, and if R is Noetherian, the converse is also true. ⌟

Proof: Cf.[Sta]058A. □

Prop. (5.2.5.14) [Associated Primes and Exact Sequence]. For an exact sequence $0 \to M_1 \to M \to M_2 \to 0$, $\mathrm{WeakAsso}(M) \subset \mathrm{WeakAsso}(M_1) \cup \mathrm{WeakAsso}(M_2)$ and $\mathrm{WeakAsso}(M_1) \subset \mathrm{WeakAsso}(M)$. ⌟

Proof: Cf.[Sta]0548.? □

Cor. (5.2.5.15) [F.M. Associated Primes]. For a finite module M over a Noetherian ring A, $\mathrm{Ass}_A(M)$ is finite by(5.1.1.46). ⌟

Prop. (5.2.5.16) [Associated Primes and Support]. $\mathrm{WeakAsso}(M) \subset \mathrm{Supp}\, M$, and their minimal elements are the same.

If $M \neq 0$, $\mathrm{WeakAsso}(M) \neq \varnothing$ by(5.2.5.2), and $\mathrm{WeakAsso}(A/I)$ contains all the minimal primes over I.? ⌟

Proof: If $\mathfrak{p} = \mathrm{Ann}(m)$, then m is nonzero in $M_\mathfrak{p}$, so $M_\mathfrak{p}$ is nonzero, i.e. $\mathfrak{p} \in \mathrm{Supp}(M)$.

For the second assertion, we first prove for M finite, and then write any module as sum of finite submodules, and use the fact Supp and ass are all unions of those of the submodules. Cf.[Sta]05C4 0588.? □

Prop. (5.2.5.17) [Weakly Associated Primes and Zero-divisors]. Let M a R-module, then the union of the weakly associated primes of M is the set of zero-divisors in M. ⌟

Proof: Elements in associated points are zero-divisors obviously, and conversely, if $xm = 0$, then $x \in \mathrm{Ann}(m)$ and $\mathrm{Ann}(m)$ has an associated point $\mathfrak{q}$ by(5.2.5.16). Now x must be in $\mathfrak{q}$ and $\mathfrak{q}$ is also an associated point of M by(5.2.5.16). Cf.[Sta]05C3**?** □

Cor. (5.2.5.18). Use the prime avoidance(5.1.1.5), we can prove if R is Noetherian and M is a finite R-module, then $I \subset \mathfrak{p}$ for some $\mathfrak{p} \in WeakAss(M)$ iff I consists of zero-divisors. ⌟

Prop. (5.2.5.19) [Associated Primes and Maps]. For a ring map $\varphi : R \to S$ and a S-module M, then

$$\mathrm{Spec}(\varphi)(Ass_S(M)) \subset Ass_R(M) \subset WeakAss_R(M) \subset \mathrm{Spec}(\varphi)(WeakAss_S(M)).$$

Equalities hold if S is Noetherian. Also $WeakAss_R(M) = \mathrm{Spec}(\varphi)(WeakAss_S(M))$ if φ is a finite ring map. ⌟

Proof: Cf.[Sta]05C7, 05E1.

We prove it is equal. If $\mathfrak{p} = \mathrm{Ann}_R(m)$, then we let $I = \mathrm{Ann}_S(m)$, then $R/\mathfrak{p} \subset S/I \subset M$, so by(5.1.7.25), there is a minimal prime of S over I that are mapped to $\mathfrak{p}$, now this prime is in $Ass(S/I)$ by(5.2.5.16) and also in $Ass_S(M)$ by(5.2.5.14). □

Prop. (5.2.5.20) [Associated Primes and Localization]. Let $\varphi : \mathrm{Spec}\, S^{-1}A \to \mathrm{Spec}\, A$ and M an A-module, then

$$\mathrm{Ass}_A(S^{-1}M) = \mathrm{Spec}(\varphi)(\mathrm{WeakAsso}_{S^{-1}A}(S^{-1}M)) = \mathrm{WeakAsso}_A(M) \cap \varphi(\mathrm{Spec}(S^{-1}R)).$$

⌟

Proof: Cf.[Sta]05C9**?**.

The first equality is by(5.2.5.19). For the second, if $\mathrm{Ann}_A(x) = \mathfrak{p}$ and $\mathfrak{p} \cap S = \varnothing$, then $\mathrm{Ann}_{S^{-1}A}(x/1) = S^{-1}(\mathfrak{p})$. Conversely, if $\mathrm{Ann}_{S^{-1}A}(x/s) = S^{-1}\mathfrak{p}$, then $\mathfrak{p} \cap S = \varnothing$, and $\mathrm{Ann}_A(x) \subset S^{-1}\mathfrak{p} \cap A = \mathfrak{p}$. □

Cor. (5.2.5.21) [Associated Primes are Stalkwise]. Let R be a ring and M an R-module, $\mathfrak{p} \subset R$, then the following are equivalent:

- $\mathfrak{p} \subset WeakAss(M)$.
- $\mathfrak{p}R_{\mathfrak{p}} \subset WeakAss(M_{\mathfrak{p}})$.
- $M_{\mathfrak{p}}$ contains some element m that $\sqrt{Ann(m)} = \mathfrak{p}R_{\mathfrak{p}}$.

⌟

Proof: $1 \to 2$: $\mathfrak{p}$ is a minimal prime of $I = Ann(m)$ for some $m \in M$, so $I_{\mathfrak{p}}$ is the minimal prime of $Ann(m) \subset R_{\mathfrak{p}}$.

$2 \to 3$: As $\mathfrak{p}R_{\mathfrak{p}}$ is the maximal prime, it is the only prime over $Ann(m)$, so $\mathfrak{p}R_{\mathfrak{p}} = \sqrt{Ann(m)}$.

$3 \to 1$: This means there are some $m \in M$ that $\sqrt{I_{\mathfrak{p}}} = \mathfrak{p}R_{\mathfrak{p}}$, which means that $\mathfrak{p}$ is a minimal prime over $Ann(m)$. □

Prop. (5.2.5.22). If M is an R-module, then $M \to \prod_{\mathfrak{p} \subset WeakAss(M)} M_{\mathfrak{p}}$ is injective. ⌟

Proof: Cf.[Sta]05CB.

If $m \neq 0 \in M$, there is an associated prime $\mathfrak{p}$ of Rm(5.2.5.16), then it is an associated prime of M, and then $(x)_{\mathfrak{p}} \subset M_{\mathfrak{p}}$ is not zero. □

Def. (5.2.5.23) [Embedded Primes]. A non-minimal prime in $Ass_R(M)$ is called a **embedded prime**. Equivalently, it is an associated point that is not a generic point of $\mathrm{Supp}(M)$. ⌟

Prop. (5.2.5.24). For a reduced ring R, $WeakAss_R(R)$ is just the set of minimal primes of R. ⌟

Proof: Cf.[Sta]0EMA. □

Cor. (5.2.5.25) [Reduced Ring No Embedded Primes]. A reduced ring has no embedded primes, because it has no nilpotent elements. Hence all its associated primes are just the minimal primes. ⌟

Def. (5.2.5.26) [Unmixed Ideals]. I is called **unmixed** if primes in $\mathrm{Ass}(A/I)$ all have the same height. In particular, they don't contain each other. ⌟

Primary Decomposition

Def. (5.2.5.27). For R Noetherian, a R-module M is called **coprimary** iff it has only one associated primes. A submodule N of M is called p**-primary** iff $Ass(M/N) = \{p\}$. A ring is called p**-primary** iff (0) is p-primary.

Notice coprimary is equivalent to the following: if $a \in A$ is a zero divisor for M, then for each $x \in M$, there is a n that $a^n x = 0$, i.e. **locally nilpotent**. And for ideals in a Noetherian ring, this is equivalent to $r(I)$ is a prime. ⌟

Proof: If M is p-primary, if $x \in M$ is nonzero, then $Ass(Rx) = \{p\}$, so p is the unique minimal element of $\mathrm{Supp}(Rx) = V(\mathrm{Ann}(x))$ by(5.2.5.16). So p is the radical of $\mathrm{Ann}(x)$, i.e. $a^n x = 0$ for some n(5.2.6.2).

Conversely, we know the ideal p of locally nilpotent elements equals the union of the associated primes(5.2.5.17), so if $q \in AssM = \mathrm{Ann}(x)$, then by definition, $p \subset q$. So $p = q$, and thus $AssM = \{p\}$. □

Lemma (5.2.5.28). A primary ring has no nontrivial idempotent element, because e and $1-e$ will all belong to the same minimal ideal p. ⌟

Lemma (5.2.5.29). The intersection of p-primary submodules are p-primary. (Because there is a injection $M/Q_1 \cap Q_2 \to M/Q_1 \oplus M/Q_2$). ⌟

Lemma (5.2.5.30) [Associated Prime and Primary Decomposition]. If $N = \cap Q_i$ is an irredundant primary decomposition and if Q_i belongs to p_i, then we have $Ass(M/N) = \{p_1, \ldots, p_r\}$. ⌟

Proof: There is a injection $M/N \to M/Q_1 \oplus \ldots M/Q_r$ which shows $Ass(M/N) \subset \{p_1, \ldots, p_r\}$. And for the inverse, notice $Q_2 \cap \ldots \cap Q_r/N$ is a submodule of M/Q_1, which shows $Ass(Q_2 \cap \ldots \cap Q_r/N) = \{p_1\}$ by(5.2.5.16). □

Prop. (5.2.5.31). If N is a p-primary submodule of a R-module M, and p' is a prime ideal, then

- $N_{p'} = M_{p'}$ if $p \not\subset p'$.
- $N = M \cap N_{p'}$ if $p \subset p'$.

⌟

Proof: $M_{p'}/N_{p'} = (M/N)_{p'}$, and $Ass((M/N)_{p'}) = Ass(M/N) \cap \{\text{primes contained in } p'\} = \varnothing$ by(5.2.5.20). So $M_{p'} = M_{p'}$ by(5.2.5.16).

For the second, notice it suffices to show $M/N \to M_{p'}/N_{p'}$ is injective. But this is because $A - p'$ contains no nonzero-divisor, by(5.2.5.17). □

Cor. (5.2.5.32) [Second Uniqueness of Primary Decomposition]. For an irredundant primary decomposition $N = \cap Q_i$, if Q_1 corresponds to p_1 and p_1 is minimal in $Ass(M/N)$, then $Q_1 = M \cap N_{p_1}$. In particular, the minimal prime part of a irredundant primary decomposition is uniquely determined. ⌟

Proof: By the above proposition, there are elements u_i of Q_i, i$\neq$ 1 that are mapped to units in M_{p_1}, so $Q_1 \cdot u_2 u_3 \dots u_r$ is mapped onto the image of $Q_1 \to M_{p_1}$. Then $Q_1 = M \cap (Q_1)_{p_1} = M \cap N_{p_1}$. □

Prop. (5.2.5.33). If R is Noetherian and M is a R-module, there are p-primary submodules $Q(p)$ for each $p \in \mathrm{Ass}M$ that $(0) = \bigcap_{p \in \mathrm{Ass}M} Q(p)$. ⌟

Proof: For a $p \in AssM$, we seek $Q(p)$ to be the maximal submodule N that $p \notin AssN$. This has a maximal ideal because of Zorn and the fact $Ass(\cup N_\lambda) = \cup Ass(N_\lambda)$. Then We have $\mathrm{Ass}(M/Q(p)) = \{p\}$, otherwise there is another p', then there is a $Q'/Q(p) \cong A/p'$. Now Q' is bigger than $Q(p)$. Finally, $(0) = \bigcap_{p \in \mathrm{Ass}M} Q(p)$ because it has no associated primes. □

Cor. (5.2.5.34)[Primary Decomposition]. If M is f.g. over a Noetherian ring R, then any submodule has a primary decomposition. (Notice M has only f.m. associated primes). ⌟

Def. (5.2.5.35) [Symbolic Power]. For a prime ideal $\mathfrak{p}$ in a Noetherian ring, The n-th **symbolic power** $\mathfrak{p}^{(n)}$ is defined to be the $\mathfrak{p}$-primary component of $\mathfrak{p}^n$, who has only one minimal prime(hence one associated prime). The symbolic power is giving by $\mathfrak{p}^n A_\mathfrak{p} \cap A$ by(5.2.5.32). ⌟

6 Jacobson Radical and Nilradical

Nilradical

Def. (5.2.6.1)[Nilradical]. The **nilradical** of a commutative ring R is defined to be the ideal consisting of nilpotent elements. ⌟

Prop. (5.2.6.2). The nilradical $\mathfrak{n}$ of a ring A(5.2.6.1) is the intersection of all prime ideals. ⌟

Proof: Every nilpotent element is contained in every prime, and if a is not nilpotent, then the localization A_a is nonzero, hence there is a maximal ideal, i.e. there is a prime of A not containing a. □

Cor. (5.2.6.3). In particular, $\mathrm{Spec}\, A/\mathfrak{n} \to \mathrm{Spec}\, A$ is a homeomorphism, and $A \to A/\mathfrak{n}$ induces a bijection on idempotents and units. ⌟

Jacobson Ring

Def. (5.2.6.4) [Jacobson Ring]. A commutative ring is called **Jacobson** if every prime ideal is an intersection of maximal ideals. In particular, the Jacobson radical equals the nilradical. This is equivalent to every radical ideal is an intersection of maximal primes. ⌟

Prop. (5.2.6.5). R is Jacobson iff $\mathrm{Spec}\, R$ is Jacobson space(4.12.3.21). In particular, the closed pts are dense in any closed subsets (Hilbert's Nullstellensatz satisfied). ⌟

Proof: We need to show that a locally closed subset contains a closed pt, we assume this set is of the form $V(I) \cap D(f)$, I is radical, then $f \notin I$, then by the condition, there is a $I \subset \mathfrak{m}$ that $f \notin \mathfrak{m}$, thus the result.

Conversely, for a radical ideal, let $J = \cap_{I \subset \mathfrak{m}} \mathfrak{m}$, then J is radical and $V(J)$ is the closure of $V(I) \cap X_0$, $V(I) = V(J)$, and because they are both radical, $I = J$. □

Cor. (5.2.6.6). Being Jacobson is a local property, and quotient of Jacobson ring is Jacobson, and maximal ideals of R_f are maximal in R. (Immediate from(5.2.6.5)(4.12.3.22) and(4.12.3.23)). ⌟

Prop. (5.2.6.7). If a Jacobson ring A has f.m. maximal ideals, then it is the product of its localizations at maximal primes and $\dim A = 0$. ⌟

Proof: Any prime ideal $\mathfrak{p}$ is a finite intersection of maximal ideals, so it equals one of them, so $\dim A = 0$. Now $A/I = \oplus A/\mathfrak{m}_i$ by Chinese remainder theorem, so $\operatorname{Spec} A/I$ is discrete with n pts, so by(5.1.7.8) there are n idempotents e_i that $e_i \equiv \mathfrak{d}_{ij} \mod \mathfrak{m}_j$, $\sum e_i = 1$. Thus $R = \prod Re_i$. And Re_i is just the localization at a maximal prime. □

Lemma (5.2.6.8). If R is a Jacobson domain and $R \subset K$ where K is a field, and K is f.g. over R, then R is a field and K/R is a finite field extension. ⌟

Proof: By induction, it suffices to consider the monogenic case $A = R[a]$. So a is algebraic over quotient field of R because A is a field. Let $\sum r_i t^i$ be a polynomial satisfied by a, and let $\mathfrak{m}$ be a maximal ideal of R that $r_n \notin R$(exists because $\operatorname{rad} R = 0$). Then Nakayama says $\mathfrak{m}A \not\subseteq A$. Then $\mathfrak{m} = 0$ because A is a field, hence R is a field. □

Lemma (5.2.6.9). Let $R \subset A$ be commutative domains s.t. A is f.g. over R, then $\operatorname{rad} A = 0$ if $\operatorname{rad} R = 0$. ⌟

Proof: By induction, it suffices to consider the case $A = R[a]$. If a is transcendental over quotient field of R, then we finish by(3.6.2.12). Now assume a is algebraic over quotient field of R, let $\sum r_i t^i, \sum s_i t^i$ be the polynomials satisfied by a, b of minimal degrees, then $s_0 = -\sum_{i=1}^m s_i b^i \neq 0 \in \operatorname{rad} A$, and $r_n s_0 \neq 0$.

From the fact $\operatorname{rad} R = 0$, we can find a maximal ideal $\mathfrak{m}$ that $r_n s_0 \notin \mathfrak{m}$. Then Nakayama says

$$\mathfrak{m} \cdot S^{-1}A \not\subseteq S^{-1}A.$$

In particular, $\mathfrak{A} \not\subseteq A$. Choose a maximal ideal of A containing $\mathfrak{m}A$, then it cannot contain s_0, contradicting $s_0 \in \operatorname{rad} A$. □

Prop. (5.2.6.10) [Generalized Nullstellensatz]. If R is Jacobson and S is a finitely generated R-algebra, then:

- S is Jacobson.
- The maximal ideal of S intersect with R a maximal ideal, and the quotient ring extension is finite, (in particular algebraic).

In particular, a f.g. algebra over a ring of dimension 0, (e.g. Artinian ring or field) is Jacobson. ⌟

Proof: To show S is Jacobson, consider for any prime $\mathfrak{p} \subset A$, $A/\mathfrak{p}$ is a f.g. domain over $R/\mathfrak{p} \cap R$. Because R is Jacobson, $\operatorname{rad}(R/\mathfrak{p} \cap R) = 0$, so $\operatorname{rad}(A/\mathfrak{p}) = 0$, by(5.2.6.9). And this shows A is Jacobson.

If $\mathfrak{m}$ is maximal in S, then $R/\mathfrak{m} \cap R \to S/\mathfrak{m}$ satisfies the condition of(5.2.6.8), by(5.2.6.6), so the first two assertions are proved. □

Cor. (5.2.6.11). If R is Jacobson and $S \in \mathcal{CA}\mathrm{lg}^{\mathrm{fg}}(R)$ is reduced, then $\cap_{\mathfrak{m} \subset R \text{ maximal}} \mathfrak{m}S = 0$. ⌟

Proof: This is because

$$\bigcap_{\mathfrak{m} \subset R \text{ maximal}} \mathfrak{m}S \subset \bigcap_{\mathfrak{M} \subset S \text{ maximal}} (\mathfrak{M} \bigcap R)S \subset \bigcap_{\mathfrak{M} \subset S \text{ maximal}} \mathfrak{M} = 0.$$

□

Zariski Pairs

Def. (5.2.6.12)[Zariski Pairs]. A pair (A, I) is called a **Zariski pair** iff I is contained in the Jacobson radical of A. ⌟

Prop. (5.2.6.13). If (A, I) is a Zariski pair, then the map $A \to A/I$ induces a bijection between the idempotents. ⌟

Proof: idempotents are determined by the maximal ideals that it vanishes(5.1.7.6), and $A \to A/I$ induces a bijection on the maximal ideals. □

7 Dedekind Domains

Def. (5.2.7.1)[Dedekind Domain]. A **Dedekind domain** is an integrally-closed Noetherian domain of dimension 1. A UFD is a Dedekind domain by(5.3.5.2). ⌟

Prop. (5.2.7.2) [Characterizing]. For a domain R, the following are equivalent:

1. R is a Dedekind domain.
2. R is Noetherian and each $R_{\mathfrak{m}}$ is DVR for any maximal ideal $\mathfrak{m}$.
3. each ideal of R can be written as a product of prime ideals uniquely.

⌟

Proof: $1 \iff 2$ as normal is a stalkwise and(5.3.5.20).

$3 \to 2$: If 3 is true, then $\mathfrak{p} \neq \mathfrak{p}^2$ for each prime $\mathfrak{p}$, so choose $x \in \mathfrak{p} - \mathfrak{p}^2$, then for each $y \in \mathfrak{p}$, $(x, y) = \prod p_i$, then exactly one p_i(may assume p_1) is contained in p, so $(x, y)R_p = p_1 R_p$. Now in fact $(x)R_p = p_1 R_p$, because $(x, y^2)R_p$ is also a prime, so $y = ax + by^2$ in R_p, $(1 - by)y = ax \in (x)R_p$ is a prime, so $y \in (x)R_p$. This is for all $y \in p$, so $(x)R_p = p_1 R_p$.

Now if $(x) = \mathfrak{p}_1 \cdots p_r$, then $p_1 R_p = pR_p$, so $p_1 = p$, and p is f.g. by the lemma(5.2.7.3) below. $\mathfrak{p}$ is arbitrary, so R is Noetherian and $R_{\mathfrak{m}}$ is DVR for $\mathfrak{m}$ maximal, by(5.3.5.20).

$1 \to 3$: if 1 is true, then any ideal is a unique intersection of primary ideals, and primary ideals are their radical are different, so they are coprime(5.1.1.8), so this is in fact a unique decomposition into products of primary ideals. And any primary ideal is a power of its radical, because this is the case after localization. □

Lemma (5.2.7.3). I, J be ideals in a ring A and $IJ = (f)$ where f is a non-zero-divisor, then I, J are f.g. and finitely locally free of rank 1 as A-modules. ⌟

Proof: The second assertion implies the first, by(5.3.1.7). $f = \sum x_i y_i$, and $x_i y_i = a_i f$, so $\sum a_i = 1$ as f is non-zero-divisor. Now we show I_{a_i} as J_{a_i} is free of rank 1. Now after localization, $f = xy$, so x, y are non zero divisors. Now if $x' \in I$, then $x'y = af = axy$ for some a, so $x' = ax$. □

Fractional Ideals

Def. (5.2.7.4) [Fractional Ideals]. For A an integral domain with quotient field K, then an A-submodule M of K is called a **fractional ideal** if $xM \subset A$ for some $x \neq 0$.

Every f.g. submodule in K is a fractional ideal, and if A is Noetherian, then the converse is true, because it is of the form $x^{-1}\mathfrak{a}$. ⌟

Prop. (5.2.7.5). An A-submodule $M \subset K$ is called an **invertible ideal** if there is an A-submodule $N \subset K$ that $MN = A$. If this is the case, then M, N are f.g., because there are $\sum x_i y_i = 1$, so M is generated by x_i and N is generated by y_i. ⌟

Prop. (5.2.7.6). Invertibility is a stalkwise property. ⌟

Proof: Notice $(A:M)_\mathfrak{p}=(A_\mathfrak{p}:M_\mathfrak{p})$, and M is invertible iff $M(A:M)=A$. Then use the fact isomorphism is stalkwise(5.1.4.2). □

Lemma (5.2.7.7). A local domain A is a DVR iff every non-zero fractional ideal of A is invertible. ⌟

Proof: If is a DVR, let $\mathfrak{m}=(x)$, for any fractional ideal $M<$ let $yM\subset A=(x^r)$, then $M=(x^{r-s})$, where $v(y)=s$. Conversely, if every non-zero fractional ideal of A is invertible, then they are all f.g.(5.2.7.5), so A is Noetherian. Now it suffices to prove that every ideal of A is a power of $\mathfrak{m}$, by(5.3.5.20). If this is not true, choose a maximal element $\mathfrak{a}$ in the set of ideals that is not a power of $\mathfrak{m}$(by Noetherian), then $\mathfrak{m}^{-1}\mathfrak{a}\subset\mathfrak{m}^{-1}\mathfrak{m}=A$, and $\mathfrak{m}^{-1}\mathfrak{a}\supset\mathfrak{a}$, but it is not $\mathfrak{a}$, so $\mathfrak{m}^{-1}\mathfrak{a}=\mathfrak{m}^k$ for some k, so $\mathfrak{a}=\mathfrak{m}^{k+1}$, contradiciton. □

Prop. (5.2.7.8) [Dedekind Domain Fractional Ideals are Invertible]. An integral domain is a Dedekind domain iff every non-zero fractional ideal is invertible. ⌟

Proof: Immediate from(5.2.7.7) and(5.2.7.2)(5.2.7.6). □

Def. (5.2.7.9)[Class Group]. For an integral domain $\mathcal{O}$, denote $\mathrm{Cl}(\mathcal{O})$ the Abelian group of invertible fractional ideals of $\mathcal{O}$ modulo principal fractional ideals, called the **class group** of $\mathcal{O}$. ⌟

Prop. (5.2.7.10) [Localizations of Dedekind Domains]. Let $(\mathcal{O},F)$ be a Dedekind domain and $S\subset\operatorname{Spec}\mathcal{O}$ be a finite subset of maximal ideals of $\mathcal{O}$, let $\mathcal{O}_S$ denote the localization of $\mathcal{O}$ at all such $\mathfrak{p}_i$. Then there is an exact sequence of Abelian groups:

$$1\to\mathcal{O}^*\to\mathcal{O}_S^*\to\bigoplus_{\mathfrak{p}\in S}F^\times/\mathcal{O}_\mathfrak{p}^*\to\mathrm{Cl}(\mathcal{O})\to\mathrm{Cl}(\mathcal{O}_S)\to 1.$$

⌟

Proof: The only non-trivial map is the map $\bigoplus_{\mathfrak{p}\in S}F^*/\mathcal{O}_\mathfrak{p}^*\to\mathrm{Cl}(\mathcal{O})$ given by $(\overline{a_\mathfrak{p}})$ mapsto $\prod_{x\in S}\mathfrak{p}^{v_\mathfrak{p}(a_v)}$. □

Extensions of Dedekind Domains

References are[Neu99]Chap1.8..

Prop. (5.2.7.11) [Krull-Akizuki]. If A is a Noetherian domain of dimension 1 with fraction field K and L/K is a finite field extension, then the integral closure B of A in L is a Dedekind domain with fraction field L, and $\operatorname{Spec}B\to\operatorname{Spec}A$ is surjective, and have finite fibers and induces finite residue field extension. ⌟

Proof: Cf.[Sta]09IG or [Neu99]P77.**?** □

Cor. (5.2.7.12). The integral closure of a Dedekind domain in a finite extension fields of its quotient fields is again a Dedekind domain. ⌟

Def. (5.2.7.13) [Situation]. Let $\mathcal{O}_K$ be a Dedekind domain with quotient field K, L/K a finite field extension, and $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ in L, which is also a Dedekind domain by(5.2.7.11). ⌟

Prop. (5.2.7.14). In situation(5.2.7.13), if $\alpha_1,\dots,\alpha_n$ is a basis of L/K that is contained in $\mathcal{O}_L$, and $d=d(\alpha_1,\dots,\alpha_n)$(3.2.6.33), then

$$d\mathcal{O}_L\subset\mathcal{O}_K\{\alpha_1,\dots,\alpha_n\}.$$

⌟

Proof: For any $\alpha=a_1\alpha_1+\dots+a_n\alpha_n\in\mathcal{O}_L, a_i\in K$, α satisfies the following equations

$$\mathrm{tr}_{L/K}(\alpha_i\alpha)=\sum_j\mathrm{tr}_{L/K}(\alpha_i\alpha_j)a_j$$

for any i. Notice $\mathrm{tr}(\alpha_i\alpha)\in\mathcal{O}_K$, so $da_j\in\mathcal{O}_K$ by linear algebra. □

Prop. (5.2.7.15). In situation(5.2.7.13), if L/K is separable and $\mathcal{O}_K$ is a PID, then every f.g. $\mathcal{O}_L$-module in L is a free $\mathcal{O}_K$-module of rank $[L:K]$. In particular, $\mathrm{rank}_{\mathcal{O}_K}\mathcal{O}_L=[L:K]$. ⌟

Proof: Let $\alpha_1,\dots,\alpha_n$ be a basis of L/K that is contained in $\mathcal{O}_L$, and let $d=d(\alpha_1,\dots,\alpha_n)\neq 0$ by(3.2.6.34), then by(5.2.7.14), $d\mathcal{O}_L\subset\mathcal{O}_K\{\alpha_1,\dots,\alpha_n\}$. Notice any generator of the torsion-free module $\mathcal{O}_L$ over $\mathcal{O}_K$ is a generator of the field L/K, so $\mathrm{rank}_{\mathcal{O}_K}\mathcal{O}_L\geq[L:K]$. Now if $M\subset L$ is a free $\mathcal{O}_L$-module with a set of generators $\mu_1,\dots,\mu_r$, then we can take $a\in\mathcal{O}_K$ s.t. $a\mu_i\in\mathcal{O}_L$. Then

$$adM\subset d\mathcal{O}_L\subset\mathcal{O}_K\{\alpha_1,\dots,\alpha_n\}.$$

And then

$$[L:K]\leq\mathrm{rank}_{\mathcal{O}_K}\mathcal{O}_L\leq\mathrm{rank}_{\mathcal{O}_K}M=\mathrm{rank}_{\mathcal{O}_K}(adM)\leq[L:K].$$

and the assertion follows. □

Prop. (5.2.7.16) [Integral Basis of Joins]. In situation(5.2.7.13), if $L/K, L'/K$ are two Galois extensions in $\overline{K}$ s.t. $L\cap L'=K$, and let $\omega_1,\dots,\omega_n$(resp. $\omega_1',\dots,\omega_{n'}'$) be an integral basis of L/K(resp. L'/K) with discriminants d(resp. d')(3.2.6.33). Suppose that $(d,d')=\mathcal{O}_K$, then $\omega_i\omega_j'$ is an integral basis of LL'/K with discriminant $d^{n'}(d')^n$. ⌟

Proof: The hypothesis implies that $[LL':K]=nn'$, so $\{\omega_i\omega_j'\}$ is a basis of LL'/K that is integral. To show it is an integral basis, if $\alpha=\sum_{i,j}a_{ij}\omega_i\omega_j'\in\mathcal{O}_{LL'}$, we need to show that $a_{ij}\in\mathcal{O}_K$. Let $\beta_i=\sum a_{ij}\omega_i$, and let $\mathrm{Gal}(LL'/L')=\{\sigma_1,\dots,\sigma_n\}$, $\mathrm{Gal}(LL'/L)=\{\sigma_1',\dots,\sigma_{n'}'\}$,

$$T=(\sigma_i'\omega_j')_{i,j},\quad \underline{a}=(\sigma_1'\alpha,\dots,\sigma_{n'}'\alpha)^t,\quad \underline{b}=(\beta_1,\dots,\beta_{n'})^t,$$

then $\det(T)^2=d'$, and $\underline{a}=T\underline{b}$. So $\det(T)\underline{a}=T^*\underline{b}$ has integral entries, and $d'b$ is integral. Thus $d'a_{ij}\in\mathcal{O}_K$ for each i,j. Dually, $da_{ij}\in\mathcal{O}_K$. Thus by hypothesis, $a_{ij}\in\mathcal{O}_K$.

To calculate the discriminant,

$$d=d(\{\omega_i\omega_j'\})=\det(\{\sigma_k\sigma_l'\omega_i\omega_j'\}_{k,\ell,i,j})^2=\det((\sigma_k\omega_i)_{k,i}\otimes(\sigma_l'\omega_j')_{l,j})^2=\det((\sigma_k\omega_i)_{k,i})^{2n'}\det((\sigma_l'\omega_j')_{l,j})^{2n}=d^{n'}(d')^n.$$

□

Def. (5.2.7.17) [Conductors]. Let $R\subset S\in\mathcal{CR}\mathrm{ing}$ the **conductor of** R in S is defined to

$$\mathfrak{c}=\{\alpha\in R|\alpha S\subset R\}.$$

And if (R,K) is an integral domain, the **conductor of** R is defined to be the conductor of R in the integral closure of R w.r.t. K. ⌟

Prop. (5.2.7.18). Let R be a Noetherian integral domain with integral closure S, then the conductor of R in S is nonzero iff S is f.g. as a R-module. ⌟

Proof: This follows from(5.2.7.4). □

Def. (5.2.7.19)[Conductors of an Element]. In situation(5.2.7.13) and $\alpha \in \mathcal{O}_L$, then the **conductor of** α w.r.t K is the conductor of $\mathcal{O}_K[\alpha]$ in $\mathcal{O}_L$, denoted by $\mathfrak{d}(\alpha)$. It is non-zero by(5.2.7.4) as $\mathcal{O}_L$ is f.g. over $\mathcal{O}_K[\alpha]$. ⌟

Prop. (5.2.7.20)[Inertia and Ramification]. Situation as in(5.2.7.13), let $\mathfrak{p}$ be a maximal prime of $\mathcal{O}_K$, then $\mathfrak{p}\mathcal{O}_L \cap \mathcal{O}_L$ by(5.2.1.5). Let $\mathfrak{p}\mathcal{O} = \prod_i \mathfrak{P}_i^{e_i}$ be a decomposition. Denote e_i the **ramification degree** of $\mathfrak{P}_i$ over $\mathfrak{p}$, and $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathfrak{O}_K/\mathfrak{p}]$ the **inertia degree** of $\mathfrak{P}_i$ over $\mathfrak{p}$. ⌟

Prop. (5.2.7.21)[Fundamental Identity]. Situation as in(5.2.7.13), if $\mathcal{O}_L$ is a finite $\mathcal{O}_K$-module, then for any $\mathfrak{p} = \prod_i \mathfrak{P}_i^{e_i}$,

$$\sum e_i f_i = [L : K].$$

In particular, this applies to the case that L/K is separable. ⌟

Proof: By hypothesis, $\mathcal{O}_{L,\mathfrak{p}}$ is a finite $\mathcal{O}_{K,\mathfrak{p}}$-module of rank $[L : K]$, thus $\mathcal{O}_L/\mathfrak{p}$ is an $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_L$-module of rank n. Notice there is an isomorphism $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \prod_i \mathcal{O}_L/\mathfrak{P}_i^{e_i}$, thus

$$[L : K] = \sum_i \dim_{\mathcal{O}_L/\mathfrak{p}} \mathcal{O}_L/\mathfrak{P}_i^{e_i} = \sum_i e_i f_i.$$

If L/K is separable, let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of L/K with $\alpha_i \in \mathcal{O}_K$, then as $d(\alpha_1, \ldots, \alpha_n) \neq 0$ by(3.2.6.34), $\mathcal{O}_L \subset d^{-1}(\alpha_1\mathcal{O}_K + \ldots + \alpha_n\mathcal{O}_K)$ by(5.2.7.14). So it is a finite $\mathcal{O}_K$-module, as $\mathcal{O}_K$ is Noetherian. □

Prop. (5.2.7.22) [Decompositions in a Galois Extension]. Situation as in(5.2.7.13), if L/K is Galois, then for any $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$, $\mathrm{Gal}(L/K)$ acts transitively on the set of primes over $\mathfrak{p}$. ⌟

Proof: If $\mathfrak{P}, \mathfrak{P}'$ are two primes over $\mathfrak{p}$ but $\mathfrak{P}' \neq \sigma\mathfrak{P}$ for any $\sigma \in \mathrm{Gal}(L/K)$, then by Chinese remainder theorem, there exists $x \in \mathcal{O}_L$ s.t.

$$x \equiv 0 \mod \mathfrak{P}', \quad x \equiv 1 \mod \sigma\mathfrak{P}, \forall \sigma \in \mathrm{Gal}(L/K).$$

But then $\mathrm{Nm}_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \in \mathfrak{P}' \cap \mathfrak{O}_K = \mathfrak{p}$, but none of $\sigma(x)$ is in $\mathfrak{P}$, so $\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x) \notin \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, contradiction. □

Thm. (5.2.7.23) [Dedekind-Kummer]. Situation as in(5.2.7.13), suppose $L = K(\theta)$, where $\theta \in \mathcal{O}_L$ has minimal polynomials $p(X) \in \mathcal{O}_K[X]$(such a θ exists if L/K is separable, by(3.2.6.20)). Let $\mathfrak{d}$ be the conductor of θ, then for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ prime to $\mathfrak{d}$, let

$$\overline{p}(X) = \prod_i \overline{p}_i(X)^{e_i}$$

be the decomposition of $\overline{p}(X)$ into irreducible factors in $\mathcal{O}_K/\mathfrak{p}[X]$, where $\mathfrak{p}_i(X) \in \mathcal{O}_K[X]$ are monic polynomials, then

- $\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}_L$ are different primes ideals in $\mathcal{O}_L$.
- $\mathfrak{p}\mathcal{O}_L = \prod_i \mathfrak{P}_i^{e_i}$.
- The inertia degree f_i equals $\deg(\overline{p}_i(X))$.

⌟

Proof: Cf.[Neu99]P48. □

Def. (5.2.7.24) [Ramification Notations]. Situation as in(5.2.7.20), let $\mathfrak{p}\mathcal{O} = \prod_i \mathfrak{P}_i^{e_i}$, then

- **splits completely in** L if $r = [L : K]$.
- $\mathfrak{p}$ is **non-split in** L if $r = 1$.
- $\mathfrak{P}_i$ is **unramified over** $\mathfrak{p}$ if $e_i = 1$ and the residue fields extension $(\mathcal{O}_L/\mathfrak{P}_i)/(\mathcal{O}_K/\mathfrak{p})$ is separable.
- $\mathfrak{P}_i$ is **ramified in over** $\mathfrak{p}$ if it is not unramified over $\mathfrak{p}$.
- $\mathfrak{P}_i$ is **totally ramified over** $\mathfrak{p}$ if it is ramified over $\mathfrak{p}$ and $f_i = 1$.
- $\mathfrak{p}$ is called **unramified in** L if all $\mathfrak{P}_i$ are unramified over $\mathfrak{p}$.
- L/K is called a **unramified extension** if all primes of $\mathcal{O}_K$ are unramified.

⌟

Prop. (5.2.7.25) [Almost Every Prime is Unramified]. Situation as in(5.2.7.23), then a.e. prime $\mathfrak{p}$ of $\mathcal{O}_K$ is unramified in L, by(5.2.7.39). ⌟

Prop. (5.2.7.26). Situation as in(5.2.7.13), $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{K,\mathfrak{p}} = \prod_i \mathcal{O}_{L,\mathfrak{P}_i}$. ⌟

Proof: Cf.[MIT notes, 11.7]. □

Prop. (5.2.7.27). If a prime $\mathfrak{p}$ splits completely in two separable extension LM of K, then it also splits completely in the composite LM. ⌟

Proof: We use the language of valuation. The extension of a valuation v of K corresponds to the set of equivalent classes of algebra map from L to $\overline{K_v}$ module conjugacy over K_v. So We only need to show that two different maps of LM are not conjugate over K_v. But the restrict of them to L or M is different, thus not conjugate over K_v by the assumption. □

Cor. (5.2.7.28). A prime splits completely in a separable extension L if it splits completely in the Galois closure N of L. ⌟

Proof: This is because the Galois closure is the composite of the conjugates of L. □

Differents and Discriminants

Def. (5.2.7.29) [Differents]. Let L/K be a finite separable field extension with separable residue field extension, and $\mathcal{O}_K$ is a Dedekind domain with integral closure $\mathcal{O}_L$ in L, there is a **trace form** on L: $(x, y) \to \mathrm{tr}(xy)$, which is non-degenerate.

We define the **dual module** for a fractional ideal I as $I^\vee = \{x \in L | \mathrm{tr}(xI) \in \mathcal{O}_K\}$. This is truly a fractional ideal because if $\alpha_i \in \mathcal{O}_L$ is a basis of L/K, and let $d = \det(\mathrm{tr}(\alpha_i\alpha_j))$, then for any $a \in I \cap \mathcal{O}_L$, $ad \cdot I^\vee \in \mathcal{O}_L$, because if $x = \sum x_i\alpha_i \in I^\vee$, then $\sum ax_i \,\mathrm{tr}(\alpha_i\alpha_j) = \mathrm{tr}(xa\alpha_j) \in \mathcal{O}_K$, so solve the equation shows $dax_i \in \mathcal{O}_K$.

The **different of** K/L is defined to be $\mathfrak{D}_{L/K} = ((\mathcal{O}_L)^\vee)^{-1}$. ⌟

Prop. (5.2.7.30) [Properties of Differents]. Different is compatible with composition, localization w.r.t. a prime ideal and completion. ⌟

Proof: Cf.[Neu99]P195. □

Cor. (5.2.7.31). $\mathfrak{D}_{L/K} = \prod_{\mathfrak{P}} \mathfrak{D}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$. ⌟

Prop. (5.2.7.32). If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, then $\mathfrak{D}_{L/K} = (f'(\alpha))$, where $f(X) = \mathrm{Irr}(\alpha, K; X)$. ⌟

Proof: By(3.2.6.30), if $f(X)/(X-\alpha) = \beta_0 + \beta_1 X + \ldots + \beta_{n-1}X^{n-1}$, then $\mathcal{O}_L^\vee = f'(\alpha)^{-1}(\beta_0, \ldots, \beta_{n-1})$. Now the result follows if $(\beta_0, \ldots, \beta_{n-1}) = \mathcal{O}_L$, which is easy to see if we write β_i as polynomials of α. □

Cor. (5.2.7.33). If L/K is finite separable extension of local fields, then

$$v_L(\mathfrak{D}_{L/K}) = \sum_{\sigma\in G, \sigma\neq 1} i_{L/K}(\sigma) = \int_{-1}^{\infty} (|G(L/K)_t| - 1)dt.$$

Notation as in(14.2.2.22). ⌟

Prop. (5.2.7.34) [Different as Annihilator of Kähler Differential]. The different $\mathfrak{D}_{L/K}$ is the annihilator of $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$. ⌟

Proof: It suffices to show the exact sequence

$$0 \to \mathfrak{D}_{L/K} \to \mathcal{O}_L \to \Omega_{\mathcal{O}_L/\mathcal{O}_K},$$

but because exactness is stalkwise(5.1.4.2), we can localized at a maximal ideal, then by(14.2.2.2), $\mathcal{O}_L = \mathcal{O}_K[x]$ is monogenous, thus $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$ is cyclic, and the annihilator of dx is $f'(x)$. So by(5.2.7.32) we are done. □

Prop. (5.2.7.35)[Ramification and Different]. A prime ideal $\mathfrak{P}$ of L is ramified over K iff $\mathfrak{P} \mid \mathfrak{D}_{L/K}$.

Let e be the ramification of $\mathfrak{P}$, then the power s of $\mathfrak{P}$ in $\mathfrak{D}_{L/K}$ is

$$\begin{cases} s = e-1 & \mathfrak{P} \text{ tamely ramified} \\ e \leq s \leq e - 1 + v_{\mathfrak{P}}(e) & \mathfrak{P} \text{ wildly ramified} \end{cases}.$$

⌟

Proof: Cf.[Neu99]P199. □

Def. (5.2.7.36)[Discriminants]. Let the situation the same as in(5.2.7.29), the **discriminant of field extension** L/K is defined to be the set $\mathfrak{d}_{L/K}$ consisting of discriminants $d(\alpha_1, \ldots, \alpha_n)$(3.2.6.33) where $\{\alpha_i\}$ is a basis of L/K s.t. $\alpha_i \in \mathcal{O}_L$.

Because $d(\alpha_1, \ldots, \alpha_n) \subset \mathcal{O}_K$ and $\mathrm{tr}_{L/K}$ is $\mathcal{O}_K$-linear, $\mathfrak{d}_{L/K}$ is an ideal of $\mathcal{O}_K$. ⌟

Prop. (5.2.7.37) [Differents and Discriminants].

$$\mathfrak{d}_{L/K} = \mathrm{Nm}_{L/K}\, \mathfrak{D}_{L/K}.$$

⌟

Proof: Cf.[Neu99]P201. □

Cor. (5.2.7.38) [Compositions and Discriminants]. For field extensions $M/L/K \in \texttt{Field}$, we have

$$\mathfrak{d}_{M/K} = \mathfrak{d}_{L/K}^{[M:L]} N_{L/K}(\mathfrak{d}_{M/L}).$$

⌟

Proof: Apply $\mathrm{Nm}_{M/K} = \mathrm{Nm}_{L/K} \circ \mathrm{Nm}_{M/L}$ to the equation $\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L}\mathfrak{D}_{L/K}$(5.2.7.30), we get

$$\mathfrak{d}_{M/K} = N_{L/K}(\mathfrak{d}_{M/L}) N_{L/K}(\mathfrak{D}_{L/K}^{[M:L]}) = N_{L/K}(\mathfrak{d}_{M/L})\mathfrak{d}_{L/K}^{[M:L]}.$$

□

Cor. (5.2.7.39) [Ramification and Discriminant]. Let L/K be a separable finite field extension, then a prime ideal $\mathfrak{p}$ of K ramifies in L iff $\mathfrak{p}|\mathfrak{d}_{L/K}$.

In particular, only f.m. primes are ramified in L/K, and the extension is unramified iff $\mathfrak{d}_{L/K} = 1$. ⌟

Proof: This follows from(5.2.7.35) and(5.2.7.37). □

Cor. (5.2.7.40). $\mathfrak{d}_{L/K} = \prod_{\mathfrak{P}} \mathfrak{d}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$. ⌟

Proof: This follows from(5.2.7.31) and(5.2.7.37). □

5.3 Commutative Algebra III

1 Projective

References are [Projective Modules], [Sta]and[Vak17].

Def. (5.3.1.1) [Projective Modules]. A module P over a ring R is called **projective** iff $\mathrm{Hom}(P,-)$ is exact, or equivalent, for any surjective map of modules $F \to Q \to 0$, $\mathrm{Hom}(P,F) \to \mathrm{Hom}(P,Q)$ is surjective. ⌟

Prop. (5.3.1.2). Localization and tensor product preserves projective because they are left adjoints.

And when tensoring f.f. map, then the converse is also true(5.4.2.1). ⌟

Prop. (5.3.1.3). A module over a ring is projective iff it is a direct summand of a free module, in particular, it is flat. Moreover, there is a free module Q that $P \oplus Q = F$ free. ⌟

Proof: For the second assertion, we can choose an arbitrary Q that $P \oplus Q$ free, and see $\bigoplus_{\mathbb{N}}(P \oplus Q)$ is free. □

Lemma (5.3.1.4). A projective module is a direct sum of countably generated projective modules. ⌟

Proof: This follows from(3.2.4.28). □

Prop. (5.3.1.5) [Projective over Local Ring]. A projective module P over a local ring R or a PID is free. ⌟

Proof: Local ring case: By(5.3.1.4) and(3.2.4.29), it suffices to show that any element x of P is contained in a free direct summand of P. Because P is projective, it is a direct summand of a free module F, $F = P \oplus Q$. Let B be a basis of F that the number of basis element in the expression of x is minimal. Let $x = \sum a_i e_i$. Then no a_i is contained in the ideal generated by other a_j, otherwise we can choose another basis to show this is minimal. Let $e_i = y_i + c_i$ be decompositions into P and Q components, and write $y_i = \sum a_{ij} e_i + t_i$, where t_i is combination of elements in B other than e_i. Now it suffices to show $\det(a_{ij})$ is invertible, because in this way $\{y_i\} \cup (B \backslash \{x_1\})$ is a basis of F and $x = \sum a_i y_i$ because $x \in P$. And $N = \mathit{span}\{y_i\}$ is a summand of P because $N \subset P$ and both N, P are summands of F.

To show $\det(a_{ij})$ is invertible, notice that by plugging $y_i = \sum b_{ij} e_j + t_i$ into $\sum a_i e_i = \sum a_i y_i$ shows $a_j = \sum a_i a_{ij}$, thus by the argument before, a_{ij} are non-invertible for $i \neq j$ and $1 - a_{ii}$ is non-invertible, so a_{ii} is invertible. Because R is a local ring, we can easily see $\det(a_{ij})$ is invertible.

PID case: directly from(3.2.4.21). □

Prop. (5.3.1.6). If R is a ring and I is nilpotent ideal and $\overline{P}$ is a projective R/I-module, then there exists a projective R-module P that $P/IP \cong \overline{P}$. ⌟

Proof: Cf.[Sta]P07LV. □

Finite Projective Modules

Prop. (5.3.1.7) [Finite Projective Modules]. Let M be a R-module, the following are equivalent:

1. M is finite projective.
2. M is f.p. and flat.

3. M is f.p. and all its localizations at (maximal)primes are free.
4. M is finite locally free.
5. M is finite and locally free.
6. M is finite and all its localizations at primes are free and the function $p \to \dim_{k(p)} M \otimes_R k(p)$ is a locally constant function on $\operatorname{Spec} R$.

⌟

Proof: $1 \to 2$: $M \otimes K = R^m$ for some K and m, so K is finite and $M = R^m/K$ is f.p. And M is flat because it is a summand of R^n(5.4.1.4).

$2 \to 4$: For any prime p, choose a basis for the $k(p)$-vector space $M \otimes k(p)$, then by Nakayama, their inverse image generate M_g for some $g \notin p$(3.2.4.8), and the kernel K of this generation is finite because M_g is f.p. And $K \otimes k(p) = 0$ by the flatness of M_g. Then by Nakayama again there is a $g' \notin p$ that $M_{gg'} = 0$(3.2.4.8).

$4 \to 3$: Because f.p. is local(5.1.4.4).

$3 \to 2$: Because flatness is trivial.

$4 \to 5$: Because finite is local(5.1.4.4).

$5 \to 4, 4 \to 6$: Trivial.

$6 \to 4$: Cf.[Sta]00NX.?

$2 + 3 + 4 + 5 + 6 \to 1$: Cf.[Sta]00NX.?

Consider the stalk, it is all free by(5.3.1.2) and(5.3.1.5), thus by(6.5.1.38), it is locally free. □

Cor. (5.3.1.8) [Partially Stalkwise]. If P is fo f.p., then finite projectiveness is a stalkwise property for P. ⌟

Cor. (5.3.1.9) [Projective and Flat]. A finite module over a Noetherian ring is projective iff it is flat. ⌟

Cor. (5.3.1.10). If M is finite projective, then the canonical map $\operatorname{Hom}(M, N) \otimes L \to \operatorname{Hom}(M, N \otimes L)$ is an isomorphism. ⌟

Proof: By proposition above M is f.p. and finite locally free, so by(5.3.7.7) and tensor commutes with localization, we can check locally, where M is finite free so the isomorphism is obvious. □

Def. (5.3.1.11) [Characteristic Polynomials for Finite Projective Modules]. Let M be a finite projective module over a ring A. then we can define a characteristic polynomial in $A[X]$ for any map of A-modules $M \to M$: if M is free, then this map is defined as usual. In general, we can find an open covering $\operatorname{Spec} A_{f_i}$ of $\operatorname{Spec} A$ that M_{f_i} is free over A_{f_i}. Thus we can define the characteristic polynomial locally and glue them together to get a characteristic polynomial in $A[X]$.

In particular, we can also define trace and norm of a A-module map $M \to M$. And when B is a locally free A-algebra, then there are trace and norm maps $\operatorname{tr}: B \to A$ and $Nm: B \to A$. ⌟

Prop. (5.3.1.12). Let R be a ring and I be a locally nilpotent ideal. If $\overline{P}$ is a finite projective module over R/I, then there exists a finite projective R-module P that $P/IP \cong \overline{P}$. ⌟

Proof: Cf.[Sta]0D47. □

Prop. (5.3.1.13). Let M be a R module and I a nilpotent ideal of R. If M/IM is a projective R/I-module and M is flat over R, then M is a projective R-module. ⌟

Proof: Cf.[Sta]05CG. □

Thm. (5.3.1.14) [Serre-Suslin]. Every finite projective module over the polynomial ring $k[x_1, \ldots, x_n]$ is free. ⌟

Proof: Cf.[?]P850.**?** □

Duality of Projective Modules

Prop. (5.3.1.15) [Basis Criterion of Projectiveness]. An A-module P is projective iff there are elements x_i in P and f_i in P^* that for any x, $f_i(x) = 0$ a.e. i, and $\sum f_i(x)x_i = x$. Moreover, P is finite projective iff there are f.m. of them. ⌟

Proof: If P is projective, as a summand of a free module, then we can choose the coordinates of the inclusion map as f_i, and choose the image of the quotient map of the coordinate as x_i. The converse is verbatim. □

Cor. (5.3.1.16) [Finite Projective Duality]. If P is projective, then $P \to P^{**}$ is injective, and if P is finite projective, then it is an isomorphism. ⌟

Proof: If $f(x) = 0$ for all $f \in P^*$, then the proposition says $x = 0$. And if P is finite projective, it can be seen x_i, f_i forms a "basis" of P^*(finiteness used), so f_i generate P^*, and similarly x_i generate P^*, so $P \to P^{**}$ is surjective. □

Cor. (5.3.1.17). If P is projective over R, then $P^* \neq 0$. ⌟

Cor. (5.3.1.18). In the meanwhile of the proof, we already get: if P is finite projective, then P^* is finite projective, by(5.3.1.15). ⌟

Cor. (5.3.1.19). If P is finite projective, the the map $P \otimes M \to \mathrm{Hom}(P^*, M)$ is an isomorphism. ⌟

Proof: In(5.3.1.10), let $N = R$ and let $M = P^*$, then use the fact $P \cong P^{**}$. □

Thm. (5.3.1.20) [Quillen-Suslin]. For $k \in$ `Field`, any finite projective module over $k[X_1, \ldots, X_k]$ is free. (Highly nontrivial). ⌟

Proof: Cf.[?]P850. □

Prop. (5.3.1.21). $\prod^{\mathbb{N}} \mathbb{Z}$ is not free over $\mathbb{Z}$, by(3.1.3.4). ⌟

2 Injective

Prop. (5.3.2.1) [Baer's Criterion]. A right $R-$module I is injective iff for every right ideal J of R, every map $J \to I$ can be extended to a map $R \to I$. (Directly from (4.8.8.7)). ⌟

Cor. (5.3.2.2). A module over a PID is injective iff it is divisible. ⌟

Cor. (5.3.2.3). A is injective iff $\mathrm{Ext}^1(R/I, A) = 0$ for every ideal I of R. ⌟

Cor. (5.3.2.4) [Rank]. Let M a finite projective R-module, then M is said to have rank n if $M/\mathfrak{m}M$ is of rank n over the field $R/\mathfrak{m}$ for any arbitrary maximal ideal $\mathfrak{m}$ of R. ⌟

Prop. (5.3.2.5). The category of R-mod has enough injectives by(4.8.3.28), and it has enough projectives trivially. ⌟

Prop. (5.3.2.6). If I is an injective A-module, then for any ideal α of A, $\Gamma_\alpha(I) = \{m|\alpha^n m = 0\}$ for some n is injective. ⌟

Proof: Use Baer criterion, for any ideal b of A, it is f.g. so there is a n that $\phi(\alpha^n b) = 0$, and Artin-Rees tells us that $\phi(\alpha^N \cap b) = 0$ for some N. So we have an extension of ϕ over $b/b \cap \alpha^N$ to $A/\alpha^N \to I$, and this obviously factor through $\Gamma_\alpha(I)$, so it is done. □

Prop. (5.3.2.7). For an injective module A-module I, $I \to I_f$ is surjective. ⌟

Proof: we have the sheaf of modules $\widetilde{I}$ is flabby(6.7.1.5), thus the map to the stalk is surjective. □

Pontryagin Duality

Basic references are [Weibel Homological Algebra].

Def. (5.3.2.8). The **Pontryagin dual** $M^\vee$ of a left R-module M is the right R-module $\mathrm{Hom}_{Ab}(M, \mathbb{Q}/\mathbb{Z})$, where $(fr)(b) = f(rb)$.

It is easily verified that if $A \neq 0$, then $A^\vee \neq 0$, and $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, thus the Pontryagin dual is faithfully exact. ⌟

Prop. (5.3.2.9). M is flat R-module iff $M^\vee$ is an injective right R-module (Because $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$ is exact). ⌟

3 Homological Dimension

Def. (5.3.3.1). For a R-mod A, the **projective dimension** $\mathrm{pd}(A)$ is the minimal length of a projective resolution of A. The **injective dimension** $\mathrm{id}(A)$ is the minimal length of a injective resolution of A. The **flat dimension** $\mathrm{fd}(A)$ is the minimal length of a flat resolution of A. ⌟

Prop. (5.3.3.2). If R is Noetherian, then $fd(A) = pd(A)$ for every f.g. module A. ⌟

Proof: Use(5.3.3.3), we see that if we choose a syzygy and look at the n-th term, then it is f.p and flat, so we have it is projective by(5.4.1.14). □

Lemma (5.3.3.3) [pd]. If $\mathrm{Ext}^{d+1}(A, B) = 0$ for every B, then for every resolution

$$0 \to M \to P_{d-1} \to \ldots, P_1 \to P_0 \to A \to 0$$

where P_k is projective, then M is projective. Hence we have $pd(A) \leq d$. (Use dimension shifting, the following two are the same). ⌟

Lemma (5.3.3.4) [id]. If $\mathrm{Ext}^{d+1}(A, B) = 0$ for every A, then for every resolution

$$0 \to B \to P_0 \to \ldots, P_{n-1} \to M \to 0$$

where P_k is injectives, then M is injective. Hence we have $id(B) \leq d$ ⌟

Lemma (5.3.3.5) [fd]. If $\mathrm{Tor}_{d+1}(A, B) = 0$ for every B, then for every resolution

$$0 \to M \to F_{d-1} \to \ldots, F_1 \to F_0 \to A \to 0$$

where F_k is flat, then M is flat. Hence we have $fd(A) \leq d$ ⌟

Prop. (5.3.3.6)[Global Dimension Theorem]. The following are the same for any ring R and called the **left global dimension** of R:

1. $\sup\{id(B)\}$
2. $\sup\{pd(A)\}$
3. $\sup\{pd(R/I)\}$
4. $\sup\{d : \mathrm{Ext}^d_R(A, B) \neq 0$ for some module A,B.

⌟

Proof: This follows from(5.3.3.3),(5.3.3.4) and (5.3.2.3). □

Prop. (5.3.3.7). A $\mathbb{Z}$ has global dimension 1 because injective is equivalent to divisible, and this shows that a quotient of an injective is injective. ⌟

Prop. (5.3.3.8) [Tor Dimension Theorem]. The following are the same for any ring R and called the **Tor dimension** of R:

1. $\sup\{fd(A)\}$ for A a left module.
2. $\sup\{fd(B)\}$ for B a right module.
3. $\sup\{pd(R/I)\}$ for I a left ideal.
4. $\sup\{pd(R/J)\}$ for J a right ideal.
5. $\sup\{d : \mathrm{Tor}^R_d(A, B) \neq 0$ for some module A,B.

⌟

Proof: This follows from(5.3.3.5) applied to R and R^{op} and also(5.4.1.2). □

Prop. (5.3.3.9)[Change of Rings]. Let $S \to R$ be a ring map, let $A \in \mathcal{M}\mathrm{od}_R$, then we have $pd_S(A) \leq pd_R(A) + pd_S(R)$. ⌟

Proof: Use the Cartan-Eilenberg resolution and the total complex has length $pd_R(A) + pd_S(R)$. □

4 Depth

Regular sequences

Def. (5.3.4.1) [Regular Sequences]. If R is a commutative ring and M is an R-module, then a sequence $(f_1, \ldots, f_n)$ of elements of R is called a **M-regular sequence** if f_k is a nonzero-divisor of $M/(f_1, \ldots, f_{k-1})$ and $M/(f_1, \ldots, f_n) \neq 0$. If $M = R$, then it is simply called a **regular sequence**. ⌟

Prop. (5.3.4.2). If R is a **local ring**, M a finite R-module, and $(f_1, \ldots, f_n)$ is a M-regular sequence, then a permutation of this sequence is also an M-regular sequence. ⌟

Proof: By transposition of adjacent indices, we can assume $n = 2$. Then x is a non-zero-divisor, and $x \in \mathfrak{m}$, so Now (x, y) is an M-regular sequence iff $M \otimes^L_R R/x$ is discrete and $M \otimes^L R/x \otimes^L_R R/y$ is discrete. Then it suffices to prove y is injective on M: If $ym = 0$, then $m = xm'$ for some m', because y is injective on M/x, and then $ym' = 0$ also because x is injective on M. Then x is surjective on $\ker(y)$, thus $\ker(y) = 0$ by Nakayama. □

Prop. (5.3.4.3). Let R be a ring and $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of R-modules. Then if a sequence $(f_1, \ldots, f_r) \in R^r$ is both M_1-regular and M_3-regular, then it is also M_2-regular. ⌟

Proof: Use the snake lemma, $\ker(f_1|_M) = 0$, and $0 \to M_1/fM_1 \to M_2/fM_2 \to M_3/fM_3 \to 0$, then use induction. □

Prop. (5.3.4.4). For any integers $e_i \geq 1$, $(f_1, \ldots, f_n)$ is a M-regular iff $(f_1^{e_1}, \ldots, f_n^{e_n})$ is M-regular. ⌟

Proof: Use induction on n. $n = 1$ is trivial, and it suffices to show that $(f_1^e, f_2, \ldots, f_n)$ is M-regular. Then we use induction on e: There is an exact sequence $0 \to M/f_1M \to M/f_1^eM \to M/f^{e-1}M \to 0$, so by(5.3.4.3), if $(f_1, \ldots, f_n)$ is a M-regular, then $(f_1^e, f_2, \ldots, f_n)$ is M-regular. Conversely, if $(f_1^e, f_2, \ldots, f_n)$ is M-regular, then f_2 is injective on M/f_1^eM, so also injective on M/f_1M, thus injective on $M/f^{e-1}M$ by induction hypothesis, and also there is a further exact sequence $0 \to M/(f_1, f_2)M \to M/(f_1^e, f_2)M \to M/(f^{e-1}, f_2)M \to 0$, so we can consider f_3, and then so on, thus show $(f_1^e, f_2, \ldots, f_n)$ is M-regular. □

Prop. (5.3.4.5). Let R be a ring, then the following are equivaletn:

- any permutation of $(f_1, \ldots, f_r)$ is a regular sequence.
- Any subsequence of $(f_1, \ldots, f_r)$ is a regular sequence.
- $(f_1X_1, \ldots, f_rX_r)$ is a regular sequence of $R[X]$.

⌟

Proof: $1 \to 2$: Trivial. $2 \to 1$: Use induction on r: If $r = 2$ and (x, y) is regular, we have $M \otimes_R^L R/x, M \otimes_R^L R/y$ are both discrete, and $M \otimes_R^L R/x \otimes^L R/y$ is also discrete, thus $M \otimes_R^L R/y \otimes_R^L R/x$ is also discrete and (y, x) is regular. For $r > 2$, it suffices to show $f_{\sigma(r)}$ is regular in $M/(f_{\sigma(1)}, \ldots, f_{\sigma(r-1)})$. If $\sigma(r) = r$, then we are done, otherwise, f_r and $f_{\sigma(r)}$ are both injective on $M/(f_1, \ldots, \widehat{f_{\sigma(r)}}, \ldots, f_{r-1})$ by induction hypothesis, and $(f_{\sigma(r)}, f_r)$ is a regular sequence for this ring, then so is $(f_r, f_{\sigma(r)})$ by the $r = 2$ case, thus we are done.

$3 \iff 2$: Notice as a R-module, $R[X_1, \ldots, X_r]/(f_1X_1, \ldots, f_iX_i)$ is a direct sum of the modules $R/I_E X_1^{e_1} \ldots X_r^{e_r}$, where I_E is generated by those f_j that $j \leq i$ and $e_j > 0$. Then $f_{i+1}X_{i+1}$ is injective on this iff f_{i+1} is injective on R/I_E for any E. Then it is clear that this is equivalent to 2. □

Def. (5.3.4.6) [Quasi-Regular Sequence]. Let $f_1, \ldots, f_c \in R$ and $J = (f_1, \ldots, f_c)$, let M be a R-module, then there is a canonical map $M/JM \otimes_{R/J} R/J[X_1, \ldots, X_c] \to \otimes_{n \geq 0} J^n M/J^{n+1}M$. Then $(f_1, \ldots, f_c)$ is called ***M*-quasi-regular sequence** iff this is an isomorphism. ⌟

Depth

Prop. (5.3.4.7) [Rees]. For a f.g. module M and $IM \neq M$,

$$\mathrm{depth}_I(M) = \min\{i |\, \mathrm{Ext}^i_A(A/I, M) \neq 0\} = \min\{i |\, \mathrm{Ext}^i_A(N, M) \neq 0\}$$

where $\mathrm{depth}_I(M)$ is the length of the maximal M-regular sequence in I, N is a finite A-module with $\mathrm{Supp}(N) \subset V(I)$. ⌟

Proof: If No elements of I are M-regular, then $i \subset \cup \mathrm{Ass}(M)$ thus in one of them, so $\mathrm{Hom}_{A_p}(k, M_p) \neq 0$, and we have $N_p/PN_p = N \otimes_A k_p$ nonzero by Nakayama, thus $\mathrm{Hom}_k(N \otimes_A k_p, k_p) \neq 0$, thus $\mathrm{Hom}_{A_p}(N_p, M_p) = (\mathrm{Hom}_A(N, M))_p \neq 0$, so $\mathrm{Ext}^0_A(N, M) \neq 0$. Other dimensions follows by induction, consider the cokernel of $M \xrightarrow{a_1} M$.

Conversely, use induction, then we have an injection $\mathrm{Ext}^i_A(N,M)\xrightarrow{a_1}\mathrm{Ext}^i_A(N,M)$ for $i<n$. And the condition shows that $I\subset\sqrt{\mathrm{Ann}(M)}$, so $a_1^rN=0$, thus the result. □

Cor. (5.3.4.8). Two maximal regular sequence in a f.g. module have the same length. ⌟

Cor. (5.3.4.9). For a module M over a Noetherian ring A, we know $\Gamma_I(M)=\{m|I^nm=0 \text{ for some } n\}$, and H^n_I is its right derived functor, then we have $\mathrm{depth}_I(M)\geq n \iff H^i_I(M)=0$ for $i<n$. (Because derived functor commutes with colimits, consider $N=A/I^k$). ⌟

Lemma (5.3.4.10) [Ischebeck]. For a Noetherian local ring A, if M,N are finite modules, then we have $\mathrm{Ext}^i_A(N,M)=0$ for $i<\mathrm{depth}(M)-\dim N$. ⌟

Proof: □

Prop. (5.3.4.11). Let A be a local ring and M is finite A-module, then $\mathrm{depth}(M)\leq\dim A/P\leq\dim M$ for every $P\in\mathrm{Ass}(M)$. (Because $\mathrm{Hom}(A/P,M)\neq 0$.) ⌟

Proof: □

Prop. (5.3.4.12) [Auslander-Buchsbaum Formula]. For a local ring R, if M is a finitely generated R-mod, if $pd(M)<\infty$, then we have $\mathrm{depth}(R)=\mathrm{depth}(M)+\mathrm{pd}(M)$. ⌟

Proof: Cf.[Weibel P109]. □

Cohen-Macaulay

Def. (5.3.4.13) [Cohen-Macaulay Modules]. For A Noetherian local, a f.g. A-module M is called **Cohen-Macaulay** if $\mathrm{depth}(M)=\dim M$. In view of(5.3.4.11), this is equivalence to $\mathrm{depth}(M)=\dim A/P$ for all $P\in\mathrm{Ass}(M)$. A **Cohen-Macaulay ring** is a ring A that is Cohen-Macaulay over itself.

A localization of a C.M local ring is C.M, so we call a ring **Cohen-Macaulay** if all its localization at primes are C.M. ⌟

Prop. (5.3.4.14) [Gorenstein Ring]. A ring R is called **Gorenstein** iff $id_RR<\infty$. A Gorenstein local ring is C.M. In this case, $\mathrm{depth}(R)=id_RR=\dim R$, and $\mathrm{Ext}^q_R(R/m,R)\neq 0\iff q=\dim R$. ⌟

Proof: Cf.[Weibel P107]. □

Prop. (5.3.4.15). A ring is C.M. iff for all ideals, the associated primes of A/I all have the same height as I, i.e. unmixed. ⌟

Proof:

□

Prop. (5.3.4.16). If a local ring is C.M. and $I=(x_1,\ldots,x_r)$ is a regular sequence, then $(x_1,\ldots,x_r)$ is . ⌟

Proof: ? Isn't this always true? □

Prop. (5.3.4.17). Let A is a Noetherian local ring and M a f.g. module, if a set of elements $(x_1,\ldots,x_r)$ forms a regular sequence for M, then $\dim M/(x_1,\ldots,x_r)=\dim M-r$. The converse is also true when A is C.M. If this is the case, then $A/(x_1,\ldots,x_r)$ is also C.M. ⌟

Proof: By(5.2.2.19), we have $<$, for the converse, $\mathrm{Supp}(M/fM) = \mathrm{Supp}(M) \cap \mathrm{Supp}(A/fA) = \mathrm{Supp}(M) \cap V(f)$, and when f is M-regular, $V(f)$ doesn't contain any $\mathrm{Ass}(M)$ thus no minimal elements of $\mathrm{Supp}(M)$, so $\dim(M/fM) < \dim M$, thus we have $>$.

When A is C.M.:**?** □

Prop. (5.3.4.18). Let $R \to S$ be a local homomorphism of Noetherian local rings, if R is C.M. and S is finite flat over R or S is flat over R and $\dim S \leq \dim R$, then S is C.M., and $\dim R = \dim S$. ⌟

Proof: Cf.[Sta]00R5. □

5 Normal & Regular Rings

Normal Ring

Def. (5.3.5.1)[Normal Rings]. A **normal domain** is a domain and is integrally closed in its fraction field.

A domain is normal iff all its localizations are normal, so we can define a **normal ring** to be a ring that all its stalks are normal local rings. In particular, a normal ring is reduced. ⌟

Proof: The localization of a normal domain is normal, and the converse follows from $A = \cap A_{\mathfrak{m}}$(5.1.1.34). □

Prop. (5.3.5.2) [UFD is Normal]. A UFD is a normal domain. ⌟

Proof: If A is a UFD, then for any $x \in \mathrm{Frac}(A)$ integral over A, checking the primes dividing the coefficients, we see $x \in A$. □

Prop. (5.3.5.3). A normal ring R is integrally closed in its ring of fractions. ⌟

Proof: Let $x \in Q(R)$ be integral over R, and $I = \{f \in R | fx \in R\}$, then for any prime $\mathfrak{p}$ of R, $R \to R_{\mathfrak{p}}$ is injective, so $R_{\mathfrak{p}} \subset \mathrm{Frac}(R) \otimes_R R_{\mathfrak{p}}$, and $x \otimes 1$ is integral over $R_{\mathfrak{p}}$, thus $x \otimes 1 \subset R_{\mathfrak{p}}$, which means $x \otimes 1 = 1 \otimes a/f$ for some $a, f \in R, f \notin \mathfrak{p}$. This means $f'(fx - a) = 0 \in Q(R)$ for some $f' \notin \mathfrak{p}$, so $ff' \in I$, and thus I is not contained in any prime ideal, so $I = 1$ and $x \in R$. □

Prop. (5.3.5.4). Let R be a reduced ring with f.m. minimal prime ideals, then the following are equivalent:

- R is a normal ring.
- R is integrally closed in its ring of fractions.
- R is a finite product of normal domains.

In particular, a Noetherian normal domain is a finite product of normal domains(5.1.1.47). ⌟

Proof: $3 \to 1$ is trivial, $1 \to 2$ is by(5.3.5.3), for $2 \to 3$: let $\mathfrak{p}_i$ be the minimal prime ideals of R, then $\mathrm{Frac}(R) = \prod_{i=1}^r Q_{\mathfrak{p}_i}$(5.1.7.22), with each $Q_{\mathfrak{p}_1}$ field because R is reduced. Denote the idempotents of $\mathrm{Frac}(R)$ by e_i. Then e_i is integral thus in R. These idempotents make R into a product of domains, which are just $R/\mathfrak{p}_i$, because the kernel of the map $R \to R_{\mathfrak{p}_i}$ is $\mathfrak{p}_i$. Now R is integrally closed in $Frac(R)$ implies each $R/\mathfrak{p}_i$ is integrally closed in $R_{\mathfrak{p}_i}$, thus R is a finite product of normal domains.
□

Def. (5.3.5.5) [Normalization]. The **normalization** of an integral domain is the alg.closure of it in its quotient field. It commutes with localization. ⌟

Def. (5.3.5.6)[Completely Normal Domains]. A domain is called **completely normal** iff all almost normal elements are in A, i.e. $\{u|\exists a, au^n \in A\ \forall n\} \in A$. For Noetherian ring, completely normal is equivalent to normal. ⌟

Proof: Cf.[Sta]00GX. □

Prop. (5.3.5.7). A is a normal domain, then so does $A[X]$. If A is Noetherian normal domain, then so does $A[[X]]$. ⌟

Proof: Cf.[Sta]030A, 0BI0. □

Prop. (5.3.5.8). Direct limits of normal rings are normal. ⌟

Proof: Let $\mathfrak{p}$ be an ideal of $R = \varinjlim R_i$, $\mathfrak{p}_i = \mathfrak{p} \cap R_i$, then $R_\mathfrak{p} = \varinjlim (R_i)_{\mathfrak{p}_i}$, so it suffices to prove for normal domains, the rest is easy. □

Prop. (5.3.5.9)[Closure in Separable Extension]. Let R be a Noetherian normal domain with field of fraction K and L/K is a finite separable field extension, then the integral closure S of R in L is finite over R. ⌟

Proof: Let $\mathrm{tr} : L \times L \to K : (x, y) \mapsto \mathrm{tr}(xy)$ be the trace pairing, then as L/K is finite separable, this is non-degenerate. Now if $x \in L$ is integral over R, then $\mathrm{tr}(x) \in R$. So if $x_1, \ldots, x_n$ are integral and form a basis of L over K, then $M = \{y \in L|\langle x_i, y\rangle \in R\}$ is an R-module and $M \cong R^n$, and $S \subset M$, so S is finite over R as R is Noetherian. □

Prop. (5.3.5.10)[Field Extension]. Let A be a K-algebra, and L/K is a field extension, then if A_L is a normal integral domain, so is A. And the converse is also true if L/K is separable. ⌟

Prop. (5.3.5.11)[Algebraic Hartogs's Lemma]. Principal ideals in a Noetherian normal domain is unmixed and $A = \cap_{\mathrm{ht}\, p=1} A_p$. ⌟

Proof: Cf.[Matsumura P124].**?** [Rising Sea, P320], [Sta]031T. □

Prop. (5.3.5.12)[Krull]. If A is a normal domain with fraction field K, L is a normal extension field of K and B is the integral closure of A in L that $A \subset B$ is integral, then any two prime ideals of B lying over a prime in A are conjugate by an action of $G_{L/K}$. ⌟

Proof: Firstly if $G_{L/K}$ is finite, and P, P' be primes of B that $P \cap A = P' \cap A$. Let $P_i = \sigma_i(P)$. If $P' \neq P_i$ for any i, then $P' \not\subseteq P_i$ for any i by(5.2.1.5), so there is some $x \in P'$ not in any of P_i. Now let $y = (\prod_i \sigma_i(x))^q$ where $q = 1$ if $\mathrm{char}(K) = 0$ and $q = p^r$ for r large if $char(K) = p$, then $y \in K$ thus in A because A is normal, and it is not in P by hypothesis. But $y \in P' \cap A = P \cap A$, contradiction.

For the infinite field extension case, let K' be the fixed field of $G_{L/K}$ so that K'/K is purely inseparable, then there is clearly exactly one prime of K' over any prime of A. So we can assume L/K is Galois, then use profinite group technique to find a $\sigma \in G_{L/K}$ that $\sigma(P) = P'$. □

Prop. (5.3.5.13)[Hironaka]. Let A be a local Noetherian domain that is a localization of an algebra of f.t. over a field k. Let $t \in A$ that

- tA has only on eminimal associated prime ideal p.
- t generate the maximal ideal of A_p.
- A/p is normal.

Then $p = tA$ and A is normal. ⌟

Proof: Cf.[Hartshorne P264]. □

Prop. (5.3.5.14) [Quadratic Extension is Normal]. If A is a UFD that 2 is invertible in A and $f \in A \backslash A^2$, then $A[Z]/(Z^2 - f)$ is integral and normal. ⌟

Proof: It is integral by(3.2.3.14). To show it is normal, assume $F(T) \in B[T]$ that $f(\alpha) = 0$, where $\alpha \in K(B) \backslash B$, then by replacing F by $\overline{F}F$, we can assume $F(T) \in A[T]$. We can assume $\alpha \notin K(A)$, thus $\alpha = g + hZ$, then the minimal polynomial of α is $Q(T) = T^2 - 2gT + (g^2 - h^2 f) \in K(A)[T]$. Then $F(T) = P(T)Q(T)$ in $K(A)[T]$. By Gauss's lemma, $2g, g^2 - h^2 f \in A$, so $g, f \in A$ by hypothesis. □

Cor. (5.3.5.15). If k is a field of characteristic$\neq 2$, then
- $k[x_1, \ldots, x_n]/(x_1^2 + \ldots + x_m^2)$ is integral normal for $n \geq m \geq 3$.
- $k[x, y, z, w]/(wz - xy)$ is normal.(Diagonalize).

⌟

Prop. (5.3.5.16). $\mathbb{Z}[\sqrt{n}]$ is integrally closed for $n \equiv 3 \mod 4$, and $\mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ is integrally closed for $n \equiv 1 \mod 4$, by(14.4.1.44). ⌟

Regular Ring

Def. (5.3.5.17) [Regular Rings]. A Noetherian local ring $(A, \mathfrak{m}, k)$ is called **regular local** iff it $\mathrm{rank}_k\, \mathfrak{m}/\mathfrak{m}^2 = \dim A$. This is equivalent to $\mathrm{rank}_k\, \mathfrak{m}/\mathfrak{m}^2 \leq \dim A$, or $\mathrm{gr}\ A \cong k[X_1, \ldots, X_d]$ by(5.2.2.19).

Localization of a regular local ring at primes are regular local, Cf.[Sta]0AFS. Hence we define a **regular ring** to be a Noetherian ring that all its localization at primes are regular local. ⌟

Proof: Cf.[Matsumura P139]. □

Prop. (5.3.5.18). If A is regular, then $A[X_1, \ldots, X_n]$ is regular, and $A[[X_1, \ldots, X_n]]$ is regular. ⌟

Proof: Cf.[Matsumura P176]. □

Prop. (5.3.5.19) [Auslander-Buchsbaum]. A regular local ring is UFD. In particular it is a normal domain. Thus a regular ring is normal and thus reduced(5.3.5.1). ⌟

Proof: Cf.[Matsumura P142],[Weibel P106]. □

Cor. (5.3.5.20). A regular local ring of dimension 0 is a field, and a regular local ring of dimension 1 is a DVR. ⌟

Prop. (5.3.5.21). A regular local ring is Gorenstein hence C.M.. ⌟

Proof: □

Prop. (5.3.5.22)[Regular Local Ring and Regular Sequences]. Let $(R, \mathfrak{m})$ be a regular local ring of dimension d,
- If $x_1, \ldots, x_c$ be a sequence that maps to linearly independent elements in $\mathfrak{m}/\mathfrak{m}^2$, then $(x_1, \ldots, x_c)$ is a regular sequence, and $R/(x_1, \ldots, x_c)$ is a regular local ring of dimension $d - c$.

- If $I \subset \mathfrak{m}$ and R/I is a regular local ring, then $I = (x_1, \ldots, x_c)$ where $(x_1, \ldots, x_c)$ is a regular sequence.
- If $(x_1, \ldots, x_c)$ is a regular sequence in $\mathfrak{m}$ and $R/(x_1, \ldots, x_c)$ is a regular local ring, then R is also a regular local ring.

⌟

Proof: 1: We can complete it to a sequence $(x_1, \ldots, x_d)$ that $(x_1, \ldots, x_d)$ generate $\mathfrak{m}/\mathfrak{m}^2$, then by Nakayama $(x_1, \ldots, x_d) = \mathfrak{m}$. Now by Krull's height theorem(5.2.4.18), $R/(x_1)$ has dimension$\geq d-1$ and $(x_2, \ldots, x_d)$ generate the maximal ideal, so $R/(x_1)$ is a regular local ring by definition. Now $x_1 \neq 0$ because R is a domain(5.3.5.19), thus we can use induction to show $(x_1, \ldots, x_c)$ is a regular sequence.

2: Let $\dim(R/I) = d - c$, then the hypothesis shows $(I + \mathfrak{m}^2)/\mathfrak{m}^2 \cong I/\mathfrak{m}I$ has rank c, thus we can choose $(x_1, \ldots, x_c) \in I$ that generate $I/\mathfrak{m}I$. Thus by Nakayama $I = (x_1, \ldots, x_c)$, and $(x_1, \ldots, x_c)$ is a regular sequence by item1.

3: By induction, it suffices to prove the $c = 1$ case, then any lift of x_1 together with $d-1$ generator of the maximal ideal of $R/\mathfrak{m}$ is a set of generator of $\mathfrak{m}$. □

Cor. (5.3.5.23). A regular local ring is C.M., by item1. ⌟

Prop. (5.3.5.24). If a quotient of a Noetherian local ring by a non-zerodivisor is regular, then it is itself regular. ⌟

Prop. (5.3.5.25) [Serre]. A Noetherian local ring A is regular iff the global dimension of A is finite. ⌟

Proof: Cf.[Mat P139]. □

Prop. (5.3.5.26). For A a regular local ring and M a f.g. A-module,

$$pd(M) + \text{depth } M = \dim A.$$

Cf.[Hartshorne P237]. ⌟

Cor. (5.3.5.27). For a f.g. module M over a regular local ring A, $pd(M) \leq n$ iff $\operatorname{Ext}^i(M, A) = 0$ for all $i > n$. ⌟

Proof: This is because we can use dimension shifting to show $\operatorname{Ext}^i(M, N) = 0$ for all N f.g., then(5.3.3.3) says that $pd(M) \leq n$. □

Prop. (5.3.5.28) [Regular and Regular Sequence]. Let ⌟

Prop. (5.3.5.29). Let $R \to S$ be a flat local homomorphism of Noetherian local rings that R is regular, $S/\mathfrak{m}_S$ is regular, then S is also regular. ⌟

Proof: Cf.[Sta]031E. □

Serre Conditions R_k & S_k

Def. (5.3.5.30). A ring is called R_k iff for all prime p of height $\leq k$, A_p is regular.

A ring is called S_k iff $\text{depth}(A_p) \geq \min(k, \text{ht}(p))$ for all prime p.

A module M is called S_k iff $\text{depth}(M_p) \geq \min(k, \dim \operatorname{Supp} M_p)$ for all prime p.

⌟

Prop. (5.3.5.31).

- M is S_1 iff M has no associated embedded primes. Cf.[Sta]031Q.
- A Noetherian ring is reduced iff it is R_0 and S_1. Cf.[Sta]031R.
- (Serre Criterion)A Noetherian ring is normal iff it is R_1 and S_2. Cf.[Sta]031S.
- A ring is C.M. iff it is $S_{\mathbb{N}}$.

⌟

Proof: □

Cor. (5.3.5.32) [Regular and Normal]. A regular ring is normal, and normal ring is regular in codimension 1. ⌟

Proof: By(5.3.5.31), it suffices to prove that a regular ring satisfies R_1 and S_2. A regular ring is C.M.(5.3.5.21) so it is S_2 by(5.3.5.31), it is R_1 by(5.3.5.17) □

Cor. (5.3.5.33)[Normal and Regular Dimension 1]. A Noetherian local ring of dim 1 is normal iff it is regular. i.e. integral domain and integrally closed iff maximal ideal is principal. ⌟

6 Geometric Properties

Def. (5.3.6.1).

- A k-algebra S is called **geometrically reduced/integral/connected**... over a field k iff for any field extension k'/k, $\operatorname{Spec} S_{k'}$ is reduced/integral/connected....
- A Noetherian k-algebra S is called **geometrically regular** iff for any f.g. field extension K/k, S_K is regular(Notice $A \otimes_k k'$ is Noetherian(5.1.1.45), so this makes sense).

⌟

Prop. (5.3.6.2)[Geometrically reduced]. If S is a k-algebra, the following are equivalent.

1. S is geometrically reduced.
2. $S \otimes_k \overline{k}$ is reduced.
3. $S \otimes_k k^{per}$ is reduced.
4. $S \otimes_k k'$ is reduced for any finite purely inseparable field extension k'/k.
5. $S \otimes_k k^{1/p}$ is reduced.
6. residue fields of S at maximal points are reduced.
7. $S \otimes_k R$ is reduced for every reduced k-algebra R.

⌟

Proof: 1 → 7: We can assume R is f.g., thus R is contained in a finite product of fields Cf.[Sta]030V**?**, and then we can assume R is a product of fields, and we are done.

1 → 2 → 3 → 4 is clear. 3 → 5 is clear.

4 → 1: For any field extension K/k, we can assume WLOG K/k is f.g., thus**?**

5 → 1: **?** 6:**?** Cf.[Sta]030V and [Gortz 135]. □

Prop. (5.3.6.3)[Geometrically Irreducible]. Let S be a k-algebra, the following are equivalent:

1. S is geometrically irreducible.

2. For any finite separable field extension k'/k, the spectrum of $S_{k'}$ is irreducible.
3. The spectrum of $S_{k^{sep}}$ is irreducible.
4. The spectrum of $S_{\overline{k}}$ is irreducible.

⌟

Proof: Cf.[Sta]037K.**?** □

Prop. (5.3.6.4). Let S be a geometrically irreducible k-algebra and R is a k-algebra, then the map

$$\operatorname{Spec}(R \otimes_k S) \to \operatorname{Spec} R$$

induces a bijection on irreducible components. ⌟

Proof: Cf.[Sta]037O.**?** □

Prop. (5.3.6.5) [Geometrically Integral]. Let S be a k-algebra, the following are equivalent:

1. S is geometrically integral.
2. For any finite separable field extension k'/k, $S_{k'}$ is an integral domain.
3. $S_{\overline{k}}$ is an integral domain.
4. $S \otimes_k R$ is an integral domain for any integral domain R over k.

⌟

Proof: This follows from(5.3.6.3)(5.3.6.2) and(5.3.6.4). □

Prop. (5.3.6.6). It suffices to check geometrically regular for k'/k finite purely inseparable. ⌟

Proof: Cf.[Sta]0381.**?** □

7 Finitely Presentedness

Finite Presented Modules

Def. (5.3.7.1) [Finitely Presented Modules]. A **finitely presented module** is a module of the form R^m/R^n.

Finite presentation is stable under base change because tensoring is right exact. ⌟

Prop. (5.3.7.2). Given an exact sequence of R-modules $0 \to M_1 \to M_2 \to M_3 \to 0$,

- If M_1, M_3 are f.p., then so does M_2.
- If M_3 is f.p. and M_2 is f.g., then M_1 is f.g.
- If M_2 is f.p. and M_1 is f.g., then M_3 is f.p.

⌟

Proof: 1: e can find an commutative diagram $\begin{array}{ccccccccc} 0 & \longrightarrow & R^m & \longrightarrow & R^{m+n} & \longrightarrow & R^m & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \end{array}$ and use the snake lemma to see the kernel is f.g..

2: Use the diagram
$$\begin{array}{ccccccccc} & & R^m & \longrightarrow & R^n & \longrightarrow & M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow & & \downarrow{\scriptstyle\mathrm{id}} & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \end{array}$$
. and snake lemma, then image and cokernel of α are all finite, so M_1 is finite.

3: Choose a presentation $R^m \to R^n \to M_2$ and a surjection $f : R^k \to M_1$, then we can lift f to $R^k \to R^n$, and then M_3 can be written as a quotient $R^{m+k} \to R^n \to M_3$. □

Cor. (5.3.7.3). A direct summand of a f.p. module is f.p.. ⌟

Prop. (5.3.7.4). If $R \to S$ is a f.g. ring map and a S-module M is f.p. over R, then it is f.p. over S. ⌟

Proof: Let $S = R[x_1, \ldots, x_n]$, and $M = R[y_1, \ldots, y_m]/(\sum a_{ij}y_j), 1 \leq i \leq t$, then as M is a S-module, we let $x_iy_j = \sum a_{ijk}y_k$, and forms a quotient $S^{mn+t} \to S^m \to N \to 0$, where S^{mn+t} corresponds to the relations $\sum a_{ij}y_j$ and $x_iy_j - \sum a_{ijk}y_k$. Then there is a surjective A-module map $N \to M$, and we check it is injective: if $z = \sum b_jy_j$ are mapped to 0, where $b_j \in S$, then we can transform z into the shape $\sum c_jy_j$, where $c_j \in R$ by relations $x_iy_j - \sum a_{ijk}y_k$. Thus it is zero by definition. □

Prop. (5.3.7.5)[Direct Limits of F.P. Modules]. Any module is a direct limit of f.p. modules. This can be seen by considering all finite submodules and f.m relations between them. ⌟

Prop. (5.3.7.6)[Characterizing Finite and F.P. Modules]. Let N be an R-module, then

- N is finite R-module iff for any filtered colimits $M = \varinjlim M_i$ of R-modules, the map $\varinjlim \mathrm{Hom}(N, M_i) \to \mathrm{Hom}(N, \varinjlim M_i)$ is injective.
- N is a f.p. R-module iff for any filtered colimits $M = \varinjlim M_i$ of R-modules, the map $\varinjlim \mathrm{Hom}(N, M_i) \to \mathrm{Hom}(N, \varinjlim M_i)$ is a bijection.

⌟

Proof: 1: If N is generated by x_i and a map $f : N \to M_i$ maps to $0 \in \mathrm{Hom}(N, \varinjlim M_i)$, then there is a j that $f : M \to M_i \to M_j$ is 0. Thus $f = 0$. Conversely, N is the sum of its f.g. submodules N', thus $N \to \varinjlim N/N_i = 0$, which implies the identity map $N \to N$ vanishes for some N/N' where N' is a finite submodule of N, so $N = N'$ and N is a finite.

2: If M is f.p., we can get the assertion by writing M as a quotient of free modules and use the fact filtered colimit is exact(5.1.1.25). Conversely, write N as a filtered colimits of f.p. modules(5.3.7.5), then $\mathrm{id} : M \to M$ factors through some f.p. module, so it is a direct summand of a f.p. module, thus f.p. by(5.3.7.3). □

Cor. (5.3.7.7)[FP and Localization]. For M f.p., $S^{-1}\mathrm{Hom}_R(M, N) = \mathrm{Hom}_{S^{-1}R}\mathrm{Hom}(S^{-1}M, S^{-1}N)$ for any R-module N. (Use the presentation and Hom is left exact). ⌟

Proof: $\mathrm{Hom}_{S^{-1}R}\mathrm{Hom}(S^{-1}M, S^{-1}N) \cong \mathrm{Hom}_R(M, S^{-1}N)$ by duality, and then we can use(5.3.7.6), as localization is a filtered colimit. □

Finitely Presented Ring Map

Def. (5.3.7.8) [Finitely Presented Ring Map]. A ring map is called **of finite presentation** iff it is a quotient of a free algebra by a free algebra. ⌟

Prop. (5.3.7.9). Finite presentation is stable under composition(choose a presentation form to see) and base change because tensoring is right exact.

It is local on the source and target by(5.1.4.4). ⌟

Prop. (5.3.7.10). For S f.p. over R, then the kernel of any surjective ring map $R[X_1,\ldots,R_n]\xrightarrow{\alpha}S$ is f.g.. ⌟

Proof: Let $S=R[Y_1,\ldots,Y_m]/(f_1,\ldots,f_k)$, then if $\alpha(X_i)\cong g_i(Y)$, then $\alpha:R[X_1,\ldots,R_n]\to R[X_1,\ldots,X_m,Y_1,\ldots,Y_m]/(f_1,\ldots,f_k,X_i-g_i)$. And the Y_i are in the image, thus we let Y_i are mapped onto by $h_j(X)$, then $\ker\alpha=(f_i(h_j(X)),X_i-g_i(X))$. □

Prop. (5.3.7.11). If $g\circ f:R\to S'\to S$ is of finite presentation and f is of finite type, then g is of finite presentation. ⌟

Proof: Let $S'=R[y_1,\ldots,y_a]$ and $S=R[X_1,\ldots,X_n]/(f_1,\ldots,f_m)$, then let $h_i(X)\cong y_i$ in S, then $S=S'[X_1,\ldots,X_n]/(f_1,\ldots,f_m,h_i-y_i)$. □

Prop. (5.3.7.12) [Normal Form of F.P.]. If S is f.p. over R that S has a presentation $S=R[X_1,\ldots,X_n]/I$ that I/I^2 is free over S, then S has a presentation $R[X_1,\ldots,X_m]/(f_1,\ldots,f_c)$ that $(f_1,\ldots,f_c)/(f_1,\ldots,f_c)^2$ is freely generated by $f_1,\ldots,f_c$. ⌟

Proof: Cf.[Sta]07CF. □

Prop. (5.3.7.13) [Finite Type Locally of Finite Presentation]. If $R\to S$ is a injective map of f.t. of domains, then there are $f\neq0\in R,g\neq0\in S$ that $R_f\to S_{fg}$ is of f.p. ⌟

Proof: Use induction on the number of generators of S/R. If $S=R[x]$, then $S=R[X]/\mathfrak{q}$. If $q=0$, then S is of f.p.. If $g=fx^d+a_{d-1}x^{d-1}+\ldots a_0$ be a polynomial of minimal degree in $\mathfrak{q}$, then $R\to S_f$ is of f.p.

The more generator case can be reduced to the single generator case, because f.p. ring map is stable under composition(5.3.7.9). □

Lemma (5.3.7.14) [Filtered Colimits and F.P.]. Let $R\to A$ be a ring map, then the category of f.p. R-algebras A' with an R-algebra map $A'\to A$ is filtered, and the colimit is just A. ⌟

Proof: Cf.[0BUF]. □

8 Nagata & Excellent Rings

Def. (5.3.8.1) [Japanese & Nagata Rings]. Let R be a domain with quotient field K, then R is called **N-1** iff the integral closure of R in K is a finite R-module.

R is called **N-2** or **Japanese** iff for any finite field extension L/K, its integral closure in L is a finite R-module.

A ring R is called **universally Japanese** if for any domain S of f.t. over R, S is Japanese.

A ring R is called **Nagata** if it is Noetherian and for any prime p, R/p is Japanese.

All these properties are local properties(5.1.4.4). And they are in fact stable under any localizations. ⌟

Prop. (5.3.8.2) [Nagata]. Let R be a ring, the following are equivalent:

- R is Nagata,
- any f.g. R-algebra is Nagata.
- R is universally Japanese and Noetherian.

⌟

Proof: Cf,[Sta]0334. □

Prop. (5.3.8.3)[Nagata and Formal Fibers]. Let $(A, \mathfrak{m})$ be a Noetherian local ring, then A is Nagata iff the formal fibers of A are geo.reduced. ⌟

Proof: Cf.[Sta]0BJ0. □

Excellent Rings

Def. (5.3.8.4) [G-Rings]. A **G-ring** is a Noetherian ring s.t. for any prime $\mathfrak{p} \subset R$, the map $R_{\mathfrak{p}} \to R_{\mathfrak{p}}^{\wedge}$ is regular. ⌟

Def. (5.3.8.5) [Excellent Rings]. A **quasi-excellent ring** is a ring that is Noetherian, G-ring and J-2. A **excellent ring** is a quasi-excellent ring that is universally catenary. ⌟

Prop. (5.3.8.6). Quasi-excellent rings are Nagata. ⌟

Proof: Cf.[Sta]07QV. □

Prop. (5.3.8.7) [Examples]. The following rings and f.g. algebras over them are excellent rings:

- fields.
- Noetherian complete local rings
- Dedekind domain with fraction field of characteristic 0.

In particular, ring of integers in all local fields and number fields are excellent. ⌟

Proof: Cf.[Sta]0335. □

Cor. (5.3.8.8). The above rings are all Nagata, by(5.3.8.6). ⌟

9 Separability

Main references are [Matsumura Ch10], [Weibel Chap P309] and [Sta]10.41, 10.43.

Def. (5.3.9.1) [Separable Algebra]. A f.d semisimple algebra R over a field k is called **separable** iff for every field extension K/k, $R \otimes_k K$ is semisimple. ⌟

Def. (5.3.9.2). A field extension K/k is called **separably generated** iff it K is a separable algebraic extension of a purely transcendental field L/k.

A field extension K/k is called **separable** iff all f.g. subextensions are separably generated.

An algebra A/k is called **separable** iff $A \otimes_k k'$ is reduce for any k'/k algebraic. ⌟

Prop. (5.3.9.3). If $k \subset K$ is a f.g. field extension, then there is a finite purely inseparable field extension $k \subset k'$ that $k' \subset k'K$ is separable. ⌟

Proof: □

Prop. (5.3.9.4) [Separable and Geo.Reduced]. Let K/k be a field extension, then K/k is separable iff K/k is geometrically reduced. ⌟

Proof: Cf.[Sta]030W.? □

Cor. (5.3.9.5). If K/k is a separable field extension and S is a reduced k-algebra, then $S \otimes_k K$ is reduced. ⌟

Proof: Cf.[Sta]030U. □

Cor. (5.3.9.6). A separably generated field extension is separable. ⌟

10 Henselian Ring

Main References are [Sta]Chap10.148.

Def. (5.3.10.1). A local ring $(R, \mathfrak{m}, k)$ is called **Henselian** iff for every $f \in R[X]$ and $a_0 \in k$ that $\overline{f}(a_0) = 0$ and $\overline{f}'(a_0) \neq 0$, then there is a root α of f lifting a_0. It is called **strict Henselian** if moreover its residue field is separably closed. ⌟

Henselian Pairs

Def. (5.3.10.2). A **Henselian pair** is a pair (A, I) that is Zariski and for any f, g in $A[T]$ monic and $\overline{f} = \overline{g}\overline{h} \in A/I[T]$ that is coprime and monic, there is a factorization $f = gh$ lifting the decomposition.

In particular, if f has a simple root $\overline{x}$ in A/I, then it has a root $x \in A$ lifting $\overline{x}$. ⌟

Prop. (5.3.10.3). Filtered limits of Henselian pairs is Henselian, this is clear from the definition(5.3.10.2). ⌟

Lemma (5.3.10.4). If A is a ring with ideal I, if $\overline{f} = \overline{g}\overline{h}$ be a factorization of a polynomial $f \in A[T]$ in $A/I[T]$, then there is an étale ring map $A \to A'$ that $A/IA \cong A'/IA'$, and a factorization $f = g'h' \in A'[T]$ lifting the factorization. ⌟

Proof: Cf.[Sta]0ALH**?** □

Prop. (5.3.10.5) [Topological Invariance of Étale Sites]. If I is locally nilpotent, then (A, I) is Henselian, in particular $A_{ét} \cong (A/I)_{ét}$(5.3.10.9). ⌟

Proof: First if $A \to S$ is étale, then $A/I \to S/IS$ is étale by base change(5.4.7.5) and the map is essentially surjective by(5.4.7.15). And any map $B/IB \to B'/IB'$ can be lifted to $B \to B$ because étale is smooth and use(5.4.5.16). And the lifting is unique, otherwise if f, g are two lifting, because étale is unramified, so if we choose an idempotent e generating the kernel of $B \otimes_A I \to B \to B$(5.4.6.10), then $f \otimes g(e) \in IB'$, which is locally nilpotent, thus $f \otimes g(e) = 0$, thus $f = g$.

For then Henselian, I is clearly contained in the Jacobson radical, and for the decomposition, by(5.3.10.4) these is an étale map $A \to A'$ that $A/IA \cong A'/IA'$ that lifts the factorization, but $A = A'$, by what we have seen above. □

Cor. (5.3.10.6) [Complete Pair is Henselian]. If (A, I) is a pair that A is I-adically complete, then (A, I) is Henselian. ⌟

Proof: I is in the Jacobson radical because $1 + I$ consists of units, and by(5.3.10.5) and(5.3.10.4) we can lift the decomposition to A/I^n inductively. As $A = \lim A/I^n$, we are done. □

Prop. (5.3.10.7) [Equivalent Definitions of Henselian Pair]. The following are all equivalent to (A, I) being Henselian:

- Given any étale ring map $A \to A'$, then any $A' \to A/I$ lifts to an A-algebra map $A' \to A$.
- For any finite/integral A-algebra B, the map $B \to B/IB$ induces a bijection on idempotents.
- (Gabber) (A, I) is Zariski and every monic polynomial $f(T) \in A[T]$ of the form $T^n(T-1) + a_nT^n + \ldots + a_1T + a_0$ with $a_i \in I$ has a root $\alpha \in 1 + I$.

Moreover, root in item3 is unique. ⌟

Proof: Cf.[Sta]09XI. □

Cor. (5.3.10.8). if (A, I) is Henselian and $A \to B$ is integral, then (B, IB) is also Henselian. ⌟

Prop. (5.3.10.9)[Henselian Lifting]. If (A, I) is a Henselian pair, then there is a natural equivalence of categories: $A_{ét} \cong (A/I)_{ét}$. ⌟

Proof: Cf.[Sta]09ZL.? □

Prop. (5.3.10.10). A Zariski pair (R, I) is Henselian iff the pair $(\mathbb{Z} \oplus I, I)$ is Henselian. In particular, the property of being Henselian only depends on the non-unital ring I. ⌟

Proof: Cf.[Almost Ring Theory, 5.1.9]. □

5.4 Commutative Algebra IV

1 Flatness

Def. (5.4.1.1) [Flatness]. A modules M over a ring R is called **flat** if $M \otimes_R - : \mathrm{Mod}_R \to \mathrm{Mod}_R$ is an exact functor. This is compatible with the definition(6.2.2.15). ⌟

Prop. (5.4.1.2). Flatness need only be checked for finite modules, and it is equivalent to $\mathrm{Tor}_1(M, A/I) = 0$ for any f.g. ideal I(i.e $I \otimes M \to M$ is injective). ⌟

Proof: This is because of(6.3.3.12) and the fact tensor product commutes with colimit. □

Cor. (5.4.1.3). If $0 \to M' \to M \to M'' \to 0$, then M' and M'' flat implies M is flat. ⌟

Prop. (5.4.1.4). If M is flat then $\mathrm{Tor}_i^A(M, N) = 0$ for all $i > 0$, because we have: if $0 \to M_1 \to M_2 \to M_3 \to 0$ M_2, M_3 flat, then M_1 is flat (Use 9 entry sequence and the fact that Tor is symmetric(5.9.2.5)). So $\mathrm{Tor}_{n+1}(M_3, N) = \mathrm{Tor}_n(M_1, N) = 0$ by induction.

And a direct summand of a flat module is flat. Thus we have the class of flat modules is adapted $- \otimes N$ for all N (because free is flat). ⌟

Prop. (5.4.1.5) [Faithfully Flatness]. The following are equivalent:

- M is flat and for any $N \neq 0$, $N \otimes_R M \neq 0$.
- M is flat and for any (maximal)prime ideal $\mathfrak{m}$ of R, $k(\mathfrak{m}) \otimes_R M \neq 0$. (When $\mathfrak{m}$ is maximal, which means $\mathfrak{m}M \neq M$).

And such a M is called **faithfully flat** over R. ⌟

Proof: $1 \to 2$ is easy. $2 \to 1$: any nonzero module has a submodule R/I, choose a maximal ideal $\mathfrak{m}$ containing I, then $(A/I) \otimes_A M \subset N \otimes_A M$ surjects to $k(\mathfrak{m}) \otimes_A M \neq 0$. □

Prop. (5.4.1.6) [Flatness and Base Change].

- (Faithfully)Flatness is stable under base change.
- Flatness satisfies f.f. descent(5.4.2.1).
- Flatness is stable under filtered colimit because filtered colimit commutes with tensoring(3.2.4.13) and is exact(5.1.1.25). In particular, $S^{-1}A$ is flat(5.1.1.28).
- Let $S \to S'$ be a map of R-algebras, M is an S-module, $M' = M \otimes_S S'$, then if M is flat over R, so does M'. The converse also holds if $S \to S'$ is f.f..
- If $R \to S$, and a S-module M is R-flat and S-f.f., then $R \to S$ is flat.

⌟

Proof:

4: For any injection of R-modules $N \to N'$, use the fact $\ker(N \otimes_R M \to N' \otimes_R M) \otimes_S S' = \ker(N \otimes_R M' \to N' \otimes_R M')$.

5: For any injection of R-modules $N \to N'$, use the fact $\ker(N \otimes_R S \to N' \otimes_R S) \otimes_S M = \ker(N \otimes_R M \to N' \otimes_R M)$. □

Prop. (5.4.1.7) [Equational Criterion of Flatness]. For a R-module M, a relation $\sum f_i x_i = 0$ where $f_i \in R, x_i \in M$ are called **trivial** iff $\overrightarrow{x} = A\overrightarrow{y}$ for some $A \in M_{n\times n}(R)$, $\overrightarrow{y} \in M^n$, and $\overrightarrow{f}^t A = 0$. Then M is flat iff all relations of elements of M is trivial. ⌟

Proof: Assume M if flat over R, and $\sum_i f_i x_i = 0$ is a relation in M, Let $I = (f_1, \ldots, f_n)$ and let $K = \ker(R^n \to I : (x_i) \mapsto \sum x_i f_i)$, then $\sum f_i \otimes x_i = 0 \in I \otimes_R M$ by flatness, then $\sum e_i \otimes x_i \in K \otimes_R M$. Let $\sum e_i \otimes x_i = \sum k_j \otimes y_j$, and $k_j = \sum_i a_{ij} e_i$, then this is the desired relations.

Conversely, suppose every relation is trivial, and I is an ideal of R, let $x = \sum f_i \otimes x_i \subset I \otimes M$ be an element mapping to $0 \in R \otimes M = M$, then $\sum f_i x_i$ is a relation, so it is trivial, and then $x = \sum f_i \otimes x_i = \sum f_i \otimes (a_{ij} y_j) = \sum (f_i a_{ij}) y_j = 0$. □

Prop. (5.4.1.8) [Gororov-Lazard]. Any flat A-module is isomorphic to a direct limit of finite free modules. ⌟

Proof: Cf.[Sta]058G. □

Prop. (5.4.1.9). Flat module is torsion-free. ⌟

Proof: If $x \in R$ is a nonzero-divisor, $R \xrightarrow{x} R$ is injective, thus $M \xrightarrow{x} M$ is also injective. □

Prop. (5.4.1.10) [Flat over Local Rings]. A finite module M over a local ring A is flat iff it is free. In particular, finite modules over a field are all flat. ⌟

Proof: Let $A/\mathfrak{m} = k$, choose a k-basis x_i of $M/\mathfrak{m}M$, then they generate M by Nakayama. It suffices to prove that x_i are independent over R. For this, use equational criterion of flatness(5.4.1.7), we prove that if x_i is independent over k, then they are independent over A. Use induction, if $x \neq 0$ in $M/\mathfrak{M}$, if $fx = 0$ for some $f \in A$, then $x = \sum a_j y_j$ that $f a_j = 0$, but then some a_j is a unit, so $f = 0$.

If $\sum f_i x_i = 0$, then by hypothesis, $f_i \in \mathfrak{m}$, and there are y_j that $x_i = \sum a_{ij} y_j$, $\sum f_i a_{ij} = 0$. As $x_n \notin \mathfrak{m}M$, there is a $a_{nj} \notin \mathfrak{m}$, so $f_n = \sum (-a_{ij}/a_{nj}) f_i$. then $\sum_{i \neq n} f_i (x_i - a_{ij}/a_{nj} x_n) = 0$, but $x_i - a_{ij}/a_{nj} x_n$ is also independent over k, so by induction, $f_i = 0$, also does f_n, so we are done. □

Prop. (5.4.1.11) [Flat over Bézout Domains]. A module M over a Bézout domain R is flat iff it is torsion-free. ⌟

Proof: One direction is clear by(5.4.1.9). If it is torsion-free, we use the equational criterion of flatness(5.4.1.7):

Let $\sum a_i x_i = 0$ where $a_i \in R^*, x_i \in M$, then consider $(a_1, \ldots, a_n) = (a)$, thus $a_i = a b_i$ for some $b_i \in R$, and $\sum c_i b_i = 1$ for some $c_i \in R$ as R is a domain. Because M is torsion-free, $\sum_i b_i x_i = 0$. Notice $\vec{x} = (1 - \vec{c}\vec{b}^t)\vec{x}$, so we can take $\vec{y} = \vec{x}$, $A = 1 - \vec{c}\vec{b}^t$. Then $\vec{b}^t A = \vec{b}^t - \vec{b}^t \vec{c}\vec{b}^t = 0$. □

Cor. (5.4.1.12) [Flat over Valuation Rings]. A module over a valuation ring is flat iff it is torsion free. In particular, if $(A, \mathfrak{m})$ is a DVR with a uniformizer t, then $M \in \mathcal{M}od_A$ is flat iff t is injective on M. ⌟

Proof: Because valuation ring is Bézout (11.2.2.8), we can use(5.4.1.11). □

Cor. (5.4.1.13) [Flat Module over a Dedekind Domain]. If A is a Dedekind domain, then an A-module is flat iff it is torsion-free. ⌟

Proof: Because flatness and torsion-freeness is stalkwise(5.1.4.2), so it suffices to prove for its localization, which is DVR(5.2.7.2), so the result follows from(5.4.1.12). □

Prop. (5.4.1.14) [Finite Flat is Locally Free]. Finitely presented flat module is equivalent to finite projective and equivalent to finite locally free. (Immediate from(5.3.1.7)). ⌟

Prop. (5.4.1.15). if M is a flat R-module, then $IM \cap JM = (I \cap J)M$ for ideals of A. ⌟

Proof: Tensoring the exact sequence $0 \to I \cap J \to I \oplus J \to J \cup J \to 0$ with M. □

Prop. (5.4.1.16) [Local & Infinitesimal Criterion of Flatness]. Let $(A, \mathfrak{m}) \to (B, \mathfrak{n})$ be a local homomorphism of Noetherian local rings, and M is a finite B-module, then the following are equivalent:

- M is flat over A.
- $\mathrm{Tor}_1^A(M, A/\mathfrak{m}) = 0$.
- $M/\mathfrak{m}^n M$ is flat over $A/\mathfrak{m}^n$ for sufficiently large n.

⌟

Proof: $1 \to 2, 1 \to 3$ is trivial. For the converse, we need to prove $\mathrm{Tor}^1_A(M, A/I) = 0$ for any ideal $I \subset A$, or $I \otimes M \to M$ is injective.

If 2 holds, then $\mathrm{Tor}_1^A(M, N) = 0$ for any A-module of finite length, because by devissage we can reduce N to $A/\mathfrak{m}$.

Tensoring the exact sequence $0 \to \mathfrak{m}^n \cap I \to I \to I/I \cap \mathfrak{m}^n \to 0$ with M, we get

$$\mathfrak{m}^n \cap I \otimes M \to I \otimes M \to (I/I \cap \mathfrak{m}^n) \otimes M \to 0$$

and also the exact sequence $0 \to I/I \cap \mathfrak{m}^n \to R/\mathfrak{m}^n \to R/(I + \mathfrak{m}^n) \to 0$ gives

$$0 \to (I/I \cap \mathfrak{m}^n) \otimes M \to M/\mathfrak{m}^n M \to M/(I + \mathfrak{m}^n)M \to 0$$

by the fact $R/(I + \mathfrak{m}^n)$ has finite length in case2 or the fact they are all $R/\mathfrak{m}^n M$ modules in case3.

Thus the kernel of $I \otimes M \to M$ is contained in $(\mathfrak{m}^n \cap I) \otimes M$ for any n, which means it is contained in $\mathfrak{m}^n(I \cap M)$ for any n by Artin-Rees(5.2.2.13). Thus the kernel is trivial by Krull's intersection theorem(5.2.2.14) as $I \otimes M$ is finite over S. □

Prop. (5.4.1.17). ⌟

Flat ring extension

Prop. (5.4.1.18)[Flatness is Local]. Flatness is stalkwise both on the target and source, thus flatness is local both on the target and the source(5.1.4.2). ⌟

Cor. (5.4.1.19) [Going-down]. Going-down holds for flat ring map. ⌟

Proof: The ring map $R_{\mathfrak{p}'} \to S_{\mathfrak{q}'}$ is flat by(5.4.1.18), thus it is f.f. by(5.4.1.23). Then(5.4.1.21) says $\mathfrak{p} \subset \mathfrak{p}'$ is in the image. □

Prop. (5.4.1.20). if rings $A \subset B \subset C$ and $C/A, C/B$ is flat, then B/A is flat. ⌟

Proof: Cf.[GAGA Serre P26]. □

Prop. (5.4.1.21). The following are equivalent:

- $A \to B$ is f.f.
- It is flat and $\mathrm{Spec}\, B \to \mathrm{Spec}\, A$ is surjective.
- It is flat and Spec map contains all the closed pts.

⌟

Proof: This follows form(5.4.1.5) as we see that $\mathfrak{p}$ is in the image of Spec map iff $k(\mathfrak{p})\otimes_A B\neq 0$. □

Cor. (5.4.1.22). Integral flat injective ring extension is f.f., by(5.2.1.5). ⌟

Cor. (5.4.1.23). Flat local ring map of local rings is f.f.. ⌟

Cor. (5.4.1.24). Filtered colimits of f.f. rings over R is f.f. ⌟

Proof: If is flat by(5.4.1.6), and for a maximal ideal $\mathfrak{m}$ of R, $S_i/\mathfrak{m}S_i$ is non-zero, hence there direct limit is non-zero because 1 is contained. So $\mathfrak{m}$ is in the image, hence it is f.f. by(5.4.1.21). □

Cor. (5.4.1.25)[Filtered Colimit of Flat Ring Maps]. If I is filtered and $R_i\to S_i$ are (faifhfully)flat ring maps, then $\mathrm{colim}_I R_i\to \mathrm{colim}_I S_i$ is (faithfully)flat. ⌟

Proof: For any $\mathrm{colim}\, R_i$-module M, $(\mathrm{colim}\, S_i)\otimes_{\mathrm{colim}\, R_i} M=\mathrm{colim}(S_i\otimes_{R_i} M)$, so it is flat, because colim is exact. For the faithfully flatness, for any maximal ideal $\mathfrak{m}$ of $\mathrm{colim}\, R_i$, let $\mathfrak{m}_i=\mathfrak{m}\cap R_i$, then $S_i/\mathfrak{m}_iS_i\neq 0$, thus the direst limit is also $\neq 0$, so $\mathfrak{m}$ is in the image, hence it is f.f. by(5.4.1.21). □

Prop. (5.4.1.26). If $R\to S$ is (faithfully)flat ring map and M is a (faithdully)flat S-module, then M is a (faithfully)flat R-module. In particular, (faithfully) flatness is stable under composition. Also (faithfully)flatness is stable under base change. ⌟

Prop. (5.4.1.27). If B is flat over A, then

$$\mathrm{Tor}_i^A(M,N)\otimes B=\mathrm{Tor}_i^B(M_{(B)},N_{(B)}),\quad \mathrm{Ext}_i^A(M,N)\otimes B=\mathrm{Ext}^B(M_{(B)},N_{(B)}).$$

⌟

Prop. (5.4.1.28) [Faithfully Flat Ring Map is Injective]. A f.f. ring map $R\to S$ is universally injective. In particular, tensoring with R/I, we get $R\cap IS=I$ for an ideal I of R. ⌟

Proof: Because $R\to S$ is f.f., we only need to show that $N\otimes_R S\to N\otimes_R S\otimes_R S$ is injective for any N, but this is true because it has a left inverse. □

Prop. (5.4.1.29). A f.f. map between valuation rings is equivalent to an injective local homomorphism. ⌟

Prop. (5.4.1.30). A flat ring map maps a non-zero-divisor to a non-zero-divisor, because if we consider the principal ideal generated by it, then(5.4.1.2) shows the ideal in M is also injective, so it is not a zero-divisor. ⌟

Prop. (5.4.1.31) [Noetherian Completion is Flat]. If A is Noetherian and I is an ideal, the the I-adic completion $A^\wedge$ is flat over A by(5.2.3.14). ⌟

Prop. (5.4.1.32) [Flat Map is Open]. The Spec map of a ring map $R\to S$ of f.p. that satisfies going-down(e.g. flat), is open. ⌟

Proof: $S\to S_f$ satisfies going-down and is of f.p, so we see that $R\to S_f$ satisfies going down. It suffice to prove the image of this map is open. By Chevalley, the image is constructible, and it is stable under generalization. So it is open by(4.12.4.8). □

Cor. (5.4.1.33). The Spec map f of a f.f. ring map is an quotient map. ⌟

Prop. (5.4.1.34) [Generic Freeness+F.P.]. Let R be a reduced ring, S a f.g. R-algebra, M a finite S-module, and R is reduced, then there exists an open dense subset $U \subset \operatorname{Spec} R$ that there is a covering of U by standard opens $D(f)$ s.t.

- M_f and S_f are free over R_f.
- S_f is a f.p. R_f-algebra.
- M_f is a f.p. S_f-module.

In particular, it is generically flat. ⌟

Proof: Cf.[Sta]051Z.**?** □

Prop. (5.4.1.35) [Miracle Flatness]. Let $f : A \to B$ be a local map of local Noetherian rings s.t.

- A is regular.
- B is Cohen-Macauley.
- $\dim B = \dim A + \dim(A/f(\mathfrak{m}_A)B)$.

Then f is flat. ⌟

Proof: Cf.[Sta]00R4. □

Prop. (5.4.1.36) [Slicing Criterion for Flat Modules on the Target]. Let $R \to S$ be a local homomorphism of local rings s.t.

- S is essentially of f.p. over R,
- M is of f.p. over S,
- $\operatorname{Tor}_1^R(M, R/I) = 0$.
- M/IM is flat over R/I.

Then M is flat over R. ⌟

Proof: Cf.[Sta]0471.**?** □

Prop. (5.4.1.37) [Slicing Criterion for Flatness on the Source]. Let $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a local homomorphism of local rings s.t.

- S is essentially of f.p. over R,
- S is flat over R,
- t is a non-zero divisor of $S/\mathfrak{m}S$.

Then S/fS is flat over R, and f is a non-zero divisor in S. ⌟

Proof: Cf.[Sta]046Z. □

Prop. (5.4.1.38) [Fibral Criterion of Flat Modules]. Let $R \to S \to S'$ be local homomorphisms of local rings and $\mathfrak{m}$ is the maximal ideal of R. If

- $R \to S'$ is essentially of f.p.
- $R \to S$ is essentially of f.t.
- $M \neq 0 \in \mathcal{M}\mathrm{od}(S')$ is of f.p. over S.
- $M/\mathfrak{m}M$ is flat over $S/\mathfrak{m}S$.
- M is flat over R.

Then S is essentially of f.p. and flat over R and M is flat over S. ⌟

Proof: [Sta]05UV. □

2 Faithfully Flat Descent

Prop. (5.4.2.1) [Faithfully Flat Descent]. List of properties that descent through faithfully flat morphism. Let $R \to R'$ be a f.f. ring map.

1. Finiteness for modules over a ring.
2. F.p. for modules over a ring.
3. Flatness for modules over a ring.
4. Finite locally freeness and invertibility for modules over a ring.
5. Mittag-Leffler for modules over a ring.
6. Projectiveness for modules over a ring.
7. F.g. for ring maps.
8. F.p. for ring maps, both on the target and source.
9. (Formal)Smoothness for ring maps.
10. Noetherian for rings.
11. Reducedness for rings.
12. Normal for rings.
13. Regular for rings.
14. Being Noetherian and has property (R_k) for rings.
15. Local Complete Intersection ring maps.

$\lrcorner$

Proof:

1. Cf.[Sta]03C4.
2. Cf.[Sta]03C4.
3. Let M be a R-module, and $M' = M \otimes_R R'$, if M' is R-flat, then for any R-module N, $(N \otimes_R M) \otimes_R S = (N \otimes_R S) \otimes_S M'$, so as $\cdot \otimes_R S$ is exact and reflects exactness, $\cdot \otimes_R M$ is exact, so M is R-flat.
4. This follows from f.f. descent for f.p. and flatness and(5.3.1.7).
5. Cf.[Sta]05A5.
6. Cf.[Sta]05A9.
7. Cf.[Sta]00QP.
8. Cf.[Sta]00QQ, 00EP.
9. Use criterion(5.4.5.3), we see by flatness that the sequence $I/I^2 \to \Omega_{P/R} \otimes_P S \to \Omega_{S/R} \to 0$ commutes with flat base change, and when it is f.f., then use(5.4.3.6) and descent for projectiveness(5.4.2.1) that $\Omega_{S/R}$ is projective, so it is a split exact sequence. The smooth case follows from definition(5.4.5.12) as f.p. can descend.
10. Because for $S \to S'$ faithfully flat and a chain of ideals I_k in S, $I_k S' = I_k \otimes_S S'$, and $I_k S'$ is stable if S' is Noetherian, so also I_k is stable because it is faithfully flat.
11. $S \to S'$ is f.f. hence injective(5.4.1.28).

12. Normality is stalkwise, so it suffices to assume $R \to S$ is f.f. and R, S are both local. Then S is normal integral thus by(5.4.1.28), R is also normal integral. Now if $a/b \in R$, then $a/b \in S$, $a \in bS$, thus $a \in bS \cap R = bR$ by(5.4.1.28), so $a/b \in R$.
13. Cf.[Sta]07NG.?
14. Cf.[Sta]0353.
15. flatness and f.p. both satisfies f.f. descent, so it suffices to show that if $\mathfrak{p}' \subset R'$ is a prime lying over $\mathfrak{p} \subset R$, then $S \otimes_R k(\mathfrak{p})$ is a local complete intersection iff $S' \otimes_{R'} k(\mathfrak{p}') = S \otimes_R k(\mathfrak{p}) \otimes_{k(\mathfrak{p})} k(\mathfrak{p}')$ is a local complete intersection, and this follows from [Sta]00SI.

□

Prop. (5.4.2.2) [fpqc-Poincaré Lemma]. If a ring map $A \to B$, either has a section $B \to A$, or it is faithfully flat, then the Amitsur complex $s(M)$ for the canonical descent datum (with augmentation):

$$0 \to M \to B \otimes_A M \to B \otimes_A B \otimes_A M \to \dots$$

with Čech-like maps, is exact. ⌟

Proof: In the case $A \to B$ has a section s, It suffices to construct a nullhomotopy of the case $M = A$. Then we can just let $h(e_0 \otimes e_1 \otimes \dots \otimes e_r) = s(e_0)e_1 \otimes \dots \otimes e_r$.

The f.f. case can be reduced to the first case by tensoring B to consider $B \to B \otimes_A B$, because it has a section. □

Cor. (5.4.2.3) [Glueing Functions]. Let R be a commutative ring, M a R-module, and $(f_1, \dots, f_n) = (1)$, then there is an exact sequence

$$0 \to M \to \prod_i M_{f_i} \rightrightarrows \prod_{i,j} M_{f_i f_j}.$$

In particular this holds for $M = R$. ⌟

Proof: This is just(5.4.2.2) applied to $A \to \prod_i A_{f_i}$, which is faithfully flat. □

Formal Glueing of Modules

Main references are [Sta]Chap15.80 and 15.81.

Lemma (5.4.2.4). Let $R \to S$ be a ring map and $I = (f_1, \dots, f_r) \subset R$ be an ideal, then for any R-module M we can define a complex

$$0 \to M \xrightarrow{\alpha} M \otimes_R S \times \prod M_{f_i} \xrightarrow{\beta} \prod (M \otimes_R S)_{f_i} \times \prod M_{f_i f_j}$$

where $\alpha(m) = (m \otimes 1, m, \dots, m)$, $\beta(m', m_1, \dots, m_t) = (m' - m_1 \otimes 1, m' - m_2 \otimes 1, \dots, m' - m_t \otimes 1, m_1 - m_2, \dots, m_{t-1} - m_t)$.

Assume that $R \to S$ is flat and $R/I \to S/IS$ is an isomorphism, then this complex is exact. ⌟

Proof: Cf.[Sta]05EK. □

Def. (5.4.2.5) [Category of Gluing Data]. Let $R \to S$ be a ring map and $I = (f_1, \dots, f_r) \subset R$ be an ideal, then we define the category $Glue(R \to S, f_1, \dots, f_r)$ of gluing data $Glue(R \to S, f_1, \dots, f_t)$ consisting of objects $M = (M', M_i, \alpha_i, \alpha_{ij})$ where M' is a S-module, M_i are R_{f_i}-modules, $\alpha_i : (M')_{f_i} \to M_i \otimes_R S$ and $\alpha_{ij} : (M_i)_{f_j} \to (M_j)_{f_i}$ are isomorphisms that

- $\alpha_{ij}\circ\alpha_i=(\alpha_j)_{f_i}$.
- $\alpha_{jk}\circ\alpha_{ij}=\alpha_{ik}$.

There is a canonical functor $Can:\mathcal{M}\mathrm{od}_R\to Glue(R\to S,f_1,\dots,f_r)$ and also a morphism $H^0:Glue(R\to S,f_1,\dots,f_r)\to\mathcal{M}\mathrm{od}_R$ where

$$H^0(M)=\ker(M'\times\prod M_i\to\prod M'_{f_i}\times\prod(M_i)_{f_j}).$$

H^0 is a left inverse of Can, by(5.4.2.4). ⌟

Lemma (5.4.2.6). If $R\to S$ is flat, then $Glue(R\to S,f_1,\dots,f_r)$ is an Abelian category, and Can is an exact functor that commutes with arbitrary colimits.

If moreover $(f_1,\dots,f_r)=R$, then Can and H^0 induces an equivalence of categories. ⌟

Proof: The kernels and cokernels can be constructed because $-\otimes_R S$ is exact, and Can is exact because R_{f_i} and S are flat over R, and also tensoring commutes with taking colimits.

For the last assertion, by(5.4.2.5) it suffices to show that Can is essentially surjective. For this, just use(5.4.2.3) on both R and S. □

Prop. (5.4.2.7). In the setting of(5.4.2.5), if $R/I\to S/IS$ is an isomorphism, then Can and H^0 induces an equivalence of categories. ⌟

Proof: Cf.[Sta]05ER. □

Cor. (5.4.2.8). If $R\to S$ is a flat ring map and $f\in R$ that $R/fR\cong S/fS$ is an isomorphism, then there is a pullback diagram of categories:

$$\begin{array}{ccc}\mathcal{M}\mathrm{od}_R & \longrightarrow & \mathcal{M}\mathrm{od}_{R_f}\\ \downarrow & & \downarrow\\ \mathcal{M}\mathrm{od}_S & \longrightarrow & \mathcal{M}\mathrm{od}_{S_f}\end{array}$$

and we can also restrict to the category of f.g./f.p/flat/projective(any property satisfying f.f. descent) modules. ⌟

Proof: For the last assertion, notice $R\to R^\wedge\times\prod R_{f_i}$ is f.f. by(5.2.3.7), then use f.f. descent(5.4.2.1). □

Cor. (5.4.2.9). If R is a Noetherian ring, $f\in R$ and $R^\wedge$ the f-adic completion of R, then there is an pullback of categories:

$$\begin{array}{ccc}\mathcal{M}\mathrm{od}_R & \longrightarrow & \mathcal{M}\mathrm{od}_{R_f}\\ \downarrow & & \downarrow\\ \mathcal{M}\mathrm{od}_{R^\wedge} & \longrightarrow & \mathcal{M}\mathrm{od}_{R^\wedge_f}\end{array}$$

and we can also restrict to the category of f.g./f.p/flat/projective(any property satisfying f.f. descent) modules. ⌟

Proof: This satisfies the hypothesis of(5.4.2.7) by(5.2.3.14). □

Def. (5.4.2.10) [Gluing Pairs]. Let $R \to R'$ be a ring map and $f \in R$ that induces an isomorphism $R/f^n R \cong R'/f^n R'$ for any $n > 0$, then $(R \to R', f)$ is called a **gluing pair** if the sequence

$$0 \to R \to R' \oplus R_f \to R'_f \to 0$$

is exact. The pair (R, f) is called a gluing pair if $(R \to \widehat{R}, f)$ is a gluing pair(This makes sense by(5.2.3.6)).

This is equivalent to $R[f^\infty] \to R'[f^\infty]$ is bijective.

Let M be an R-module, then M is called a **glueable module** for $(R \to R^\wedge, f)$ if the sequence

$$0 \to M \to M_{R'} \oplus M_{R_f} \to M_{R'_f} \to 0$$

is exact.

This is equivalent to $M[f^\infty] \to M_{R'}[f^\infty]$ is a bijection. And when $(R \to R', f)$ is a gluing pair, this is equivalent to $M[f^\infty] \to M_{R'}[f^\infty]$ is injective. ⌟

Proof: Cf.[Sta]0BNR, 0BNW. □

Prop. (5.4.2.11) [Flatness and Gluing]. $(R \to R', f)$ is a gluing pair when $R \to R^\wedge$ is flat. In particular (R, f) is a gluing pair then R is Noetherian or f is a nonzero-divisor(5.2.3.10), Cf.[Sta]0BNT.

If $(R \to R', f)$ is gluing, then M is glueable if $\mathrm{Tor}_1^R(M, R')$ is f-power torsion, or equivalently $\mathrm{Tor}_1^R(M, R'_f) = 0$. In particular this is the case when M is flat R-module or f is not a zero-divisor. And when $R \to R'$ is flat, any R-module M is glueable, in particular this is the case for (R, f) when R is Noetherian. Cf.[Sta]0BNX. ⌟

Prop. (5.4.2.12) [Beauville-Laszlo]. Let A be a commutative ring and $f \in A$ is a nonzero-divisor, let $\widehat{A}$ be the f-adic completion, then there is a pullback diagram of categories:

$$\begin{array}{ccc} \mathcal{M}\mathrm{od}_A & \longrightarrow & \mathcal{M}\mathrm{od}_{A[\frac{1}{f}]} \\ \downarrow & & \downarrow \\ \mathcal{M}\mathrm{od}_{\widehat{A}} & \longrightarrow & \mathcal{M}\mathrm{od}_{\widehat{A}[\frac{1}{f}]} \end{array}$$

⌟

Proof: Cf.[Sta]Ch15.81. □

3 Kähler Differentials

Def. (5.4.3.1) [Derivations]. A **derivation** over S from an S-algebra R to an S-module M is a morphism of S-modules $\delta : R \to M$ that $\delta(ab) = a\delta(b) + b\delta(a)$. The set of all derivatives from R to M is denoted by $\mathrm{Der}_S(R, M)$ ⌟

Def. (5.4.3.2) [$A \ltimes_R M$]. For any R-algebra A, there is a functor $A \ltimes -$ from $\mathcal{M}\mathrm{od}_R$ to $(Alg_R)_{/A}$ that $A \ltimes_R M = A \otimes M$ with the algebra given by

$$(a, x)(b, y) = (ab, ay + bx).$$

Then there is a bijection of sets

$$(\mathcal{C}\mathcal{A}\mathrm{lg}_R)_{/A}(X, A \ltimes_R M) \cong \mathrm{Der}_R(X, M).$$

⌟

Def. (5.4.3.3) [Kähler Differential]. Let $S \to R$ a ring map, Then the **Kahler Differential** $\Omega_{R/S}$ is defined as a R-module that $\mathrm{Der}_S(R, M) \cong \mathrm{Hom}_S(\Omega_{R/S}, M)$. In particular, $\mathrm{Der}_S(R, R)$ is the R-dual of $\Omega_{R/S}$. ⌟

Prop. (5.4.3.4). One construction is by the free group generated by elements of R module some relations.

It can also be constructed as follows: there are two ring maps λ_i from S to $R \otimes_R S$, and one map ε from $S \otimes_R S$ to S. Let $I = \ker \varepsilon$ as a R module by λ_1, then $I/I^2 \cong \Omega_{S/R}$ by (5.4.3.8) that

$$0 \to I/I^2 \to \Omega_{S\otimes_R S/S} \otimes_{S\otimes_R S} S \to \Omega_{S/S} \to 0.$$

So $I/I^2 \cong \Omega_{S/R} \otimes_S (S \otimes_R S) \otimes_{S\otimes_R S} S \cong \Omega_{S/R}$. And it can be verified that $a \otimes 1 - 1 \otimes a$ corresponds to da. ⌟

Prop. (5.4.3.5) [Adjointness]. The functor $X \to A \otimes_X \Omega_{X/R}$ is left adjoint to the functor $A \ltimes_R -$ defined in(5.4.3.2) as a functor from $(\mathcal{CA}\mathrm{lg}_R)_{/A} \to \mathcal{M}\mathrm{od}_A$. ⌟

Proof: Because they are both equivalent to $\mathrm{Der}_R(X, M)$. □

Cor. (5.4.3.6) [Functoriality]. From the first construction, we can see directly that for a family of morphisms $R_i \to S_i$,

$$\Omega_{\mathrm{colim}\, S_i/\,\mathrm{colim}\, R_i} = \mathrm{colim}\, \Omega_{S_i/R_i}.$$

In particular, we have:

$$T^{-1}\Omega_{B/A} = \Omega_{T^{-1}B/A}, \quad \Omega_{S^{-1}B/S^{-1}A} = S^{-1}\Omega_{B/A}.$$

Moreover, we have

$$\Omega_{S/R} \otimes_R R' = \Omega_{S\otimes_R R'/R'}, \quad (S \otimes_R \Omega_{T/R}) \oplus (T \otimes_R \Omega_{S/R}) \cong \Omega_{S\otimes_R T/R}$$

by universal properties. ⌟

Proof: We prove for the localization: it suffices to show the following two assertions:

1. $S^{-1}\Omega_{A/B} \cong \Omega_{S^{-1}A/B}$.
2. If $T \subset B$ is a multiplicatively closed subset that $i(t)$ are all invertible in A, then $\Omega_{A/T^{-1}B} \cong \Omega_{A/B}$.

We check the universal properties: For any $S^{-1}A$-module M,

$$\mathrm{Hom}_{S^{-1}A}(S^{-1}\Omega_{A/B}, M) \cong \mathrm{Hom}_{S^{-1}A}(S^{-1}A \otimes_A \Omega_{A/B}, M) \cong \mathrm{Hom}_A(\Omega_{A/B}, M) \cong \mathrm{Der}_B(A, M),$$

$$\mathrm{Hom}_{S^{-1}A}(\Omega_{S^{-1}A/B}, M) \cong \mathrm{Der}_B(S^{-1}A, M)$$

There is a map $\mathrm{Der}_B(S^{-1}A, M) \to \mathrm{Der}_B(A, M)$ by restriction, and the converse is given by

$$d \mapsto d(\frac{a}{s}) = \frac{sda - ads}{s^2}.$$

This is well-defined as

$$d(\frac{at}{st}) = \frac{std(at) - atd(st)}{s^2t^2} = \frac{sda - ads}{s^2},$$

and it satisfies

$$\begin{aligned} d(\frac{a_1}{t_1}+\frac{a_2}{t_2}) &= d(\frac{a_1t_2+a_2t_1}{t_1t_2}) \\ &= \frac{(a_1d(t_2)+t_2d(a_1)+a_2d(t_1)+t_1d(a_2))t_1t_2-(a_1t_2+a_2t_1)(t_1d(t_2)-t_2d(t_1))}{t_1^2t_2^2} \\ &= \frac{t_1t_2^2d(a_1)+t_1^2t_2d(a_2)-a_2t_1^2d(t_2)+a_1t_2^2d(t_1)}{t_1^2t_2^2} \\ &= d(\frac{a_1}{t_1})+d(\frac{a_2}{t_2}) \end{aligned}$$

$$\begin{aligned} d(\frac{a_1a_2}{t_1t_2}) &= \frac{(a_1d(a_2)+a_2d(a_1))t_1t_2-a_1a_2(t_1d(t_2)+t_2d(t_1))}{t_1^2t_2^2} \\ &= \frac{a_1(t_2d(a_1)-a_2d(t_2))}{t_1t_2^2}+\frac{a_2(t_1d(a_2)-a_1d(t_1))}{t_2t_1^2} \\ &= \frac{a_1}{t_1}d(\frac{a_2}{t_2})+\frac{a_2}{t_2}d(\frac{a_1}{t_1}) \end{aligned}$$

Thus this d is an extension of the derivative to $S^{-1}A$. Thus we get the desired isomorphism by Yoneda lemma. □

Prop. (5.4.3.7) [Jacobi-Zariski Sequences]. For a sequence of commutative rings: $A \to B \to C$, there is an exact sequence

$$C\otimes_B \Omega_{B/A} \to \Omega_{C/A} \to \Omega_{C/B} \to 0$$

of C-modules. It has a left inverse and splits iff any derivation over A from B to a C-module can be extended to a derivation over A from C to M. This is trivially true when $B \to C$ has a retraction, and true when C/B is formally smooth by(5.4.5.5). ⌟

Proof: Taking Hom with an arbitrary C-module M, by universal property, we need to check the exactness of $0 \to \mathrm{Der}_B(C,M) \to \mathrm{Der}_A(C,M) \to \mathrm{Der}_A(B,M)$, which is easy. □

Prop. (5.4.3.8) [Second Exact Sequence]. (This is a special case of(7.1.1.5)). If $S' = S/I$, then there is an exact sequence of R'-modules:

$$I/I^2 \to \Omega_{S/R}\otimes_S S' \to \Omega_{S'/R} \to 0.$$

Where $f\in I$ is mapped to $df\otimes 1$ and it has a left inverse and splits iff $S/I^2 \to S'$ has a right inverse.

And in fact $\Omega_{S/R}\otimes S' \cong \Omega_{(S/I^2)/R}\otimes S'$. ⌟

Proof: For a S/I-module M, we check:

$$0 \to \mathrm{Der}_R(S/I,M) \to \mathrm{Der}_R(S,M) \to \mathrm{Hom}_{S/I}(I/I^2,M)$$

To prove $\Omega_{S/R}\otimes S' \cong \Omega_{(S/I^2)/R}\otimes S'$, we apply Hom for a S'-module M.

So to prove the left exactness, we may assume $I^2 = 0$. If we have an inverse $\Omega_{S/R}\otimes_S S' \to I$. then it gives a derivation $D: A \to I$ that is identity on I, so $a - D(a)$ gives a R-ring map $S \to S$ that is trivial on I(because $I^2 = 0$). Hence it gives a $S/I \to S$ that is inverse to the projection.

For the converse, if $d: S/I \to S$ is a right inverse, then $a - d(\overline{a})$ is a derivation $S \to I$, which is identity on I, so it gives a inverse map $\Omega_{S/R}\otimes_S S' \to I$ by universal property. □

Cor. (5.4.3.9). If $R \to S$ is of f.p., then $\Omega_{S/R}$ is of f.p. over S. If $R \to S$ is of f.t., then $\Omega_{S/R}$ is of f.t. over S. (Follows from the second exact sequence(5.4.3.8) and(5.4.3.10)). ⌟

Cor. (5.4.3.10) [Examples].

1. $\Omega_{A[X_1,\ldots,X_n]/A} = A[X_1,\ldots,X_n]\{dX_1,\ldots,dX_n\}$.
2. If $S = A[X_i]/\{f_j\}$, then $\Omega_{S/A} = S[dX_i]/\{df_j\}$.
3. $\Omega_{A[X_i]/k} = \Omega_{A/k} \otimes_A A[X_i] \oplus A[X_i]\{dX_1 \ldots, dX_n\}$.
4. (Standard Étale Algebra)For $A = R[x]_g/(f)$, where f' has image invertible in $A, \Omega_{A/R} = 0$.
5. The differential for the inclusion $k[y^2, y^3] \to k[y]$ is $k[y]/(2y, 3y^2)\{dy\}$.

⌟

Cor. (5.4.3.11). 1: Use the differential operator and universal property.

2: Use item1 and(5.4.3.8).

3: Use item1 and the fact(5.4.3.8) splits because any derivative of A/k can be extended to derivative of B/k by acting on the coefficients.

4:

5: Use definition. ⌟

Cor. (5.4.3.12). If S/I is a field k that embeds in S, then $I/I^2 \cong \Omega_{S/k} \otimes_S k$. ⌟

Prop. (5.4.3.13). Let $k \subset K \subset L$ be fields, and L/K f.g., then

$$\dim_L \Omega_{L/k} \geq \dim_K \Omega_{K/k} + \operatorname{tr.deg}(L/K).$$

Equality holds if L/K is separably generated, i.e. separable over a transcendental basis. If $K = k$, then the equality hold iff L/k is separably generated. In particular, L/k is separable algebraic extension iff $\Omega_{L/k} = 0$. ⌟

Proof: Take a subfield $K \subset K(t_1,\ldots,t_n) \subset L$ that L is separable algebra over $K(t_1,\ldots,t_n)$. Then it suffices to add one element a time, so we may assume $L = K(\alpha)$.

1: If α is transcendental over K, then $\Omega_{K[\alpha]/t} \cong \Omega_{K/k} \otimes K[\alpha] \oplus K[\alpha]dt$ by(5.4.3.10), and by localization(5.4.3.6) we get $\Omega_{L/K} \cong \Omega_{K/k} \otimes_K L \oplus Ldt$, thus $\operatorname{rank}\Omega_{L/k} = \operatorname{rank}\Omega_{K/k} + 1$.

2: If α is separable over K, then there is a monic polynomial $f \in K[X]$ that $K[\alpha] \cong K[X]/(f)$. Then f' is invertible in $K[\alpha]$, and by(5.4.3.10) $\Omega_{K[\alpha]/k} = \Omega_{K/k} \otimes_K L \oplus LdX/(d(f) + f'dX) \cong \Omega_{K/k} \otimes_K L$. Thus $\operatorname{rank}\Omega_{L/k} = \operatorname{rank}\Omega_{K/k}$.

3: If K has characteristic p and $L = K[X]/(X^p - a)$ and $d_{K/k}(a) = 0$, then $\Omega_{K[\alpha]/k} = \Omega_{K/k} \otimes_K L \oplus LdX/(d(a)) \cong \Omega_{K/k} \otimes_K L \oplus LdX$. Thus $\operatorname{rank}\Omega_{L/k} = \operatorname{rank}\Omega_{K/k} + 1$.

4: If K has characteristic p and $L = K[X]/(X^p - a)$ and $d_{K/k}(a) \neq 0$, then $\Omega_{K[\alpha]/k} = \Omega_{K/k} \otimes_K L \oplus LdX/(d(a))$ has rank $\operatorname{rank}\Omega_{K/k}$.

Thus the assertion is clear. □

Prop. (5.4.3.14) [Differential and Regularity]. Let B be a Noetherian local ring containing its residue field k and k is perfect, then $\Omega_{B/k}$ is a free B-module of rank $\dim B$ iff B is regular. [Hartshorne Ex.2.8.1] has a generalization of this fact. ⌟

Proof: One way is by(5.4.3.12). Conversely, if B is regular, then it is integral(5.3.5.19), so $\Omega_{B/k} \otimes_B K = \Omega_{K/k}$(5.4.3.6) is of K-dimension $tr.\deg K/k = \dim B$, where K is the quotient field of B, and $\Omega_{B/k} \otimes k \cong m/m^2$ is of k-dimension $\dim B$ once again. These two facts shows that $\Omega_{B/k}$ is free B-module of rank $\dim B$ by(5.4.8.1). □

Prop. (5.4.3.15). The Kähler differential $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$ for an extension of number fields is cyclic. ⌟

Proof: Because it is locally cyclic**?**(5.2.7.34). □

4 Complete Intersections

Koszul Complex

Prop. (5.4.4.1) [Koszul Complex]. The complex of $\mathbb{Z}[X_1,\ldots,X_n]$-modules $K_\bullet$, where

$$K_r = \wedge^{r+1}\mathbb{Z}[dX_1,\ldots,dX_n]\otimes_{\mathbb{Z}}\mathbb{Z}[X_1,\ldots,X_n]$$

and the morphism is given linearly by

$$\iota : dX_{i_0}\wedge dX_{i_1}\wedge\ldots\wedge dX_{i_r}\mapsto\sum_k X_{i_k}dX_{i_0}\wedge\ldots\wedge dX_{i_{k-1}}\wedge dX_{i_{k+1}}\wedge\ldots\wedge dX_{i_r}$$

Then this is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}[X_1,\ldots,X_n]$. ⌟

Proof: We can use induction. If $r=1$, then this is clear. For the induction process, if $\iota(dX_1\wedge\alpha+\beta)=0$, and $\beta\in K_i$, where β,α has no dX_1 involved. Notice if $dX_1\wedge\alpha\in K_0$, then we may assume α has no constant coefficient, because this is impossible.

then $X_1\alpha - dX_1\wedge\iota(\alpha)+\iota(\beta)=0$. Then we see that $\iota(\alpha)=0$. We can write $\alpha=\alpha_0+X_1\alpha_1+X_1^2\alpha_2+\ldots$, where α_i has no X_i involved, then we see that $\iota(\alpha_i)=0$, then by induction hypothesis $\alpha=\iota(\alpha')$(notice α_0 has no constant coeffienct), and $\iota(\beta)+X_1\iota(\alpha')=0$. If $\beta=X_1\beta_1+\beta_2$, where β_2 has no X_1 involved, then $\iota(\beta_2)=0$, so $\beta_2=\iota(\beta_2')$, and $\iota(\beta_1+\alpha')=0$, so $\beta_1+\alpha'=\iota(\beta_1')$. So

$$dX_1\wedge\alpha+\beta = dX_1\wedge\iota(\alpha')+\iota(X_1\beta_1'+\beta_2')-X_1\alpha'=\iota(X_1\beta_1'+\beta_2'-dX_1\wedge\alpha').$$

And in degree0, this is clear. □

Def. (5.4.4.2) [Koszul Complex]. Let A be a ring and $I=(f_1,\ldots,f_n)\in A$ is an ideal, then the **Koszul complex** for $Kos(A,f_1,\ldots,f_n)$ is an object in $D(A)$ defined by

$$Kos(A,f_1,\ldots,f_n)=A\otimes^L_{\mathbb{Z}[X_1,\ldots,X_n]}\mathbb{Z},$$

where A is a $\mathbb{Z}[X_1,\ldots,X_n]$-algebra by mapping $X_i\to f_i$. If M is an A-module, then we define $Kos(M,f_1,\ldots,f_n)=M\otimes^L_A Kos(A,f_1,\ldots,f_n)$. ⌟

Prop. (5.4.4.3). If $f_1,\ldots,f_n\in R$, then $I=(f_1,\ldots,f_n)$ annihilates $H^*(K(f_1,\ldots,f_n))$. In particular, $Kos(A,f_1,\ldots,f_n)$ is in the image of $D(A/I)\subset D(A)$. ⌟

Proof: This is because every $H^i(A\otimes^L_{\mathbb{Z}[X_1,\ldots,X_n]}\mathbb{Z})$ is an $H^0(A\otimes^L_{\mathbb{Z}[X_1,\ldots,X_n]}\mathbb{Z})=A/I$-algebra, because it is a simplicial algebra. □

Prop. (5.4.4.4). $K(A,f_1,\ldots,f_n,g_1,\ldots,g_m)=K(A,f_1,\ldots,f_n)\otimes_A K(A,g_1,\ldots,g_m)$. (Easy). ⌟

Prop. (5.4.4.5). The cone of the map

$$f_n : K(f_1,\ldots,f_{n-1})\to K(f_1,\ldots,f_{n-1})$$

is isomorphic to $K(f_1,\ldots,f_n)$. ⌟

Proof: This is because $\mathbb{Z}[X]\xrightarrow{X}\mathbb{Z}[X]\to\mathbb{Z}$ is an exact triangle, so $A\xrightarrow{f_n}A\to A\otimes^L_{\mathbb{Z}[X]}\mathbb{Z}$ is an exact triangle, so $Kos(A,f_1,\ldots,f_{n-1})\xrightarrow{f_n}K(A,f_1,\ldots,f_{n-1})\to K(A,f_1,\ldots,f_n)$ is an exact triangle. □

Prop. (5.4.4.6). Let A be a ring and M be an A-module. Let $f_1,\ldots,f_{r-1},f,g$ be elements of A, then there is a natural distinguished triangle

$$Kos(M,f_1,\ldots,f_{r-1},f)\to Kos(M,f_1,\ldots,f_{r-1},fg)\to Kos(M,f_1,\ldots,g).$$

⌟

Proof: We use(5.4.4.5) to consider $Kos(M,f_1,\ldots,f_{r-1},f)$ as a cone of $f_n:Kos(M,f_1,\ldots,f_{r-1})\to Kos(M,f_1,\ldots,f_{r-1})$. Then this distinguished triangle is given by(4.8.4.15) applied to the diagram

$$\begin{array}{ccc} Kos(M,f_1,\ldots,f_{r-1}) & = & Kos(M,f_1,\ldots,f_{r-1}) \\ \downarrow f & & \downarrow fg \\ Kos(M,f_1,\ldots,f_{r-1}) & \xrightarrow{g} & Kos(M,f_1,\ldots,f_{r-1}) \end{array}$$

□

Prop. (5.4.4.7) [Koszul Complex and Čech Complex]. Let A be a commutative ring and $I=(f_1,\ldots,f_n)\subset A$, $K_n^\bullet=Kos(A,f_1^n,\ldots,f_r^n)=A\otimes^L_{\mathbb{Z}[X_1,\ldots,X_r]}\mathbb{Z}$. Then there are natural maps

$$\ldots\to K_3^\bullet\to K_2^\bullet\to K_1^\bullet$$

compatible with the inverse system $H^0(K_n^\bullet)=A/(f_1^n,\ldots,f_r^n)$. Then there is a description of $R\operatorname{colim}K_n^\vee$(5.9.5.6) as the alternating Čech complex

$$R\to\bigoplus_{i_0}R_{f_{i_0}}\to\bigoplus_{i_0<i_1}R_{f_{i_0}f_{i_1}}\to\ldots\to R_{f_1f_2\ldots f_r}$$

where R sits in degree 0. ⌟

Proof: Cf.[Sta]0913, which is not hard. □

Def. (5.4.4.8)[Koszul-Regular Sequence]. Let A be a ring and $(f_1,\ldots,f_n)\in A$ be a sequence, then $f_1,\ldots,f_n$ is called **M-Koszul-regular** iff $Kos(M,f_1,\ldots,f_n)=0$. It is called **Koszul-regular** iff $Kos(A,f_1,\ldots,f_n)=0$. ⌟

Prop. (5.4.4.9). If $(f_1,\ldots,f_r)$ is (M-Koszul)regular and $n_i>0$, then $(f_1^{n_1},\ldots,f_r^{n_r})$ is also (M-Koszul)regular. ⌟

Proof: This follows from(5.4.4.6). □

Prop. (5.4.4.10) [Regular and Koszul-Regular]. A M-regular sequence(5.3.4.1) is M-Koszul-regular. A regular sequence is Koszul-regular. ⌟

Proof: Let $(f_1,\ldots,f_r)$ be a regular sequence. The assertion is clear when $r=1$. For the induction:

$$\begin{aligned}Kos(M,f_1,\ldots,f_n)&=Kos(M,f_2,\ldots,f_n)\otimes^L_{\mathbb{Z}[X]}\mathbb{Z}=Kos(A,f_2,\ldots,f_n)\otimes^L_A M\otimes^L_{\mathbb{Z}[X]}\mathbb{Z}\\&=Kos(A/f_1,f_2,\ldots,f_n)\otimes^L_{A/f_1}M/f_1M=Kos(M/f_1M,f_2,\ldots,f_n)\end{aligned}$$

so we can use induction. □

Complete Intersections

Def. (5.4.4.11)[Global Complete Intersections]. A ring map $R \to S$ is called **global intersection** if $S = R[x_1, \ldots, x_n]/(f_1, \ldots, f_c)$ that every non-empty fiber of $\operatorname{Spec} S \to \operatorname{Spec} R$ has dimension $n - c$. ⌟

Prop. (5.4.4.12). Global intersection is stable under base change and composition. And $S \to S_f$ a global intersection, so it is stable under localization. ⌟

Proof: Base change: this is because flatness, f.p. is stable under base change, and the fibers are the same.

Localization: $S_f = S[X]/(fX - 1)$ has trivial fibers.

Composition: It suffices to assume R is a field and calculate the dimension of the fibers, which is true by dimension formula(5.2.4.13). □

Prop. (5.4.4.13)[Noetherian Approximation]. Let R be a ring and $S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c)$ is a global intersection over R, then there is a f.g. $\mathbb{Z}$-algebra $R_0 \subset R$ that $f_i \in R_0[X_1, \ldots, X_n]$, and $S_0 = R_0[X_1, \ldots, X_n]/(f_1, \ldots, f_c)$ is a global intersection over R. ⌟

Proof: Cf.[Sta]00SU. □

Prop. (5.4.4.14) [Complete Intersection is Regular]. Let R be a ring and $S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c)$ be a global complete intersection, then $\operatorname{Spec} S \to \operatorname{Spec} R[X_1, \ldots, X_n]$ is a regular embedding(6.6.8.1), and S is flat over R. ⌟

Proof: Cf.[Sta]00SV. □

Local Complete Intersections

Def. (5.4.4.15)[Local Complete Intersections]. Let S be a R-algebra, then S is a **local complete intersection** over R iff S is locally a global complete intersection over R. Local complete intersection is flat, by(5.4.4.14). ⌟

Prop. (5.4.4.16). Local complete intersection is local on the source and target. In fact satisfies f.f. descent(5.4.2.1). ⌟

Lemma (5.4.4.17). If S is a f.t. k-algebra and K/k is a field extension, then S is a local complete intersection iff S_K is a local complete intersection. ⌟

Prop. (5.4.4.18) [Global Intersections and Fibers]. Let $R \to S$ be a ring map and $\mathfrak{q} \subset S$ be a prime lying over $\mathfrak{p} \subset R$, then the following are equivalent:

- $R \to S$ is a global complete intersection around $\mathfrak{q}$.
- $R \to S$ is a f.p. around $\mathfrak{q}$, $S_\mathfrak{q}/R_\mathfrak{p}$ is flat, and (the fiber)$S_\mathfrak{q}/\mathfrak{p}S_\mathfrak{q}$ is a local complete intersection ring over $k(\mathfrak{p})$.

⌟

Proof: $1 \to 2$ follows from(5.4.4.14). For $2 \to 1$, Cf.[Sta]00SY. □

Prop. (5.4.4.19) [Local Complete Intersection over Fields is Stalkwise]. For a f.g. k-algebra S, S is a local complete intersection iff all localization at (maximal)primes are complete intersection local rings over k. In particular, being local complete intersection is a stalkwise property. ⌟

Proof: This is because over field everything is f.p. and flat, and use(5.4.4.18). □

Prop. (5.4.4.20). If S is a f.g. local complete intersection over a field k, then it is a CM ring. ⌟

Proof: Cf.[Sta]00SB. □

Def. (5.4.4.21) [Complete Intersection Local Rings]. Let A be a local ring essentially of f.t. over a field k, then A is called a **complete intersection local ring** over k if there exists a surjection $R \to A$ from a regular local ring essentially of f.t. over k that the kernel is generated by a regular sequence. ⌟

Prop. (5.4.4.22). When A is f.g. local ring over a field k, then A is a complete intersection local ring iff A is local complete intersection over k(5.4.4.11). ⌟

Proof: Cf.[Sta]00SC. □

See more in [Sta]Chap 23.8.

5 Smoothness

Formally Smoothness

Def. (5.4.5.1). A ring map $R \to S$ is called **formally smooth** if has right lifting property w.r.t all ring maps $A \to A/I$ where $I^2 = 0$.

Formal smooth is stable under base change and composition, by universal arguments. A polynomial algebra is formally smooth. ⌟

Prop. (5.4.5.2). Giving a presentation $S = P/J$ where P is formally smooth(e.g. polynomial algebra), S is formally smooth iff there is a map $S \to P/J^2$ that is right converse to the obvious projection. ⌟

Proof: One way is from the definition of formally smooth applied to P/J^2 and J. Conversely, for any A and I, we notice the map $P \to S \to A/I$ can be lifted to $P \to A$, and J is mapped to I, so J^2 is mapped to 0, so we have a map $P/J^2 \to A$. Then $S \to P/J^2 \to A$ is the lifting. □

Cor. (5.4.5.3). If $P \to S$ is a presentation of S/R by polynomial algebra with kernel I, then S/R is formal smooth iff

$$0 \to I/I^2 \to \Omega_{P/R} \otimes_P S \to \Omega_{S/R} \to 0$$

is split exact as in(5.4.3.8). ⌟

Proof: This sequence is split exact iff $P/J^2 \to S$ has a right converse, by(5.4.3.8). □

Now we consider the relation of Formal Smoothness and Kahler Differentials.

Cor. (5.4.5.4) [Equivalence Definition]. S/R is formally smooth iff $NL_{S/R}$ is quasi-isomorphic to a projective S-module at degree 0. ⌟

Proof: If S/R is formally smooth, then choose a presentation will suffice by(5.4.5.3). The converse is also true by projectiveness and(5.4.5.3). □

Cor. (5.4.5.5). If C/B is formally smooth, then the Jacobi-Zariski sequence

$$0 \to C \otimes_B \Omega_{B/A} \to \Omega_{C/A} \to \Omega_{C/B} \to 0$$

as in(5.4.3.7) is split exact, by(7.1.1.5). In particular, any derivation of B to a C-module can be extended to a derivation C to a C-module. ⌟

Cor. (5.4.5.6). If $A \to B \to C$ with $A \to C$ formally smooth and $B \to C$ surjective with kernel I, then there is an split sequence

$$0 \to I/I^2 \to \Omega_{B/A} \otimes_B C \to \Omega_{C/A} \to 0$$

by(7.1.2.6). ⌟

Standard Smooth Algebra

Def. (5.4.5.7). A **standard smooth algebra** over R is a algebra $S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c)$, where $c \leq n$ and $J(\frac{f_1,\ldots,f_c}{X_1,\ldots,X_c})$ is invertible in S. ⌟

Prop. (5.4.5.8) [Standard Smooth Localization]. If $R \to S$ is standard smooth, then $R \to S_g$ is standard smooth, and $R_f \to S_f$ is standard smooth(because stable under base change(5.4.5.9)). ⌟

Proof: For localization at $g \in S$, let h be an inverse image of g in $R[X_1, \ldots, X_n]$, then $S_g = R[X_1, \ldots, X_n, X_{n+1}]/(f_1, \ldots, f_c, X_{n+1}h - 1)$, and it is standard smooth. □

Prop. (5.4.5.9). Standard smoothness is stable under base change and composition. ⌟

Proof: For base change, notice the Jacobi matrix is the base change of the Jacobi matrix, so it is also invertible. For composition, write out the presentation, the determinant is the product of the presentation. □

Lemma (5.4.5.10) [Kähler Differential of Smooth Algebra is Free]. The Kähler differential of a standard smooth algebra S over a field k is free of rank $\dim S$, and $(f_1, \ldots, f_c)/(f_1, \ldots, f_c)^2$ is free over S with basis $f_1, \ldots, f_c$. Moreover, S is pure dimensional. ⌟

Proof: The naive cotangent complex for S/R is

$$d : (f_1, \ldots, f_c)/(f_1, \ldots, f_c)^2 \to S[dX_1, \ldots, dX_n].$$

By hypothesis and linear algebra it is a split injection, and $\Omega_{S/R} = S[dX_{c+1}, \ldots, dX_n]$, so it is free of rank $n - c = \dim S$, because S is a global complete intersection(5.4.5.11). □

Prop. (5.4.5.11) [Standard Smooth and Complete Intersection]. A standard smooth algebra $S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c)$ is a global complete intersection(5.4.4.11). ⌟

Proof: It suffices to show any fiber of S has dimension $n - c$. For this, notice $S \otimes_R k(\mathfrak{p})$ is also standard smooth, then we reduce to the field case. Now $I = (f_1, \ldots, f_c)$ satisfies $I/I^2 \to \oplus S dx_i$ is a split injection. For any maximal ideal $\mathfrak{m}$ containing I, tensoring $k(\mathfrak{m})$, we get an injection $I/\mathfrak{m}I \to \oplus k(\mathfrak{m}) dx_i$. Notice there is a commutative diagram

$$\begin{array}{ccc} I & \longrightarrow & S/\mathfrak{m} \otimes I \cong I/\mathfrak{m}I \\ \downarrow{\scriptstyle d} & & \downarrow{\scriptstyle incl} \\ \oplus S dx_i & \xrightarrow{dx_i \mapsto 1 \otimes x_i} & S/\mathfrak{m} \otimes \mathfrak{m} \cong \mathfrak{m}/\mathfrak{m}^2 \end{array}.$$

And the lower horizontal map is an isomorphism by Hilbert's Nullstellensatz, so the image of f_i in $\mathfrak{m}_i/\mathfrak{m}_i^2$ are linearly independent over $k(\mathfrak{m})$, thus we can use(5.3.5.22) to show that $\dim S = n - c$. □

Smoothness

Def. (5.4.5.12)[Smooth Ring Map]. A ring map $R \to S$ is called **smooth** if it satisfies the following equivalent conditions:

- It is of f.p. and the naive cotangent complex $NL_{S/R}$ is quasi-isomorphic to a finite locally free S-module placed at degree 0. In other words,
$$0 \to I/I^2 \to \Omega_{P/R} \otimes_P S \to \Omega_{S/R} \to 0$$
is exact and $\Omega_{S/R}$ is finite locally free. By(7.1.1.1), we only need to prove for a single presentation of S.
- It is locally standard smooth.
- It is formally smooth and of f.p..

We say S is smooth at x if it is smooth on a nbhd of x. ⌟

Proof: 1 → 3: by(5.4.5.4). 3 → 1: By(5.4.5.4), $\Omega_{S/R}$ is f.p. and projective, so it is finite projective.

At this point we already know that the first definition is stable under base change and composition, because f.p. and formally smoothness both do(5.4.5.1)(5.3.7.9).

And also the first definition is local on source because f.p. does(5.1.4.4) and NL commutes with localization(7.1.1.6) so we can use the local properties of triviality(5.1.4.2) and finite projectiveness(5.3.1.7).

Now it is also local on the source because it is stable under base change and composition and $R \to R_{f_i}$ does by locality on the source.

2 → 1:Now the property are all local on source. It suffices to prove a standard smooth map is smooth. This follows from(5.4.5.10).

1 → 2:We need to prove, assuming the first definition, it is locally standard smooth. For this, Cf.[Sta]00TA**?**. □

Cor. (5.4.5.13). Smoothness is stable under composition and base change. Smoothness is local on the source and target(In particular, $R \to R_f$ is smooth). (Already proved in the proof of(5.4.5.12)). ⌟

Prop. (5.4.5.14). A smooth map is a local complete intersection(5.4.4.15), hence flat. ⌟

Proof: Clear from(5.4.5.12). □

Prop. (5.4.5.15)[Noetherian Descent]. A smooth ring map $R \to S$ is a base change of smooth ring map over a ring f.g. over $\mathbb{Z}$. ⌟

Proof: Use the equivalence definition(5.4.5.2), we know that there is a map
$$S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c) \to R[X_1, \ldots, X_n]/(f_1, \ldots, f_c)^2,$$
which if we write $\sigma(X_i) = h_i$, then must satisfy
$$f_i(h_1, \ldots, h_n) = \sum a_{ijk} f_j f_k.$$
Then we consider the subalgebra generated by f_i, h_i, a_{ijk}, then by the same reason, they form a smooth algebra over $\mathbb{Z}$, and its tensor with R gives out S. □

Cor. (5.4.5.16) [Strong Lifting Property]. For a smooth ring map, the lifting property is true for $A \to A/I$, where I is locally nilpotent. ⌟

Proof: By(5.4.5.15), $R \to S$ is a base change of a smooth ring map $R_0 \to S_0$ where R_0 is f.g. over $\mathbb{Z}$. Now if S_0 is generated by $x_1, \ldots x_n$ and $a_1, a_n \in A$ maps to the image of $x_1, \ldots, x_n$ in A/I, then consider the subring A_0 generated by R_0 and a_i, and let $I_0 = A_0 \cap I$, then it suffices to prove this case followed by base change. But now A_0 is f.g. over $\mathbb{Z}$, so it is Noetherian, and then I is nilpotent, thus we have a desired lifting. □

Prop. (5.4.5.17) [Stalkwise]. If $R \to S$ is f.p., then it is smooth iff it is S_q/R_p is smooth for every (maximal)prime q of S and p under it. ⌟

Proof: Because of f.p., we only need to check triviality of $H_1(NL)$ and finite projectivity of $\Omega_{S/R}$(5.4.5.12). But both triviality and finite projectivity is stalkwise(5.1.4.2). (Notice $R \to R_p$ is smooth). □

Cor. (5.4.5.18) [Smooth Locus and Flat Base Change]. If $R \to S$ is of f.p. and $R \to R'$ is flat. Then the smooth locus of $S' = S \otimes_R R'/R'$ is the inverse image of smooth locus of S/R. ⌟

Proof: One direction is because smooth is stable under base change. Conversely, the local ring map is f.f., so $H_1(NL_{S'/R',q}) = H_1((NL_{S/R} \otimes_S S')_q) = H_1(NL_{S/R,p} \otimes_{S_p} S'_q)$. Then the result follows as S'_q/S_p is f.f. and triviality and finite projective descents for f.f. map(5.4.2.1). □

Lemma (5.4.5.19). A global complete intersection $S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c)$ is smooth at a point $\mathfrak{p}$ iff the Jacobian has rank $\geq n - \dim_{\mathfrak{q}}(S)$ at $\mathfrak{q}$, i.e. $J(\frac{f_1,\ldots,f_c}{X_1,\ldots,X_c})$ is not in $\mathfrak{q}$ for some permutation of $X_1, \ldots, X_n$. ⌟

Proof: This is a special case of(5.4.5.24). However, we need to prove it first here. If it is smooth at $\mathfrak{q}$, then $\Omega_{S/R}$ is locally free of dimension $\geq n - \dim_{\mathfrak{q}}(S)$ at $\mathfrak{q}$ by(5.4.5.10), so the Jacobian has rank $\geq n - \dim_{\mathfrak{q}}(S)$. Conversely, if $g = J(\frac{f_1,\ldots,f_c}{X_1,\ldots,X_c}) \notin \mathfrak{q}$, then $S_g = R[X_1, \ldots, X_n, X_{n+1}]/(f_1, \ldots, f_c, gX_{n+1} - 1)$ is a standard smooth map. □

Prop. (5.4.5.20) [Fiberwise]. For a ring map $R \to S$ and $\mathfrak{q}$ is a prime of S over $\mathfrak{p}$. Then S/R is smooth at $\mathfrak{q}$ iff S/R is of f.p. around $\mathfrak{q}$ and $S_{\mathfrak{q}}/R_{\mathfrak{p}}$ is flat and $S \otimes_R k(\mathfrak{p})/k(\mathfrak{p})$ is smooth at $\mathfrak{q}$. ⌟

Proof: One direction is because smooth is flat, f.p. and stable under base change. Conversely, by(5.4.5.14) and(5.4.4.18), change R to R_g for some $g \notin \mathfrak{p}$, we may assume $S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c)$ is a global complete intersection. Then we may use(5.4.5.19) to see the map is smooth on the standard open subset defined by the product of Jacobians of f_i. □

Prop. (5.4.5.21). If $A \to A[X_1, \ldots, X_n] \to R$ is smooth, then $A[X_1, \ldots, X_n] \to R$ is smooth. ⌟

Proof: The desired map is firstly of f.p. by(5.3.7.11), and it can be verified to be formally smooth, because $A[X_1, \ldots, X_n]$ is free. □

Smooth over Fields

Lemma (5.4.5.22). Let S be f.g. over a alg.closed field k and $\mathfrak{m}$ a maximal ideal, then the following are equivalent:

- $S_{\mathfrak{m}}$ is regular.
- $\dim_k \Omega_{S/k} \otimes_S k \leq \dim S_{\mathfrak{m}}$
- $\dim_k \Omega_{S/k} \otimes_S k = \dim S_{\mathfrak{m}}$
- S/k is smooth at $\mathfrak{m}$.

⌟

Proof: Cf.[Sta]00TS. □

Prop. (5.4.5.23) [Differential Criterion of Smoothness]. For a ring S f.g. over a field k, S is smooth in a nbhd of $\mathfrak{q}$ iff $\dim_{k(\mathfrak{q})}\Omega_{S/k}\otimes k(\mathfrak{q})\leq \dim_{\mathfrak{q}}(S)$.

And in this case, equality hold, and $S_{\mathfrak{q}}$ is regular. ⌟

Proof: Cf.[Sta]00TT.

If S is smooth at x, then $\Omega_{S/R}$ is finite free on a nbhd of x of rank equals to the dimension(5.4.5.10), so the equation holds.

Conversely, if $\dim_{k(x)}\Omega_{S/k}\otimes k(x)\leq \dim_x(X)$, then □

Cor. (5.4.5.24)[Jacobian Criterion of Smoothness]. For a f.p. ring $S=R[X_1,\ldots,X_n]/(f_1,\ldots,f_c)$ and $\mathfrak{q}\subset S$, S is smooth at $\mathfrak{q}$ iff the Jacobian has rank$\geq n-\dim_{\mathfrak{q}}(S)$ at $\mathfrak{q}$ iff the Jacobian has rank$= n-\dim_{\mathfrak{q}}(S)$ at $\mathfrak{q}$. ⌟

Lemma (5.4.5.25). Let k be a field and $(R,\mathfrak{m},\kappa)$ be a Noetherian local ring containing k. If the residue field of R is a f.g. field extension of k, then the derivation map

$$\mathfrak{m}/\mathfrak{m}^2\to\Omega_{R/k}\otimes_R\kappa$$

is injective. ⌟

Proof: Cf.[Sta]00TU. □

Prop. (5.4.5.26) [Smooth and Regular at Geometric Points]. Let S be f.g. over a field k, if $k(\mathfrak{q})/k$ is separable(e.g. char 0) for $\mathfrak{q}$ a prime of S, then S is smooth at $\mathfrak{q}$ iff it is regular at $\mathfrak{q}$. ⌟

Proof: Let $R=S_{\mathfrak{q}}$ with maximal ideal $\mathfrak{m}$. By(5.4.5.25) and(5.4.3.8) there is an exact sequence

$$0\to\mathfrak{m}/\mathfrak{m}^2\to\Omega_{R/k}\otimes_R k(\mathfrak{q})\to\Omega_{k(\mathfrak{q})/k}\to 0.$$

Since $k(\mathfrak{q})/k$ is separable, $\dim_{k(\mathfrak{q})}\Omega_{k(\mathfrak{q})/k}=\operatorname{tr.deg}(k(\mathfrak{q})/k)$. So

$$\dim_{k(\mathfrak{q})}(\Omega_{R/k}\otimes_R k(\mathfrak{q}))=\dim_{k(\mathfrak{q})}\mathfrak{m}/\mathfrak{m}^2+\operatorname{tr.deg}(k(\mathfrak{q})/k)\geq\dim R+\operatorname{tr.deg}(k(\mathfrak{q})/k)=\dim_{\mathfrak{q}}(S)$$

with identity iff R is regular(The last identity comes from(6.6.3.7)). So we are done by differential criterion of smoothness(5.4.5.23). □

Prop. (5.4.5.27) [Smooth over Fields and Geo.Regular]. Let S be f.g. over a field k, then S is smooth over k iff S is geo.regular(5.3.6.1). ⌟

Proof: If S is smooth at x, then all its base change is smooth at x(5.4.5.13), and the stalk is regular by(5.4.5.23), so it is geometrically regular at x.

Conversely, if X is geometrically regular, then for any point $x\in X$, $k(x)$ is f.g. over k, so by(5.3.9.3) there is a finite purely inseparable extension k'/k that the compositum $k'k(x)$ is separable over k'. Then by(5.1.7.26), $\operatorname{Spec} A\otimes_k k'$ is homeomorphic to $\operatorname{Spec} A$, so there is a unique prime p' of $X_{k'}$ over X, and its residue field is $k'k(x)$. So by(5.4.5.26), as $k'k(x)/k'$ is separable, $X_{k'}$ is smooth over k' at p'. And f.f. descent for smoothness(5.4.2.1) says X is also smooth over k at p. □

Cor. (5.4.5.28) [Differential and Smoothness]. Let k be a field of characteristic 0 and S a f.g. algebra over k, and $\mathfrak{q}$ a prime ideal of S, if $\Omega_{S/k,\mathfrak{q}}$ is free over $S_{\mathfrak{q}}$, then S is smooth in a nbhd of $\mathfrak{q}$. ⌟

Proof: Cf.[Sta]00TX. □

Prop. (5.4.5.29) [Generic Smoothness]. Let $R \to S$ be an injective ring map of f.t. with R, S domains, then it is smooth at (0) iff the quotient field map is separable. ⌟

Proof: If S is smooth at 0, then replacing S by S_g for some g, we can assume $R \to S$ is smooth. Then $K \to S \otimes_R K$ is also smooth(5.4.5.13), and also for any field extension K' of K. Then $S \otimes_R K'$ is regular, by(5.4.5.23), a priori reduced(6.4.1.5). Thus $S \otimes_R K$ is geometrically reduced. Hence also L is geometrically reduced over K, thus separable, by(5.3.9.4).

Conversely, by(5.4.1.34), we may assume $R \to S$ is of f.p., thus to show it is smooth at (0), it suffices to show $S \otimes_R K$ is smooth at (0), by(5.4.5.20). Then this follows from(5.4.5.26). □

Smoothing Ring Maps

Prop. (5.4.5.30). A regular homomorphism of Noetherian rings is a filtered colimit of smooth ring maps. ⌟

Proof: Cf.[Sta]07GC. □

6 Unramified

Formally Unramified

Def. (5.4.6.1). A ring map $R \to S$ is called **formally unramified** if for every R-ring A and an ideal I of A that $I^2 = 0$, a map $S \to A/I$ has at most one extension to a map $S \to A$.

Formally unramified is equivalent to $\Omega_{S/R} = 0$. So it is stable under composition by Jacobi-Zariski sequence(5.4.3.7). ⌟

Proof: Let $J = \ker(S \otimes_R S \to S)$, let $A_{univ} = S \otimes_R S/J^2$, then $J/J^2 \cong \Omega_{S/R}$(5.4.3.4), so we have two natural map from S to A_{univ}, they differ by the universal differential $S \to \Omega_{S/R}$. If S/R is unramified, then $ds = 0$ for all $s \in S$, so $\Omega_{S/R} = 0$.

Conversely, if there is a A and A/J that there are two liftings τ_1, τ_2, then we let $A_{univ} \to A$ defined by $s_1 \otimes s_2 \to \tau_1(s_1)\tau_2(s_2)$, this is well-defined, and because $A_{univ} \cong S$, this map descends to S, so $\tau_1(s_1 s_2) = \tau_2(s_1 s_2)$. □

Prop. (5.4.6.2) [Formally Unramified Stalkwise]. Formally unramified is stalkwise both on the source and target(5.1.4.2). ⌟

Prop. (5.4.6.3). Colimits of formally unramified rings over R is formally unramified. (Trivial as one renders on the diagram in the definition of formally unramified). ⌟

Unramified Map

Def. (5.4.6.4)[Unramified Maps]. A ring map is called **unramified** iff it is formally unramified and f.g..

A ring map is called G-**unramified** iff it is formally unramified and of f.p.. In particular, an étale map is G-unramified.

These two notions are stable under composition and base change. These two notions are local on the source and target. $R \to R_f$ is G-unramified.(5.4.6.1)(5.1.4.2) ⌟

Prop. (5.4.6.5). $R \to R/I$ is unramified, and if I is f.g., then it is G-unramified. (Trivial). ⌟

Prop. (5.4.6.6) [Stalkwise and Fiberwise]. If $R \to S$ is of f.t(f.p.), then it is unramified(G-unramified) at a prime q of S iff $(\Omega_{S/R})_q = 0$ iff $\Omega_{S/R} \otimes_S k(q) = 0$ iff $(\Omega_{S\otimes k(p)/k(p)})_q = 0$ iff $\Omega_{S\otimes k(p)/k(p)} \otimes k(q) = 0$. ⌟

Proof: By Nakayama, two pair of them are equivalent, and if $\Omega_{S/R,q} = 0$, then $\Omega_{S/R,g} = 0$ for some $g \notin q$(because support of finite module is open), so $R \to S_g$ is (G-)unramified. And notice in fact $\Omega_{S/R} \otimes_S k(q) = \Omega_{S\otimes k(p)/k(p)} \otimes_{k(p)} k(q)$. □

Prop. (5.4.6.7) [Equivalent Definition of Unramifiedness]. A f.g. ring map $R \to S$ is unramified at a prime q of S over p iff $pS_q = qS_q$ and $k(q)/k(p)$ is finite separable. ⌟

Proof: Suppose $R \to S_g$ is unramified, then $S \otimes k(p)$ is unramified over $k(p)$, hence by(5.4.5.23), it is also smooth, so it is étale, and(5.4.7.9) gives the result.

For the converse, Cf[Sta]02FM]. □

Prop. (5.4.6.8). A ring map is unramified iff it is locally a quotient of a standard étale map. ⌟

Proof: Cf.[Sta]0395]. □

Prop. (5.4.6.9). Any G-unramified map is a base change of a G-unramified map over a ring R_0 f.g. over $\mathbb{Z}$. And similarly any unramified map is a quotient of a base change of a G-unramified map over a ring R_0 f.g. over $\mathbb{Z}$. ⌟

Proof: Let $S = R[X_1, \ldots, X_n]/(g_1, \ldots, g_c)$, then we have $dX_i = \sum a_{ij} dg_j + a_{ijk} g_j dX_k$, so we let R_0 be generated by g_i, a_{ij}, a_{ijk}, so $S_0 = R_0[X_1, \ldots, X_n]/(g_1, \ldots, g_c)$ is G-unramified. □

Prop. (5.4.6.10) [Unramifiedness and Idempotent]. If $R \to S$ is of f.t., then it is unramified iff $S \times_R S \to S$ is isomorphic to $S \otimes_R S \to (S \otimes_R S)_e$ for some diagonal idempotent $e \in S \otimes_R S$ that $e\ker(\mu) = 0$, i.e. $S \otimes_R S \cong S \times S'$. ⌟

Proof: If it is G-unramified, the kernel I satisfies $I/I^2 = 0$, and I is f.g.(by $x_i \otimes 1 - 1 \otimes x_i$) so we can use(5.1.7.7).

Conversely, the existence of the diagonal idempotent e implies that $I = I^2$. □

7 Étale

Formally Étale

Def. (5.4.7.1). A ring map $R \to S$ is called **formally étale** iff it is formally smooth and formally unramified. ⌟

Prop. (5.4.7.2). Colimits of formally étale rings over R is formally étale. (The lifting are compatible because of uniqueness). ⌟

Prop. (5.4.7.3). $R \to S^{-1}R$ is formally étale. ⌟

Proof: It suffice to prove that if $\varphi(s)$ is invertible modulo I, then $\varphi(s)$ is invertible, but this is true because I is nilpotent. □

Étale Map

Def. (5.4.7.4). A ring map $R \to S$ is called **étale** if it is of f.p. and the naive cotangent complex is exact, i.e. $I/I^2 \cong \Omega_{P/R} \otimes_P S$.

In particular, étale is equivalent to smooth+formally unramified($\Omega_{R/S} = 0$). ⌟

Cor. (5.4.7.5) [Properties of Étale].

1. Étale map is stable under base change and composition.
2. Étale map is local on the source and target. In particular, $R \to R_f$ is étale.
3. If $R \to S$ is of f.p. and $R \to R'$ is flat. Then the set of primes in $S' = S \otimes_R R'$ that has a nbhd that is étale over R' is the inverse image of set of primes in S that has a nbhd that is étale over R. (The same as(5.4.5.18)).
4. Étale map is syntomic, hence flat.
5. Any Étale map is a base change of an étale map over a ring R_0 f.g. over $\mathbb{Z}$. (Cf.[Sta]00U2).

⌟

Cor. (5.4.7.6) [Étale Localness of Differential]. For ring morphisms $A \to R \to S$, if $R \to S$ is étale, then $\Omega_{S/A} = \Omega_{R/A} \otimes_R S$. ⌟

Proof: This follows from(5.4.7.4) and(5.4.5.5). □

Prop. (5.4.7.7) [Jacobson Criterion]. Any étale map is equivalent to a standard smooth ring map $S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$ that $J(\frac{f_1,\ldots,f_n}{X_1,\ldots,X_n})$ is invertible in S. ⌟

Proof: $I/I^2 \cong \Omega_{P/R} \otimes_P S$, so I/I^2 is free, so by(5.3.7.12), there is a presentation of S that $f_1, \ldots, f_c$ freely generate I/I^2, then obviously $c = n$ and $J(\frac{f_1,\ldots,f_c}{X_1,\ldots,X_n})$ is invertible in S, i.e. S is standard smooth. □

Cor. (5.4.7.8) [Example of Étale Maps]. The ring

$$S = R[X_1, \ldots, X_n, X_{n+1}]/(f_1, \ldots, f_n, X_{n+1} \det(\frac{f_1, \ldots, f_n}{X_1, \ldots, X_n}) - 1)$$

is étale over R. ⌟

Prop. (5.4.7.9). If $R \to S$ is étale at a nbhd of a prime q of S over p, then $pS_q = qS_q$, and $k(q)/k(p)$ is finite separable. ⌟

Proof: We can replace S by S_g so S_g/R is étale. Then $S \otimes k(p)/k(p)$ is étale, that is S_p/pS_p is a finite product of finite separable fields, so $S_q/pS_q = (S_p/pS_p)_q =$ some separable closed field. □

Lemma (5.4.7.10). If $R \to S$ is an étale map and q is a prime of S over p, then S/R is étale in a nbhd of q if

- $R \to S$ is of f.p.
- $R_p \to S_q$ is flat.
- $pS_q = qS_q$.
- $k(q)/k(p)$ is a finite separable field extension.

⌟

Proof: Cf.[Sta]00U6. □

Prop. (5.4.7.11) [Equivalent Definition of Étale]. A ring map $R \to S$ is **étale** iff it is flat, of f.p. and $\Omega_{S/R}$ vanishes. ⌟

Proof: One direction is by definition, and the converse is by(5.4.7.10) and(5.4.6.7). □

Prop. (5.4.7.12). A ring map of f.p. is formally étale iff it is étale. (Because in this case, formally smooth is equivalent to smooth(5.4.5.12).) ⌟

Prop. (5.4.7.13). If S/R and S'/R are étale, then any R-algebra map $S \to S'$ is étale. ⌟

Proof: $S \to S'$ is of f.p. by(5.3.7.11), the rest Cf.[Sta]00U7. □

Prop. (5.4.7.14) [Étale Algebra seen explicitly as Finite Projective Modules]. Étale algebras are finite projective, by(5.3.1.7). And we can see this clearly as follows: There is an diagonal idempotent as it is unramified(5.4.6.10), If $e = \sum a_i \otimes b_i$, then we can realize S as a direct command of R^n through maps

$$S \xrightarrow{\alpha} R^n \xrightarrow{\beta} S$$

where $\alpha(f) = (\mathrm{tr}_{S/R}(fa_i))$, and $\beta((g_i)) = \sum g_i b_i$. ⌟

Proof: We check that $\beta \circ \alpha = \mathrm{id}$: Notice first that $\mathrm{tr}_{i_2}(e) = \mathrm{tr}_{S/S}(1) = 1$, following from the decomposition above, so $\sum \mathrm{tr}_{S/R}(a_i)b_i = 1$, thus shows that $\beta\alpha(1) = 1$.

Now for general f, using the formula $(f \otimes 1)e = (1 \otimes f)e$, we get $\sum \mathrm{tr}(fa_i)b_i = \sum \mathrm{tr}(a_i)b_i f = f$. □

Prop. (5.4.7.15). If R is a ring and I is an ideal, then any étale ring map $R/I \to \overline{S}$ comes from an étale ring map $R \to S$. ⌟

Proof: Use(5.4.7.7), an étale map is of the form $\overline{S} = R/I[X_1, \ldots, X_n]/(\overline{f}_1, \ldots, \overline{f}_n)$ that $\delta = J(\frac{f_1,\ldots,f_n}{X_1,\ldots,X_n})$ is invertible in S, then we take $S = R[X_1, \ldots, X_n, X_{n+1}]/(f_1, \ldots, f_n, X_{n+1}\delta - 1)$, then it is étale by(5.4.7.8) and maps to $\overline{S}$. □

Standard Étale

Def. (5.4.7.16). A ring map $R \to R' = R[X]_g/(f)$ is called **standard étale** iff f is monic and the derivative f' is invertible in R'.

Standard étale is stable under base change and principal localization, but not stable under composition. ⌟

Prop. (5.4.7.17) [Étale and Standard Étale]. A ring map is étale iff it is locally standard étale. ⌟

Proof: For a standard étale algebra $R[X]_g/(f) = R[X,Y]/(f, gY - 1)$ which is standard smooth and $\Omega_{R'/R} = 0$(5.4.3.10), so it is étale. To prove if it is locally standard étale then it is étale, Cf.[Sta]00UE. □

Prop. (5.4.7.18). Giving any ring R and a prime p, if there is a finite separable extension $L/k(p)$, then there is a standard étale map $R \to R'$ that for some q', $k(q') \cong L$ over k. ⌟

Proof: $L = k(p)[\alpha]$ by primitive element theorem, so the minimal polynomial of α is separable, and if we change α to $c\alpha$ for some $c \in k(p)$, we can assume f can be lifted to a $f \in R[X]$. Now $f'(\alpha)$ is invertible in L, so there is a map from $R[X]_{f'}/(f)$ to L, whose kernel gives the desired prime q. □

Étale over Fields

Prop. (5.4.7.19) [Étale over Fields]. An algebra over a field k is étale iff it is a finite product of finite separable extensions of k. ⌟

Proof: If k'/k is finite separable, then $k' = k(\alpha)$ for some α by primitive element theorem, thus $k' = k[X]/(f)$ that f' is invertible in k', thus it is étale by(5.4.7.7).

Conversely, Cf.[Sta]00U3. □

Cor. (5.4.7.20) [Étale over Perfect Fields]. Let k be a perfect field. If R is a k-algebra that is a finite as a k-module, then it is étale over k iff it is reduced. ⌟

Proof: If it is étale , then it is reduced, by(5.4.7.19). Conversely, if it is finite and reduced, then it is a reduced Artinian ring(5.1.3.4), so a product of fields over k, so étale as k is perfect. □

Prop. (5.4.7.21) [Étale and Trace Form]. Let A be a f.d. k-algebra, then A is étaleover k iff the trace form: $A \times A \to k : (a, b) \mapsto \mathrm{tr}_{A/k}(ab)$ is non-degenerate. ⌟

Proof: If it is étale, then the trace form is non-degenerate by(5.4.7.19) and(3.2.6.32). Conversely, if the trace form is non-degenerate, then A is reduced, because if $a \in A$ is nilpotent, then ab are nilpotent for any $b \in A$, and $\mathrm{tr}_{A/k}(ab) = 0$. Then as a reduced Artinian ring, A is isomorphic to a product of fields, then by(3.2.6.32), all the fields are separable over k. □

Prop. (5.4.7.22) [Étale and Unramified over Fields]. For $k \in \mathtt{Field}$, a f.g. k-algebra is étale iff it is (G-)unramified over k, by(5.4.5.23). ⌟

Prop. (5.4.7.23) [Maximal Étale Subalgebra]. Let A be an algebra of f.t. over a field k, then there is a maximal étale k-subalgebra of A. Also this subalgebra commutes with arbitrary field base change. ⌟

Proof: If R is an étale subalgebra of A, then $R_{\overline{k}}$ is étale over $\overline{k}$, thus isomorphic to $(\overline{k})^n$ for some n. Now n is smaller than the number of connected components of Spec $A_{\overline{k}}$, which is finite. So it suffices to show the composite of two étale subalgebras of A is étale. For this, notice RR' is a quotient of $R \otimes_k R'$, which is a finite product of finite separable fields over k, thus its quotient is also a finite product of finite separable fields over k, which is étale.

□

8 Local Algebras

Main references are [Local Algebra, Serre].

Prop. (5.4.8.1). If A is a Noetherian local integral domain with residue field k and quotient field K, if M is a f.g. A-module that $\dim_k M \otimes_A k = \dim_K M \otimes_A K = r$, then M is free of rank r.

In other words, if the rank of M at the generic point and closed pt of B are the same, then M is free. ⌟

Proof: First M is generated by r elements by Nakayama and the kernel R of $A^r \to M$ vanishes when tensoring K, thus vanish because it is torsion-free. □

Prop. (5.4.8.2). Let $A \to B$ be a local ring map of local rings that

- B is finite as an A-module.

- $\mathfrak{m}_B$ is a f.g. ideal.
- $A/\mathfrak{m}_A \cong B/\mathfrak{m}_B$.
- $\mathfrak{m}_A/\mathfrak{m}_A^2 \cong \mathfrak{m}_B/\mathfrak{m}_B^2$.

Then $A \to B$ is surjective. ⌟

Proof: By Nakayama, to show it is surjective, it suffices to show $A/\mathfrak{m}_A \to B/\mathfrak{m}_A B$ is surjective, then it suffices to show $\mathfrak{m}_A \otimes_A B \to \mathfrak{m}_B$ is surjective. For this, use Nakayama again on B to reduce to the fact $\mathfrak{m}_A \otimes_A B/\mathfrak{m}_B \to \mathfrak{m}_B \otimes B/\mathfrak{m}_B$ is surjective, which is satisfied because this is just $\mathfrak{m}_A/\mathfrak{m}_A^2 \to \mathfrak{m}_B/\mathfrak{m}_B^2$. □

5.5 p-adic Commutative Algebras

1 $\mathbb{F}_p$-Algebras

Def. (5.5.1.1) [relative Frobenius]. Let $S \to R$ be a ring map, then the **relative Frobenius** $\varphi_{R/S}$ is the map $R \otimes_{S,\mathrm{Frob}} S \to R$ induced by universal property. ⌟

Def. (5.5.1.2) [Perfect Rings]. A ring of characteristic p is called **perfect** iff the Frobenius $\mathrm{Frob}/\varphi : P \to P$ is an isomorphism. It is called **semi-perfect** iff Frob is surjective. ⌟

Prop. (5.5.1.3) [Perfection and Coperfection]. If R is of char p, we define $R_{\mathrm{perf}} = \varinjlim_\varphi R$ and $R^{\mathrm{perf}} = \varprojlim_\varphi R$.

The $(\cdot)_{\mathrm{perf}}$ and $(\cdot)^{\mathrm{perf}}$ are respectively the left and right adjoint to the forgetful functor from the category of perfect rings to the category of rings of characteristic p.

In particular, the category of perfect rings admits limits and colimits, and it equals the limits and colimits in the category of rings. ⌟

Proof: First both R_{perf} and R^{perf} are perfect: for R_{perf}, every element in R_{perf} is represented by an element $a_n \in R_n$, and this element is equivalent to $a_n^p \in R_{n+1}$, so its p-th root is $a_n \in R_{n+1}$. For R^{perf}, an element $(\dots, x_n, \dots, x_0)$ has p-th root $(\dots, x_{n+1}, \dots, x_1)$.

Second it is easily checked to be a functor because Frob is natural. The universal property is easy. □

Prop. (5.5.1.4) [Perfection Kills Nilextensions]. If $f : R \to S$ is a map of rings of characteristic p that is surjective with nilpotent kernel, then $R_{\mathrm{perf}} \to S_{\mathrm{perf}}$ and $R^{\mathrm{perf}} \to S^{\mathrm{perf}}$ are both isomorphisms. ⌟

Proof: $-_{\mathrm{perf}}$ map is clearly surjective, and it is injective because if a maps to 0, then $\mathrm{Frob}^k(a) \in \ker f$ for some k, so it is nilpotent, so $\mathrm{Frob}^{k+n}(a) = 0$.

$-^{\mathrm{perf}}$ is clearly injective, and it is surjective because: suppose $\ker f^n = 0$, then for a $(s_n) \in S$, let t_m be the inverse image of s_{mn}, for each m, and let $x = (x_n), x_{mn-k} = \mathrm{Frob}^k t_m$, then $(x) \in R^{\mathrm{perf}}$ and x maps to s. □

Def. (5.5.1.5) [Perfectly Finitely Presented]. A map of perfect $\mathbb{F}_p$-algebras $B \to A$ are called **perfectly finitely presented** if $A = (A_0)_{\mathrm{perf}}$ for some f.p. B-algebra A_0. ⌟

Prop. (5.5.1.6) [Aberbach-Hochster]. Let R be a perfect $\mathbb{F}_p$-algebra, $f_1, \dots, f_r \in R$, and consider the ideal $I = \sqrt{(f_1, \dots, f_r)} \in R$. Then R/I has flat dimension$\leq r$ as an R-module. ⌟

Proof: We only prove for $r = 1$.

We show $I = \varinjlim_{f^{1/p^n - 1/p^{n+1}}} R$. The map is given by $(a_n) \mapsto f^{1/p^n} a_n$. This is injective because if $f^{1/p^n} a = 0$, then $f^{1/p^{n+1}} a = 0$ by perfectness, thus a is killed by the transition map $f^{1/p^n - 1/p^{n+1}}$. □

Prop. (5.5.1.7) [Perfect Algebras are Tor Independent]. For any two perfect A-algebras B, C where A is a perfect $\mathbb{F}_p$-algebra, $\mathrm{Tor}_i^A(B, C) = 0$ for $i > 0$. ⌟

Proof: $A \to B$ can be written as a composition of a perfection of a free A-algebra and a quotient. The perfection of free algebra is flat, thus we can assume $B = A/I$. By a filtered colimit argument again, we can assume $I = (f_1^{\frac{1}{p^\infty}}, \dots, f_r^{\frac{1}{p^\infty}})$ is perfectly f.p. By induction, we can assume $r = 1$. Now the lemma(5.5.1.6) applied to $R = C$ shows that $IC = \varinjlim_{f^{1/p^n - 1/p^{n+1}}} C = I \otimes_A^L C$, so $B \otimes_A^L C = C/IC$ is discrete. □

Prop. (5.5.1.8). If R is a perfect $\mathbb{F}_p$-algebra, I is a radical ideal, and $J = R[I] \subset R$, then J and $I + J$ are both radical, and the square

$$\begin{array}{ccc} R & \longrightarrow & R/I \\ \downarrow & & \downarrow \\ R/J & \longrightarrow & R/I+J \end{array}$$

is both a fiber pullback and pushout square of commutative rings. ⌟

Proof: J is clearly a radical, and notice that $I + J$ is the kernel of the map $R \to R/I \otimes_R R/J = R/I + J$(5.1.1.23), and the target is a colimit of perfect rings thus perfect, by(5.5.1.3). Thus $I + J$ is also perfect, thus a radical ideal.

By(5.1.1.24), to show the map is a pullback square, it suffices to show that $I \cap J = 0$. If $x \in I \cap J$, then $x^2 = 0$, thus $x^p = 0$, so $x = 0$. □

Tilting

Def. (5.5.1.9)[Tilting]. For any $R \in \mathcal{CR}\text{ing}$, the ($p$-adic)**tilting** of R is defined to be $R^\flat = (R/(p))^{\text{perf}}$, endowed with the profinite topology. ⌟

Prop. (5.5.1.10). If R is a f.g. algebra over an alg.closed field k of char$p$, then $R^\flat \cong k^{\pi_0(\operatorname{Spec} R)}$. ⌟

Proof: It suffice to prove for $\operatorname{Spec} R$ connected and reduced, because by(5.5.1.4). We first prove the case $\operatorname{Spec} R$ is irreducible, i.e. R is integral:

In this case, choose a closed point x, then there is a map $R \to \widehat{R_x}$, where $\widehat{R_x}$ is the $\mathfrak{m}_x$-adic completion. By Krull(5.2.2.15) and the fact R is integral, this map is injective, so it suffices to show that $0 = (\widehat{R_x})^{\text{perf}} = \varinjlim(R_x/\mathfrak{m}_x^n)^{\text{perf}}$. But $(-)^{\text{perf}}$ is a right adjoint so commutes with colimits and $\widehat{R_x} = \varinjlim R_x/\mathfrak{m}_x^n$. But $(R_x/\mathfrak{m}_x^n)^{\text{perf}} = (R_x/\mathfrak{m}_x)^{\text{perf}} = k^{\text{perf}} = k$, by(5.5.1.4) again.

If R is not irreducible, **?** □

Prop. (5.5.1.11)[Examples of Tilting].

- $\mathbb{F}_p[t]_{\text{perf}} = \mathbb{F}_p[t^{\frac{1}{p^\infty}}]$, $\mathbb{F}_p[t]^\flat = \mathbb{F}_p[t]^{\text{perf}} = \mathbb{F}_p$.
- $(\mathbb{Z}_p)^\flat = \mathbb{F}_p$.
- If R is a perfect ring of char$p$ and $f \in R$ is a non-zerodivisor, then $(R/f)^{\text{perf}}$ is the f-adic completion of R. In particular, $(\mathbb{F}_p[t^{\frac{1}{p^\infty}}]/(t))^{\text{perf}} \cong \widehat{\mathbb{F}_p[t^{\frac{1}{p^\infty}}]}$.
- $(\widehat{\mathbb{Z}_p[p^{\frac{1}{p^\infty}}]})^{\text{perf}} \cong \widehat{\mathbb{F}_p[t^{\frac{1}{p^\infty}}]} \cong \widehat{\mathbb{F}_p[t]_{\text{perf}}} \cong (\mathbb{F}_p[t]_{\text{perf}}/(t))^{\text{perf}}$.

⌟

Proof: The first two are trivial, for the third, notice $\widehat{R_f} = \varprojlim_n R/f^n = \varprojlim_n R/f^{p^n}$, and there are commutative diagram $\begin{array}{ccc} R/f & \xrightarrow{\varphi} & R/f \\ \downarrow{\scriptstyle \varphi^{k+1}} & & \downarrow{\scriptstyle \varphi^k} \\ R/f^{p^{k+1}} & \xrightarrow{i} & R/f^{p^k} \end{array}$, so $\varprojlim_n R/f^{p^n} \cong (R/f)^{\text{perf}}$.

For the fourth, only the first equivalence needs proving, the others are consequences of the first three items. Then notice

$$(\widehat{\mathbb{Z}_p[p^{\frac{1}{p^\infty}}]})^\flat \cong \varprojlim(\widehat{\mathbb{Z}_p[p^{\frac{1}{p^\infty}}]}/p^k)^{\text{perf}} \cong (\widehat{\mathbb{Z}_p[p^{\frac{1}{p^\infty}}]}/p)^{\text{perf}} \cong (\mathbb{F}_p[t^{\frac{1}{p^\infty}}]/t)^{\text{perf}} \cong \widehat{\mathbb{F}_p[t^{\frac{1}{p^\infty}}]}$$

The last isomorphism by item3. □

Prop. (5.5.1.12). If $R \in \mathcal{CR}\mathrm{ing}$ is a p-adically complete, $\pi \in R^\times, p \in (\pi)$, then the map $R \to R/p$ induces an homeomorphism of monoids:

$$\varprojlim_{x\to x^p} R \cong \lim_{\varphi} R/\pi \overset{(5.5.1.4)}{=} \lim_{\varphi} R/p = R^\flat$$

⌟

Proof: Injectivity: if $(a_n),(b_n) \in \lim_{x\to x^p} R$ satisfies $a_n \equiv b_n \mod \pi$ for all n, then applying power lifting(2.6.3.9), $a_n \cong b_n \mod \pi^{n+k}$ for all k, so $a_n = b_n$.

Surjectivity: for $(\overline{a_n}) \in R^\flat$, choose arbitrary lifting a_n, then $a_{n+k+1}^p \equiv a_{n+k} \mod \pi$ for all $n+k$, so $k \mapsto a_{n+k}^{p^k}$ is a Cauchy sequence by power lifting(2.6.3.9) again, thus converging to some point b_n. then it's easily checked that $b_{n+1}^p = (\lim a_{n+1+k}^{p^k})^p = \lim a_{n+1+k}^{p^{k+1}} = b_n$. so (b_n) maps to $(\overline{a_n})$.

For the topology: it is clearly continuous, and for the reverse, if $(a_i),(b_i)$ satisfies that $a_i \equiv b_i \mod \pi$ for $i<k$, then the image in $\varprojlim_{x\to x^p} R$ satisfies $x_i \equiv y_i \mod p^{k-i}$ for $i<k$, thus it is open. □

Cor. (5.5.1.13) [Sharp Map]. From this proposition, we get a multiplicative **sharp map**:

$$\sharp : R^\flat \to R : (\overline{a}_n) \mapsto \lim_{k\to\infty} a_k^{p^k},$$

and its image is just the elements that has a compatible system of p^k-th roots $x^{\frac{1}{p^k}}$. These elements are also called **perfect**. ⌟

Cor. (5.5.1.14) [Addition in $R^\flat$]. From the isomorphism(5.5.1.12) above, we can read what the addition looks like in the presentation $\varprojlim_{\varphi} R$: if $(f_n),(g_n)$ are two elements, then their addition is given by (h_n), where $h_n = \lim_k (f_{n+k}+g_{n+k})^{p^k}$. ⌟

Cor. (5.5.1.15) [Fontaine's Functor]. By(7.1.4.4), the natural map $R^\flat \to R/p$ induces a map $\theta_R : W(R^\flat) \to R$ of rings, called the **Fontaine's functor**, which writes as $\sum [a_i]p^i \mapsto \sum a_i^\sharp p^i$. And we denote $A_{\mathrm{inf}}(R) = W(R^\flat)$ the **infinitesimal Fontaine's ring** of R. ⌟

Prop. (5.5.1.16). If R is p-complete, the Fontaine's functor θ_R is surjective iff R/p is semiperfect. ⌟

Proof: As R is p-complete, θ is surjective iff it is surjective modulo p. Because its reduction modulo p is $R^\flat \to R/p$ is surjective as $\varphi : R/p \to R/p$ does. □

Prop. (5.5.1.17) [Tilting as a Valuation Ring]. If R is a domain or a valuation ring, then the same is true for $R^\flat$. In the valuation case, the valuation of $R^\flat$ can in fact be chosen to be $|\cdot| \circ \sharp$, so in particular, the rank of $R^\flat$ is no more than the rank of R. ⌟

Proof: Use the isomorphism $\varprojlim_{x\to x^p} R \cong \lim_\varphi R/p = R^\flat$(5.5.1.12).

For the domain case, if $(a_n)(b_n) = 0$, then $a_n b_n = 0$, so $a_0 = 0$ or $b_0 = 0$, so $(a_n) = 0$ or $(b_n) = 0$. Similarly, if R is a valuation ring, then $R^\flat$ is firstly a domain, and it suffices to prove that for any $(a_n),(b_n) \in R^\flat$, the quotient of one by another is in $R^\flat$, by(11.2.2.3). For this, because R is valuation ring, we may assume $a_0/b_0 \in R$, so a_n/b_n is also in R, because their power do, and R is normal(11.2.2.6), thus $(a_n)/(b_n) \in R^\flat$.

For the valuation given, notice in the above proof, $|(a_n)| \le |(b_n)|$ iff $|a_0| \le |b_0|$, so the valuation are equivalent to $|\cdot| \circ \sharp$ by(11.2.3.14), so it can be chosen to be so. □

Prop. (5.5.1.18) [Tilting and Completion]. If $R = A/I$ with A/p perfect, then $R^\flat$ identifies with the I-adic completion of A/p. ⌟

Proof: $R^\flat = \varprojlim_\varphi R/p = \varprojlim_\varphi A/(p, I)$. But there are commutative diagrams

$$\begin{array}{ccc} A/(p,I) & \xrightarrow{\varphi} & A/(p,I) \\ \downarrow \varphi^{n+1} & & \downarrow \varphi^n \\ A/(p, I^{p^{n+1}}) & \longrightarrow & A/(p, I^{p^n}) \end{array}$$

where the vertical arrows are isomorphisms because A/p is perfect. So the conclusion follows. □

2 p-Local Rings

Def. (5.5.2.1) [p-Local Rings]. A commutative ring is called p-local if $p \in \operatorname{rad} A$. ⌟

Prop. (5.5.2.2). Let A be a p-adically complete ring, then A is p-local, by(5.2.3.18). ⌟

Prop. (5.5.2.3). If A is p-adically complete and has bounded p-torsions, the p-completion of a smooth A-algebra is p-completely smooth. ⌟

Proof: This follows from(5.9.7.4) and(5.9.6.16). □

Def. (5.5.2.4) [p-Normal Rings]. A p-torsion-free ring R is called p-**normal** if R is p-root closed in $R[\frac{1}{p}]$. ⌟

Complete Discrete Valuation Rings

Structure of complete p-local DVRs will be studied in this subsubsection.

Main references are [Ser79], [Integral p-adic Hodge, BMS].

Def. (5.5.2.5) [Strict p-Ring]. A p-**ring** A is a ring which is complete Hausdorff in the topology defined by the decreasing chain of ideals $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots$ such that $\mathfrak{a}_m\mathfrak{a}_n \subset \mathfrak{a}_{m+n}$ that $k = A/\mathfrak{a}_1$ is a perfect ring of characteristic p.

It is called a **strict** p-**ring** if moreover $\mathfrak{a}_n = (p^n)$ and p is a non-zero divisor of A. ⌟

Prop. (5.5.2.6) [Teichmüller Lifts]. For a p-ring, there exists a unique section map $[\cdot] : k \to A$ that is multiplicative, called the **Teichmüller lifts**.

If $\operatorname{char} A = p$, then the Teichmüller lift is also additive(but not in general). And an element is in the image of f iff it is a p^n-th power for any n. ⌟

Proof: For any $\lambda \in k$, the $\lambda^{p^{-n}}$ is unique in k, and if we consider U_n the set of all x^{p^n} where x is a lift of $\lambda^{p^{-n}}$, then U_n is a descending set. Moreover, the diameter converges to 0, because $a \equiv b \mod \mathfrak{a}_1$ implies $a^{p^n} \equiv b^{p^n} \mod \mathfrak{a}_{n+1}$ as $p \in \mathfrak{a}_1$. So it converses to a unique point $f(\lambda)$ in A. And we see that any other f' maps λ to a p^n-th root hence in U_n for any n, hence it map be equal to $f(\lambda)$. The rest is easy. □

Cor. (5.5.2.7) [Equal Characteristic case]. If A is a complete discrete valuation ring with residue field k. If k and A have the same characteristic and k is perfect, then $A \cong k[[T]]$. ⌟

Def. (5.5.2.8) [$(0,p)$-type case]. When A is a complete DVR with residue field k and quotient field K. If char$K = 0$ and char$k = p$, then p goes to 0 in k, so $e = v(p) \geq 1$, called the **absolute ramification index** of A. It is called **absolutely unramified** iff $e = 1$. ⌟

Remark (5.5.2.9) [Universal Strict p-Ring]. The canonical strict p-ring is the ring $\widehat{S} = \widehat{\mathbb{Z}}[X_\alpha^{p^{-n}}]$. Its residue ring is $\mathbb{F}_p[X_\alpha^{p^{-n}}]$ which is perfect. X_i are all Teichmüller lifts, as they has all p^n roots.

Now we consider the $* = + - \times$ in $\widehat{S}$. then there are elements $Q_i^* \in \mathbb{F}_p[X_\alpha^{p^{-n}}, Y_\alpha^{p^{-n}}]$ that $x * y = \sum f(Q_i^*)p^i$ where f is the Teichmüller lift. ⌟

Prop. (5.5.2.10) [Universal Law of p-Rings]. For any p-ring A with residue ring k, the calculation in A is dominated by Q_i^* defined in(5.5.2.9), i.e.

$$\Big(\sum f(\alpha_i)p^i\Big) * \Big(\sum f(\beta_i)p^i\Big) = \sum f(\gamma_i)p^i$$

where $\gamma_i = Q_i^*(\alpha_0, \alpha_1, \ldots, \beta_0, \beta_1, \ldots)$. ⌟

Proof: There is a map θ from $\widehat{S} = \widehat{\mathbb{Z}}[X_i^{p^{-n}}, Y_i^{p^{-n}}]$ to A induced by $f(\alpha_i), f(\beta_i)$ as they all has p^{-n}-th roots. Then notice θ induce a $\overline{\theta}$ on residue ring and these two θ commutes with Teichmüller lift, as seen by the definition of the latter. Then the theorem follows immediately. □

Prop. (5.5.2.11) [Universal Properties of Strict p-Rings]. For two p-ring A, A' that A is strict, then any map φ of their residue ring induces a unique ring homomorphism $A \to A'$. In particular, two strict p-ring with the same residue ring is canonically isomorphic. ⌟

Proof: We have already seen that ring homomorphism commutes with Teichmüller lift. Now we define

$$g(a) = \sum g(f(\alpha_i))p^i = \sum f(\varphi(\alpha_i))p^i$$

and this is the unique choice. It is a ring homomorphism by universal law of(5.5.2.10). □

3 Witt Theory

References are [Michiel Hazewinkel, Formal Groups and Applications] and [Rab14].

Witt Vectors

Def. (5.5.3.1) [Divisor Stable Subsets]. A non-empty subset $P \subset \mathbb{Z}_+$ is called **divisor-stable** if it is stable under taking divisors.

For a divisor-stable subset P and $n \in \mathbb{Z}_+$, define $P(n) = \{m \in P | m \leq n\}$. ⌟

Def. (5.5.3.2) [Witt Polynomials]. For $n \in \mathbb{N}$, the n-th **Witt polynomial** is defined to be

$$W_n = \sum_{d|n} d X_d^{n/d} \in \mathbb{Z}[\{X_d : d|n\}].$$

For example,

$$W_{p^k} = X_1^{p^k} + pX_p^{p^{k-1}} + \ldots + p^n X_{p^n}.$$

⌟

Prop. (5.5.3.3)[Commutative Coalgebra Δ_P]. For a divisor-stable set P, let $\Delta_P = \mathbb{Z}[\{X_n | n \in P\}]$, then there is a unique commutative ring scheme structure on $\operatorname{Spec}\Delta_P$ s.t. the map

$$W_* : \mathbb{Z}[X_P] \to \Delta_P : n \mapsto W_n \in \Delta_P$$

induces a homomorphism of ring schemes $\operatorname{Spec}\Delta_P \to \operatorname{Spec}\mathbb{Z}[X_P]$, where the ring structure on $\operatorname{Spec} Z[X_P]$ is given by

$$\times : \mathbb{Z}[X_P] \to \mathbb{Z}[X_P]\otimes\mathbb{Z}[Y_P] : X_n \mapsto X_n \otimes Y_n, \quad + : \mathbb{Z}[X_P] \to \mathbb{Z}[X_P]\otimes\mathbb{Z}[Y_P] : X_n \mapsto X_n\otimes 1 + 1\otimes Y_n.$$

Then for another divisor-stable set $P' \subset P$, there is a natural map $\Delta_{P'} \to \Delta_P$ that induces a homomorphism of ring schemes.

If $P = \mathbb{Z}_+$, denote $\Delta_P = \Delta$, if $P = \{1, p, p^2, \ldots\}$, denote $\Delta_P = \Delta_p$, and if $P = \{1, p, \ldots, p^k\}$, denote $\Delta_P = \Delta_{p,k}$. ⌟

Proof: □

Cor. (5.5.3.4). S_n is of the form $S_n(X_P, Y_P) = X_n + Y_n + f_n(X_{P(n-1)}, Y_{P(n-1)})$. ⌟

Proof: □

Def. (5.5.3.5) [Witt Vectors]. For a divisor-stable set P, consider the functor

$$W_P : \mathcal{CA}\mathrm{lg} \to \mathcal{CA}\mathrm{lg} : A \mapsto W_P(A) = \operatorname{Hom}(\Delta_P, A),$$

then it is an exact functor, and by(5.5.3.3), there are natural ring homomorphism

$$W_* : W_P(A) \to \prod_P A : f \mapsto (f(W_n))_W$$

For $x \in W_P(A)$, $W_n(x)$ are called the **ghost components** of x, and $W_*(x)$ is called the **Witt coordinate** of x.

If $P = \mathbb{Z}_+$, $W_P(A)$ is denoted by $W(A)$, if $P = \{1, p, p^2, \ldots\}$, $W_P(A)$ is denoted by $W_p(A)$, and if $P = \{1, p, \ldots, p^k\}$, denote $W_P(A) = W_{p,k}(A)$. ⌟

Prop. (5.5.3.6) [Natural Coordinates]. There is another map

$$\varphi_* : W_P(A) \to \prod_P A : f \mapsto (f(X_i))$$

which is an isomorphism of sets, whose components are maps of sets $\varphi_n : W_P(A) \to A, n \in P$. WARNING: it is not an isomorphism of groups. For $x \in W_P(A)$, $\varphi_n(x)$ are called the **ghost components** of x, and $\varphi_*(x)$ is called the **Witt coordinate** of x. All coordinates of elements in x will be assumed to be in the natural coordinates by default.

Then the map $W_*\varphi_*^{-1}$ is given by

$$W_*\varphi_*^{-1} : \prod_P A \to \prod_P A : (x_n)_\varphi \mapsto (W_n(\{x_P\}))_W.$$

⌟

Cor. (5.5.3.7) [Witt Coordinates are Injective]. $W_* : W_P(A) \to \prod_P A$ is injective if A is n-torsion-free for any $n \in P$, and an isomorphism iff n is invertible in A for any $n \in P$.

This is very useful because it can prove equations by checking on each W_n. Also when checking universal equations, it is even not necessary that A is n-torsion-free, because any ring A is a quotient of a free $\mathbb{Z}$-algebra. ⌟

Proof: It suffices to prove for $W_*\varphi_*^{-1}$. Using the Witt polynomials and prove inductive on $n\in P$ s.t. if $x=(x_n)$ is mapped to 0, then $x_n=0$ for any $n\in P$.

In case n is invertible in A for any $n\in P$, solve x_n out of $W_*(x)$ inductively. □

Def. (5.5.3.8)[Topology on $W_P(A)$]. Let P be a divisor-stable set, then for any $A\in \mathcal{CA}\mathrm{lg}$, the natural map

$$W_P(A)\to \varprojlim_{n\in\mathbb{Z}_+} W_{P(n)}(A)$$

is an isomorphism of rings, so we can define the **natural topology** on $W_P(A)$ is as the profinite topology.

Then this topology makes $W_P(A)$ a topological ring, and it is discrete iff $\#P<\infty$, and W_P is a functor from $\mathcal{CA}\mathrm{lg}$ to the category of profinite rings. ⌟

Prop. (5.5.3.9). Let P be a divisor-stable set and $A\in\mathcal{CA}\mathrm{lg}$, then for $x=(x_n),y=(y_n)\in W_P(A)$, if $x_ny_n=0$ for any $n\in P$, then

$$x+y=(x_n+y_n)\in W_P(A).$$

⌟

Proof: It suffices to prove on Δ_P. By(5.5.3.7), it suffices to prove $W_n((x_n+y_n))=W_n(x)+W_n(y)$ for any $n\in P$. This is true because

$$W_n((x_n+y_n))=\sum_{d|n} d(x_d+y_d)^{n/d}=\sum_{d|n} dx_d^{n/d}+\sum_{d|n} dy_d^{n/d}=W_n(x)+W_n(y).$$

□

Prop. (5.5.3.10) [Teichmüller Lifts]. Let P be a divisor-stable set and $A\in\mathcal{CA}\mathrm{lg}$, for $a\in A$, denote $[a]=(a,0,\ldots)\in W_P(A)$. Then for any $x=(x_n)\in W_P(A)$,

$$[a]x=(a^nx_n).$$

In particular, $[\cdot]:A\to W_P(A)$ is multiplicative, called the **Teichmüller lifts** of A. ⌟

Proof: It suffices to prove on Δ_P. By(5.5.3.7), it suffices to prove $W_n((a^nx_n))=W_n([a]x)$ for any $n\in P$. This is because

$$W_n((a^nx_n))=\sum_{d|n} d(a^dx_d)^{n/d}=a^n\sum dx_d^{n/d}=W_n([a])W_n(x)=W_n([a]x).$$

□

Frobenius and Verschiebung Maps

Def. (5.5.3.11) [Verschiebung Maps]. ⌟

Def. (5.5.3.12) [Frobenius Maps]. ⌟

Prop. (5.5.3.13) [Frobenius and Verschiebung]. Let $n\in\mathbb{Z}_+$ and P is a divisor-stable subset s.t. $nP\subset P$. Let $A\in\mathcal{CA}\mathrm{lg}$, let $x,y\in W_P(A)$, then

- $F_n\circ V_n=n\cdot\mathrm{id}$.
- $V_n(F_n(x)y)=xV_n(y)$.

- If $(m,n)=1$, then $V_m\circ F_n=F_n\circ V_m$.
- For $m\in\mathbb{Z}_+$, $(V_n(x))^m=n^{m-1}V_n(X^m)$.

⌟

Proof: Cf.[Rab14]P18. □

<u>p**-Typical Witt Vectors**</u>

Prop. (5.5.3.14) [Structure of Δ_p]. The ring structure on Spec Δ_p is given by

$$\times:\Delta_p\to\Delta_p\otimes\Delta_p: X_{p^k}\mapsto S_k(X_P,Y_P),\quad +:\Delta_p\to\Delta_p\otimes\Delta_p: X_{p^k}\mapsto Z_k(X_P,Y_P)$$

where

$$S_1=X_1+Y_1,\quad S_2=X_p+Y_p+\sum_{i=1}^{p-1}\frac{1}{p}\binom{p}{i}X_1^iY_1^{p-i},$$

$$Z_1=X_1Y_1,\quad Z_2=X_1^pY_p+X_pY_1^p+pX_pY_p.$$

⌟

Proof: □

Cor. (5.5.3.15) [W_2]. Let $W_2=W_P$ where $P=\{1,p\}$, then $W_2(A)$ is the set $A\times A$(as the natural coordinates) with the addition and multiplication given by

$$(x_0,x_1)+(y_0,y_1)=(x_0+y_0,x_1+y_1+\frac{x_0^p+y_0^p-(x_0+y_0)^p}{p}),\quad (x_0,x_1)(y_0,y_1)=(x_0y_0,x_0^py_1+y_0^px_1+px_1y_1)$$

There are two natural morphism of rings $\varepsilon_1,\varepsilon_2:W_2(A)\to A$:

$$\varepsilon_1((x_0,x_1))=x_0,\quad \varepsilon_2((x_0,x_1))=x_0^p+px_1.$$

⌟

Prop. (5.5.3.16). For $k\geq 1$ and $A\in\mathcal{CA}\mathrm{lg}$, the kernel of $W_1:W_{p,k}(A)\to A$ is a nilpotent ideal. ⌟

Proof: Cf.[Basic Algebra 2, Jacobson]P508.? □

Cor. (5.5.3.17). An element $x\in W_{p,k}(A)$ is a unit iff $W_1(x)\in A$ is a unit. ⌟

Example (5.5.3.18) [p-Typical Witt Vectors].

- $W_p(\mathbb{F}_q)$ is the unramified extension of $\mathbb{Z}_p$ of degree $\log_p q$.
- $W_p(\overline{\mathbb{F}}_p)$ is the completion of the maximal unramified extension of $W_p(\mathbb{F}_p)$.

⌟

Proof:

□

Lemma (5.5.3.19) [Formula for p-Rings]. For $* = +$ or $\times$, there are integral polynomials $S_*(X_i, Y_i)$ that

$$\Big(\sum f(\alpha_i)p^i\Big) * \Big(\sum f(\beta_i)p^i\Big) = \sum f(\gamma_i)p^i$$

where $\gamma_i = Q_i^*(\alpha_0, \alpha_1, \ldots, \beta_0, \beta_1, \ldots)$. And for $+$, when reduced to $\mathbb{F}_p$, Q_i^+ are polynomials in $X_i^{p^{-n}}, Y_i^{p^{-n}}$ for $i \le n$ and homogenous of degree 1. And

$$Q_i^+ = (X_n + Y_n) + (X_{n-1}^{p^{-1}} + Y_{n-1}^{p^{-1}})R_{n,n-1} + \ldots + (X_0^{p^{-n}} + Y_0^{p^{-n}})R_{n,0}.$$

⌟

Proof: We solve S_n by induction. Notice for any lift $\widehat{S}_i$ of S_i,

$$f(S_i) \equiv \widehat{S}_i(X^{1/p^{n-i}}, Y^{1/p^{n-i}})^{p^{n-i}} \mod p^{n-i+1}$$

so we mod p^{n+1} to solve S_n:

$$S_n \equiv 1/p^n\Big(X_0 + Y_0 + \ldots + p^n X_n + p^n Y_n - \widehat{S}_0(X^{1/p^n}, Y^{1/p^n})^{p^n} - \ldots - p^{n-1}\widehat{S}_{n-1}(X^{1/p}, Y^{1/p})^p\Big)$$

The rest follows by inducition. □

Lemma (5.5.3.20). If k is a perfect field of characteristic p and R is a strict p-ring with residue field k, then the map

$$f : W_p(k) \to R : (x_1, x_p, x_{p^2}, \ldots) \mapsto \sum_{n=0}^{\infty} [x_{p^n}^{1/p^n}]p^n$$

is an isomorphism of topological rings. ⌟

Proof: We need to prove this is a ring homomorphism. That on $W(A)$ is to make φ a ring homomorphism, and that on the right is usual. It suffice to prove for the canonical strict p-ring, as seen by the universal law(5.5.2.10).

For this, we let $(\sum X_i^{p^{-i}}p^i) * (\sum Y_i^{p^{-i}}p^i) = \sum f(\psi_i(X_i, Y_i))^{p^{-i}}p^i$, and $W_n(a_i) * W_n(b_i) = W_n(\varphi_i)$, where $\psi_i \in \mathbb{F}_p[X_i, Y_i]$ and $\varphi_i \in \mathbb{Z}[X_i, Y_i]$, they both exist, the latter because of(5.5.4.7).

Then we mod p^{n+1}, and let $X_i = X_i^{p^n}$, $Y_i = Y_i^{p^n}$, so

$$W_n(\varphi_i) = W_n(X_i) * W_n(Y_i) \equiv \sum_{i \le n} f(\psi_i(X_i^{p^n}, Y_i^{p^n}))^{p^{-i}}p^i \equiv W_n(\psi_i) \mod p^{n+1}$$

Now induction, $\varphi_i \equiv \psi_i \mod p$, then $p^n\varphi_n \equiv p^n\psi_n \mod p^{n+1}$ so this is true for n, too.

Cf.[Rab14]P8, 20.**?** □

Prop. (5.5.3.21) [W_p For Perfect Rings]. For any perfect ring k of char p, there exists uniquely a strict p-ring $W(k)$ that has residue ring k, which is just the ring of Witt vectors $W_p(k)$.

Then W_p is a faithful functor from the category of perfect rings to the category of p-rings with perfect residue fields that is left adjoint to the functor mapping a p-ring with perfect residue fields to its residue field, by(5.5.2.11). ⌟

Proof: For a canonical ring $\mathbb{F}_p[X_\alpha^{p^{-n}}]$, $\widehat{\mathbb{Z}}[X_\alpha^{p^{-n}}]$ is a strict p-ring. Now arbitrary perfect p-ring is a quotient of $\mathbb{F}_p[X_\alpha^{p^{-n}}]$, so we can construct its strict p-ring $W(k)$ as the quotient of $\widehat{\mathbb{Z}}[X_\alpha^{p^{-n}}]$. Uniqueness is by(5.5.2.11).

Notice it is nothing mysterious, it is just the set of all formal sum $\sum f(x_i)p^i$ under the operation defined in(5.5.2.9). See also(5.5.3.20). □

Cor. (5.5.3.22). $W_{p,k}(\mathbb{F}_p) \cong \mathbb{Z}/(p^k)$. ⌟

Def. (5.5.3.23)[Witt Vectors over Valued Rings]. If a perfect ring R itself has a complete valuation v, then we can endow $W(R)$ with a finer topology: we let $w_k(x) = \inf_{i\le k} v(x_i)$, where $x = \sum p^i f(x_i)$. Now $w_k(x+y) \ge \inf(w_k(x), w_k(y))$ by(5.5.3.19). The **weak topology** of $W(R)$ is defined by the semi-valuations w_k. ⌟

Prop. (5.5.3.24). If $a, b \in \mathcal{O}_R + p^{n+1}W(R)$, then

$$p^n v(a_n - b_n) \ge w_n(a-b) \ge \inf_{k\le n} p^{-k} v(a_{n-k} - b_{n-k}).$$

So we see that a sequence is Cauchy in $W(R)$ if each coordinate is Cauchy in R, so $W(R)$ is complete in the weak topology. ⌟

Proof: Firstly the last proposition follows from the first because we can always multiply by a $f(\alpha)$ to make the first n coordinate in $\mathcal{O}_R$.

The first is nearly an immediate consequence of(5.5.3.19). □

Prop. (5.5.3.25). $\mathcal{O}_\mathcal{E} = W(K^{\frac{1}{p^\infty}})$ is a complete ring with maximal ideal $p\mathcal{O}_\mathcal{E}$. And $\mathcal{O}_\mathcal{E}[\frac{1}{p}] = \mathcal{E}$ is complete ring of character p. And the same construction of $\overline{K^{\frac{1}{p^\infty}}}$ yields the completion of maximal unramified extension of $\mathcal{O}_\mathcal{E}$, and the Galois group is the same as G_K. ⌟

Prop. (5.5.3.26) [van Der Kallen]. If $A \to B$ is an étale morphism, then $W_r(A) \to W_r(B)$ is also étale. Moreover, if $A \to A'$ is any ring map with $B' = B \otimes_A A'$, then the natural map

$$W_r(A') \otimes_{W_r(A)} W_r(B) \to W_r(B')$$

is also an isomorphism. ⌟

Proof: Cf.[Integral p-adic Hodge, BMS]. □

Cohen Rings

Def. (5.5.3.27)[Cohen Rings]. For any $k \in \texttt{Field}^p$, there exists a unique absolutely unramified DVR of characteristic 0 and residue field k, denoted by $\mathrm{Coh}(k)$. ⌟

Proof: Cf.[Fontaine-OuYang]P185.**?** □

Cor. (5.5.3.28). If $k_0 = k^{\mathrm{perf}}$, then $W(k_0) \subset \mathrm{Coh}(k) \subset W(k)$. ⌟

4 δ-Rings

Def. (5.5.4.1)[δ-Ring]. A δ-ring structure on R characterize the deficit in lifting the Frobenius action on R/p. i.e. $\varphi(x) = x^p + p\delta(x)$. A **$\delta$-ring** is a pair (R, δ) where R is a commutative ring and $\delta : R \to R$ is a map that $\delta(0) = \delta(1) = 0$, and satisfies:

$$\delta(xy) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y), \quad \delta(x+y) = \delta(x) + \delta(y) - \frac{(x+y)^p - x^p - y^p}{p}.$$

δ-rings naturally form a category, denoted by $\mathcal{CA}\mathrm{lg}^\delta$. And in case A is p-torsionfree, a δ-structure on A is the same as a lifting of the Frobenius on A/p. ⌟

Def. (5.5.4.2) [δ-Pairs]. The category of δ**-pairs** consists of pairs (A, I) where A is a δ-ring and I is an ideal of A that morphisms $\varphi : (A, I) \to (B, J)$ are δ-ring maps $A \to B$ that $\varphi(I) \subset J$. ⌟

Prop. (5.5.4.3) [δ-Rings and W_2]. A δ-ring structure on A is the same as a section of the map $W_1 : W_2(A) \to A$, and a morphism of δ-rings is a commutative diagram of sections. ⌟

Proof: By the description of W_2 in(5.5.3.15), this is clear, the morphism is given by $A \to W_2(A) : x \mapsto (x, \delta(x))$. □

Lemma (5.5.4.4) [Initial δ-Algebra]. We usually work with δ-algebras over $\mathbb{Z}_{(p)}$. Then there is an initial object in the category of δ-rings, given by $Z_{(p)}$ with $\delta(x) = \frac{x-x^p}{p}$. ⌟

Prop. (5.5.4.5). For a δ-ring A, φ commutes with δ. ⌟

Proof: We need to check $\delta(x^p + p\delta(x)) = \delta(x)^p + p\delta(\delta(x))$. This is hard to check, but we can check $\varphi(\frac{\varphi(x)-x^p}{p}) = \frac{\varphi(\varphi(x))-\varphi(x)^p}{p}$, so the conclusion is true when A is p-torsion-free. But by(5.5.4.10), every δ-ring is a quotient of a free thus p-torsionfree ring, thus the equation is also true for arbitrary A. □

Def. (5.5.4.6) [Commutative Coalgebra $\mathbb{Z}[\delta]$]. Denote $\mathbb{Z}[\delta] = \mathbb{Z}[e, \delta_1, \ldots, \delta_n, \ldots]$. Using the formulas in(5.5.4.1), we can write $\delta^{\circ n}(xy)$ and $\delta^{\circ n}(x + y)$ as functions of $\delta^{\circ i}(x), \delta^{\circ i}(y)$ for $0 \leq i \leq n$, i.e.

$$\delta^n(xy) = M_n(x, \delta(x), \delta^{\circ 2}(x), \ldots, \delta^{\circ n}(x), y, \delta(y), \ldots, \delta^{\circ n}(y))$$

$$\delta^n(x + y) = S_n(x, \delta(x), \delta^{\circ 2}(x), \ldots, \delta^{\circ n}(x), y, \delta(y), \ldots, \delta^{\circ n}(y))$$

Then we can change $\delta^{\circ n}$ to δ_n to define a commutative ring scheme structure on $\operatorname{Spec} \mathbb{Z}[\delta]$:

$$\times : \mathbb{Z}[\delta] \to \mathbb{Z}[\delta] \otimes \mathbb{Z}[\delta] : \delta_n \mapsto M_n, \quad + : \mathbb{Z}[\delta] \to \mathbb{Z}[\delta] \otimes \mathbb{Z}[\delta] : \delta_n \mapsto S_n.$$

it is easily prove by induction that if we denote $\mathbb{Z}[\varphi] = \mathbb{Z}[e, \varphi, \varphi_2, \ldots, \varphi_n, \ldots]$, and $\operatorname{Spec} \mathbb{Z}[\varphi]$ the commutative ring scheme with the ring structure given by

$$\times : \mathbb{Z}[\varphi] \to \mathbb{Z}[\varphi] \otimes \mathbb{Z}[\varphi] : \varphi_n \mapsto \varphi_n \otimes \varphi_n, \quad + : \mathbb{Z}[\varphi] \to \mathbb{Z}[\varphi] \otimes \mathbb{Z}[\varphi] : \varphi_n \mapsto \varphi_n \otimes 1 + 1 \otimes \varphi_n,$$

then the map

$$Z[\varphi] \to \mathbb{Z}[\delta] : \varphi_n \mapsto \text{expansion of } \varphi^{\circ n} \in \mathbb{Z}[e, \delta_1, \ldots, \delta_n]$$

induces a homomorphism of ring schemes $\operatorname{Spec} \mathbb{Z}[\delta] \to \operatorname{Spec} \mathbb{Z}[\varphi]$.

There is a natural functor:

$$[\delta] : \mathbb{Z}[\delta] \to \mathbb{Z}[\delta] : \delta_i \mapsto \delta_{i+1}$$

⌟

Lemma (5.5.4.7) [δ-Component]. Let $\varphi = e^p + p\delta$ be a polynomial in e, δ, then there are polynomials $\Theta_n \in \mathbb{Z}[e, \delta_1, \delta_2, \ldots, \delta_n]$ s.t.

$$\varphi^{\circ n} = \Theta_0^{p^n} + p\Theta_1^{p^{n-1}} + \cdots + p^n\Theta_n = W_{p^n}(\Theta_0, \ldots, \Theta_n), \forall n$$

In particular, $\Theta_0 = e, \Theta_1 = \delta$.

Moreover, $\mathbb{Z}[\Theta_0, \Theta_1, \ldots, \Theta_n] = \mathbb{Z}[e, \delta_1, \delta_2, \ldots, \delta_n]$ for any n. ⌟

Proof: Use equation $\varphi \circ \varphi^n = \varphi^n \circ \varphi$ and module $p^n\mathbb{Z}[\Theta_0, \Theta_1, \ldots, \Theta_n]$.**?** □

Prop. (5.5.4.8) [Witt Vectors as δ-Rings]. By(5.5.4.7), there is an isomorphism of algebras

$$\Delta_p \cong \mathbb{Z}[\delta] : X_{p^n} \mapsto \Theta_n,$$

but it is also an isomorphism of ring schemes because of the uniqueness property of(5.5.3.3).

Then for any $A \in \mathcal{CA}\mathrm{lg}$, every element of $W_p(A)$ has a δ-coordinates:

$$f \in W_p(A) = \mathrm{Hom}(\Delta_p, A) \mapsto (f(e), f(\delta_1), f(\delta_2), \ldots)_\delta.$$

Let $W_p(A)$ be defined as in(5.5.3.5), then $[\delta] : \mathbb{Z}[\delta] \to \mathbb{Z}[\delta]$ induces a homomorphism $\delta : W_p(A) \to W_p(A)$ that can be checked to be a δ-functor from our definition of coalgebra structure on $\mathbb{Z}[\delta]$. Thus W_p is a functor $\mathcal{CA}\mathrm{lg} \to \mathcal{CA}\mathrm{lg}^\delta$. ⌟

Prop. (5.5.4.9) [Witt Vectors as an Right Adjoints]. W_p is right adjoint to the forgetful functor $\mathcal{CA}\mathrm{lg}^\delta \to \mathcal{CA}\mathrm{lg}$. ⌟

Proof: Given a ring homomorphism $f : B \to A$, let

$$f^\delta : B \to W_p(A) : x \mapsto (f(x), f(\delta(x)), f(\delta^{\circ 2}(x)), \ldots)_\delta,$$

Then f^δ is a δ-ring homomorphism: It is a homomorphism by our definition of the ring structure on $\mathrm{Spec}\,\mathbb{Z}[\delta]$(5.5.4.6), and it is a δ-ring homomorphism by our definition δ-ring structure(5.5.4.8).

And it is easy to see f^δ is the unique δ-ring homomorphism $B \to W(A)$ that restricts to $f : B \to A$, thus

$$\mathrm{Hom}^\delta(B, W(A)) \cong \mathrm{Hom}(B, A).$$

□

Prop. (5.5.4.10) [Free δ-Rings]. The ring $\mathbb{Z}\{x_i\}$ is a ring on the free generators $\{x, \delta(x_i), \delta^2(x_i), \ldots\}$ and the Frobenius morphism defined by asserting $\varphi(\delta^i(x)) = \delta^i(x)^p + p\delta^{i+1}(x)$.

Generally we can define the **free δ-ring** generated by $\{x_i\}$ over a δ-ring A as the tensor $A \otimes \mathbb{Z}\{x_i\}$, and it satisfies the universal property.

Then the Frobenius action is f.f.. ⌟

Proof: It is easily verified that for any δ-ring R over A and a map of sets $\{x_i\} \to R$, there is a unique morphism $\mathbb{Z}_{(p)}\{x_i\} \to R$ sending x to f, thus verifying the universal property.

For the f.f., notice it is a colimit of $\varphi_n : \mathbb{Z}[x, \delta(x), \ldots, \delta^n(x)] \to \mathbb{Z}[x, \delta(x), \ldots, \delta^{n+1}(x)]$, so by(5.4.1.25), it suffices to show φ_n are all f.f.. We decompose this map as n maps:

$$\mathbb{Z}[x, \delta(x), \ldots, \delta^n(x)] \cong \mathbb{Z}[x, \delta(x), \ldots, (\delta^i(x))^p, \ldots, \delta^n(x)] \subset \mathbb{Z}[x, \delta(x), \ldots, \delta^n(x)]$$

which are all f.f., so it is f.f. □

Cor. (5.5.4.11) [Frobenius is Fpqc locally Surjective]. For a δ-ring A and an element $x \in A$, there is a faithfully flat morphism of δ-rings $A \to B$ that the image of x in B is of the form $\varphi(y)$ for some $y \in B$. ⌟

Cor. (5.5.4.12). Set B as the pushout of the diagram $\mathbb{Z}_{(p)}\{s\} \leftarrow \mathbb{Z}_{(p)}\{t\} \to A$, where the arrows sends t to $\varphi(s)$ and x. B exists by(5.5.4.13) and the underlying ring is the same as the ring pushout, thus $A \to B$ is faithfully flat by(5.5.4.10). ⌟

Prop. (5.5.4.13) [Limits and Colimits of δ-Rings]. $\mathcal{CA}\mathrm{lg}^\delta$ admits limits and colimits, and their underlying rings are just the ring-theoretical limit and colimit, as the forgetful functor $\mathcal{CA}\mathrm{lg}^\delta \to \mathcal{CA}\mathrm{lg}$ has both left and right adjoints (5.5.4.9)(5.5.4.10). ⌟

Proof: Use(5.5.4.3), the construction of limits is straightforward, as W_2 commutes with limits. To construct colimits, notice the morphisms $A_i \to W_2(A_i)$ induces a morphism

$$\varinjlim A_i \to \varinjlim W_2(A_i) \to W_2(\varinjlim A_i)$$

and clearly this map is a section of $W_2(\varinjlim A_i) \to \varinjlim A_i$, thus given a δ-ring structure on $\varinjlim A_i$.

It is a colimit because any commutative diagrams $\varphi_i : (A_i \to W_2(A_i)) \to (B \to W_2(B))$ induces a unique commutative diagram

$$\begin{array}{ccccc}
\varinjlim_i A_i & \longrightarrow & \varinjlim W_2(A_i) & \xrightarrow{\varinjlim W_2(\varphi_{ij})} & W_2(\varinjlim A_i) \\
\downarrow{\scriptstyle \varinjlim \varphi_i} & & \downarrow & \swarrow{\scriptstyle W_2(\varinjlim \varphi_i)} & \\
B & \longrightarrow & W_2(B) & &
\end{array}.$$

□

<u>**Extension of δ-Structures**</u>

Lemma (5.5.4.14) [Quotients]. Let A be a δ-ring and I be an ideal, then if I is stable under δ, then there is a natural δ-structure on A/I compatible with A. In general, if J is an ideal of A, then there is a universal δ-A-algebra $B = A/J$, where $J = \cup_{n\geq 0}\delta^n(I)$. It is the universal δ-A-algebra that the image of I is 0. ⌟

Lemma (5.5.4.15) [Localization]. Let A be a δ-ring and S be a multiplicative set of A that $\varphi(S) \in S$, then there is a unique δ-structure on $S^{-1}A$, and it satisfies the universal property. ⌟

Proof: Firstly if A is p-torsionfree, in this case a δ-structure is the same as a lifting of the Frobenius on A/p, thus the proposition is clear because $\varphi_{S^{-1}A} : S^{-1}A \to S^{-1}A$ is uniquely determined.

Generally, we choose a free δ-ring F and a surjection $\alpha : F \to A$, then $T = \alpha^{-1}S$ is multiplicative, and $T^{-1}F$ admits a unique δ-structure. But now $S^{-1}A = T^{-1}F \otimes_F A$, so there is a δ-structure on $S^{-1}A$ as the colimit, so compatible with that of $S^{-1}A$. Then it's also the unique one(because if there is another one, the colimit properties gives a morphism of δ-rings above $\mathrm{id}_{S^{-1}A}$, which must by identity). □

Lemma (5.5.4.16) [p-adic Localization]. If A is a δ-ring with $p \in \mathrm{rad}(A)$, then the formula $\varphi(f) = f^p + p\delta(f)$ shows if f is a unit, then $\varphi(f)$ is also a unit(3.6.2.2), so $S^{-1}A = T^{-1}A$, where $T = \{S, \varphi(S), \varphi^2(S), \ldots\}$.

Thus for any δ-ring A and a multiplicative set S, the p-localization(5.1.1.32) $(S^{-1}A)_{(p)}$ is the same as the p-localization of $T^{-1}A$. Then(5.5.4.15) shows that $(S^{-1}A)_{(p)}$ carries a unique δ-structure compatible with that of A. ⌟

Lemma (5.5.4.17) [Completions]. For a δ-ring A and a f.g. ideal I, the I-adic completion of A has a unique δ-structure compatible with that of A. ⌟

Proof: Let $A \to W_2(A)$ corresponds to the δ-structure by(5.5.4.3), then there is a natural map $A \to W_2(A) \to W_2(\widetilde{A})$, then by the universal property of complete, it extends to a map $\widetilde{A} \to W_2(\widetilde{A})$, which is a ring map and is a section, all by universal properties. □

Lemma (5.5.4.18) [Derived Completion]. If A is a δ-ring and $I \subset A$ is an ideal containing p, then the derived I-completion ring $\widehat{A}$ of A admits a unique δ-structure extending that of A. ⌟

Proof: The proof is similar as(5.5.4.17). □

Prop. (5.5.4.19) [Étale Extension]. Let A be a δ-ring with a f.g. ideal I containing p. Assume B is a derived I-complete and I-completely étale A-algebra, then B admits a unique δ-structure compatible with that of A.

In particular, any δ-structure on an algebra A passes uniquely to its derived I-completion for any ideal $I \subset A$ containing p. ⌟

Proof: By Elkik's algebraization(5.9.7.9), we can write B as derived I-completion of some étale A-algebra B'. Then $W_2(A) \to W_2(B')$ is étale by van der Kallen's theorem(5.5.3.26). Then $W_2(B)$ is the derived I-completion of $W_2(B')$, with the A-algebra structure given by $A \to W_2(A) \to W_2(B')$. For the rest, Cf.[Scholze, Prism, 2.18]. □

Distinguished Elements

Def. (5.5.4.20) [Distinguished Elements]. In a δ-ring A, an element d is called a **distinguished element** if $\delta(d)$ is a unit in A. A distinguished element is preserved by a δ-ring map. ⌟

Lemma (5.5.4.21) [Distinguished up to units]. If A is a δ-ring, d is distinguished and u is a unit, then ud is also distinguished, if $d, p \in \mathrm{rad}(A)$. ⌟

Proof: $\delta(ud) = u^p\delta(d) + d^p\delta(u) + p\delta(u)\delta(d)$ is a unit. □

Lemma (5.5.4.22) [Irreducibility of Distinguished Elements]. Let A be a δ-ring and d be distinguished element in A. If $d = fh$ for some $f, h \in A$ that $f, p \in \mathrm{rad}(A)$, then f is also distinguished and h is a unit. ⌟

Proof: Notice that $\delta(d) = f^p\delta(h) + h^p\delta(f) + p\delta(f)\delta(h)$, $\delta(d)$ is a unit, $f^p\delta(h) + p\delta(f)\delta(h) \in \mathrm{rad}(A)$, thus $h^p\delta(f)$ is a unit, so we are done. □

Prop. (5.5.4.23) [Characterization of Distinguished Elements]. Fix a δ-ring A and an element d that $d, p \in \mathrm{rad}(A)$, then d is distinguished iff $p \in (d, \varphi(d))$. In particular, distinguished elements is stable under units. ⌟

Proof: If d is distinguished, then $\delta(d)$ is a unit, thus $\varphi(d) = d^p + d^p + p\delta(d)$ shows immediately $p \in (d, \varphi(d))$. Conversely, if $p = ad + b\varphi(d)$, we show $\delta(d)$ is invertible. It suffices to show it is invertible modulo (d, p) as $d, p \in \mathrm{rad}(A)$, or equivalently $(p, d, \varphi(d)) = A$. If it is not the case, then we may take a $(p, d, \varphi(d))$-adic completion to assume $p, d, \varphi \in \mathrm{rad}(A)$, thus the equation simplifies to $p(1 - b\delta(d)) = cd$. The left side is distinguished, by(5.5.4.21), and then d is also distinguished, by(5.5.4.22), so truly $(p, d, \varphi(d)) = A$. □

Prop. (5.5.4.24) [Examples of Distinguished Elements]. The element d is distinguished in the following cases:

- (Crystalline cohomology)Take $A = \mathbb{Z}_{(p)}$ and $d = p$, then $\delta(p) = 1 - p^{p-1}$ is a unit.

- (q-de Rham cohomology) Take $A = \mathbb{Z}_p[[q-1]]$ and $d = [p]_q = \sum_{i=0}^{p-1} q^i \in A$, with the δ-structure determined by $\varphi(q) = q^p$.
- (Breuil-Kisin cohomology)Fix a discretely valued field K/Q_p with uniformizer π, W the maximal unramified subring of $\mathcal{O}_K$. Take $A = W[[u]]$ with $\delta(u) = u^p$, then any generator of the kernel of the map of $A \to \mathcal{O}_K : u \mapsto \pi$ is distinguished**?**.
- (A_{inf}-cohomology)Let A be the $(p, q-1)$-completion of $\mathbb{Z}_p[q^{\frac{1}{p^\infty}}]$. Then A is p-torsion free and $\varphi(q) = q^p$ gives a δ-structure. Then $d = [p]_q$ defined in item2 is also distinguished. And $\varphi^n(d)$ is distinguished for any $n \in \mathbb{Z}$ by(5.5.4.5).

⌟

Proof: 2: It is clear φ is continuous and δ stablizes $(q-1)$, and d is distinguished because the image of $\delta(d)$ in $A/(q-1) \cong \mathbb{Z}_q$ is $\delta(p) = 1 - p^{p-1}$ is a unit, thus it is also a unit in A. □

Perfect δ-Ring

Def. (5.5.4.25) [Perfect δ-Ring]. A **perfect δ-ring** is a δ-ring that φ is an isomorphism. ⌟

Prop. (5.5.4.26) [Perfections]. The inclusion of the category of perfect δ-rings to the category of δ-rings admits left and right adjoints, A_{perf} and A^{perf} with definition similar to(5.5.1.9). ⌟

Proof: We use(5.5.4.3), the map $A \to W_2(A) \to W_2(A_{\text{perf}})$ extends uniquely to a map $A_{\text{perf}} \to W_2(A_{\text{perf}})$ lifting the δ-action of A. Similarly, because $(-)^{\text{perf}}$ is a limit and $W_2(-)$ is a right adjoint, then $W_2(-)$ commutes with $(-)^{\text{perf}}$. In particular, there is a natural map $A^{\text{perf}} \to W_2(A^{\text{perf}})$. □

Lemma (5.5.4.27) [Frobenius Kills p-Torsion]. If A is a δ-ring and $x \in A$ satisfies $px = 0$, then $\varphi(x) = 0$. In particular, if A is perfect, then A is p-torsionfree. ⌟

Proof: Applying δ to $px = 0$, we have $0 = p^p\delta(x) + x^p\delta(p) + p\delta(x)\delta(p) = p^p\delta(x) + \varphi(x)\delta(p)$. As $\delta(p)$ is a unit, and $p^p\delta(x) = p^{p-1}(\varphi(x) - x^p) = \varphi(p^{p-1}x) - p^{p-1}x^p = 0$, thus $\varphi(x) = 0$. □

Prop. (5.5.4.28) [Perfect p-Complete δ-Rings]. The following categories are equivalent:

- The category of perfect p-adically complete δ-rings.
- The category p-adically complete and p-torsionfree rings A with A/p perfect.
- The perfect $\mathbb{F}_p$-algebras.

In particular, every perfect p-complete δ-ring is of the form $W(k)$ thus has Teichmuller expansions. ⌟

Proof: 2 and 3 are equivalent by Witt vector construction, by(7.1.4.3), noticing that there is a natural lifting on $W(k)$ lifting the Frobenius of $k/\mathbb{F}_p$ that induces a δ-functor**?**. There is a forgetful functor from 1 to 2, by(5.5.4.27)(notice A/p is also perfect because if $\varphi(x) \in (p)$, then $x \in \varphi^{-1}(p) = (p)$ as $\varphi(p) = p\varphi(1) = p$) and it is faithful. Now there is an equivalence from $3 \to 1 \to 2$, thus $1 \to 2$ is essentially surjective thus is an equivalence. □

Prop. (5.5.4.29)[Perfect Element has Rank 1]. Fix a δ-ring A and an element $x \in A$, then $\delta(x^{p^n}) \in p^nA$ for any n. In particular, if A is p-adically separated and y is perfect in A, then $\delta(y) = 0$. ⌟

Proof: By formal calculation, it suffices to show that $p\delta(x^{p^n}) \in p^{n+1}A$, which is equivalent to $\varphi(x^{p^n}) \equiv x^{p^{n+1}} \mod p^{n+1}A$, which is true by(2.6.3.9). □

Prop. (5.5.4.30) [Distinguished Elements in Perfect δ-Rings]. Let A be a perfect p-complete δ-ring(or perfect $\mathbb{F}_p$-algebra by(5.5.4.28)), and $d \in A$, then d is distinguished iff its coefficient of p in the Teichmuller expansion(5.5.4.28) is a unit.

If d is distinguished, then it is a nonzero-divisor, and $A/d[p^\infty] = A/d[p]$. ⌟

Proof: Let $d = \sum_{i\geq 0}[a_i]p^i$, then

$$\delta(d) = \frac{1}{p}(\sum_{i\geq 0}[a_i^p]p^i - (\sum_{i\geq 0}[a_i]p^i)^p) \equiv [a_1^p] \mod pA$$

thus it is a unit iff a_1 is a unit, because A is p-complete.

Now if d is distinguished, and $fd = 0$. If $f \neq 0$, we may assume $p \nmid f$, because A is p-torsionfree and p-adically complete(5.5.4.28). Now

$$\varphi(f)\delta(fd) = \varphi(f)(f^p\delta(d) + \delta(f)\varphi(d)) = \varphi(f)f^p\delta(d) = 0,$$

so $f^p\varphi(f) = 0$, and $f^{2p} \equiv 0 \mod p$. Hence $f \equiv 0 \mod p$, but then $p|f$, contradiction.

For the last assertion, it suffices to show that $A/d[p^2] = A/d[p]$. If $p^2 f = dg$, then $\varphi(g)\delta(gd) = \varphi(g)(\delta(d)g^p + \varphi(d)\delta(g)) = \varphi(g)\delta(d)g^p + \varphi(dg)\delta(g) \in pA$, thus $\varphi(g)g^p \in pA$, hence $g^{2p} \in pA$, and hence $g \in pA$, showing $pf \in dA$. □

5.6 Divided Power Algebras

Basics

Def. (5.6.0.1)[PD-Structures]. Let I be an ideal of a commutative ring A, a **devided power structure** or **pd-structure** on I is a collection of maps $I_n : I \to A, n \geq 0$ that

- $\gamma_0(x) = 1, \gamma_1(x) = x, \gamma_n(x) \in I \forall n$.
- $\gamma_n(x+y) = \sum \gamma_{n-i}(x)\gamma_i(y)$.
- $\gamma_n(\lambda x) = \lambda^n \gamma_n(x), \lambda \in A, x \in I$.
- $\gamma_m(x)\gamma_n(x) = \binom{m+n}{n}\gamma_{m+n}(x)$.
- $\gamma_n(\gamma_m(x)) = \frac{(mn)!}{(m!)^n n!}\gamma_{mn}(x)$.

It is a simulation of the divided power $\gamma_n(x) = \frac{x^n}{n!}$ in case $n!$ is definable.

A **divided power ring** is a triple (A, I, γ) where I is an ideal of a commutative ring A and γ is a pd-structure on I. A morphism of divided power rings is a morphism of pairs (A, I) that preserves pd-structures.

For a pd-structure (A, I), denote $I^{[n]}$ the ideal generated by $\prod_i \gamma_{n_i}(x_i)$ where $x_i \in I$ and $\sum n_i \geq n$. ⌟

Prop. (5.6.0.2)[Limits and Colimits]. The category of divided power rings has all limits and colimits, the limits commute with forget functors but the colimits don't. However, the colimit always commutes with the functor taking (A, I) to A/I. This can be seen from the universal property of colimit applied to the pd-structures that $I = 0$. ⌟

Proof: The construction of the limit is clear. For the colimits, we use representability criterion(4.1.1.27), Cf.[[Sta]07GX]**?**. □

Prop. (5.6.0.3). Let A be a ring and I an ideal of A, then if γ is a pd-structure on I, then $n!\gamma(x) = x^n$. ⌟

Proof: If γ is a pd-structure, then we have $n\gamma_n(x) = \gamma_1(x)\gamma_{n-1}(x)$, so we can use induction. □

Prop. (5.6.0.4). If I, J are two ideals of A and γ a pd-structure on I and δ a pd-structure on J, then

- γ, δ agree on IJ.
- If γ, δ agree on $I \cap J$, then they extends to a pd-structure on $I + J$.

⌟

Proof: 1: for $x \in I, y \in J$, $\gamma_n(xy) = y^n\gamma_n(x) = n!\delta_n(y)\gamma_n(x) = \delta(xy)$.

2: direct calculation. □

Prop. (5.6.0.5)[p-Nilpotent and Thickening]. Let p be a prime and (A, I, γ) a pd-structure. Assume p is nilpotent in A/I, then I is locally nilpotent iff p is nilpotent in A, equivalently (A, I, γ) is a pd-thickening. ⌟

Proof: If $p^N = 0 \in A$, then for any $x \in I$, $x^{pN} = (pN)!\gamma_{pN}(x) = 0$. Then converse is trivial. □

Constructing PD-Structures

Prop. (5.6.0.6) [$\mathbb{Z}_{(p)}$-Algebras]. Cf.[[Sta]07GN]. ⌟

Prop. (5.6.0.7). Let A be a $\mathbb{Z}_{(p)}$-algebra and I is an ideal, then two pd-structures γ, γ' on γ are equal iff $\gamma_p = \gamma'$. Moreover, given a map $\delta : I \to I$ that

- $p!\delta(x) = x^p$,
- $\delta(ax) = a^p\delta(x)$ for any $a \in A, x \in I$,
- $\delta(x+y) = \delta(x) + \delta(y) + \sum_{i+j=p, i>0, j>0} \frac{1}{i!j!}x^i y^j$.

Then there exists a unique pd-structure on I that $\gamma_p = \delta$. ⌟

Proof: Just notice that $\gamma_n(x) = dx\gamma_{n-1}(x)$ for some c invertible in $\mathbb{Z}_{(p)}$, and also $\gamma_{pm}(x) = c\gamma_m(\gamma_p(x))$ for some c invertible in $\mathbb{Z}_{(p)}$, thus γ is uniquely determined, and we can also define γ_n inductively in this way, and the verification of axioms in in[[Sta]07GS]. □

Prop. (5.6.0.8). Let A be a $\mathbb{Z}$-torsion-free ring and I an ideal of A, then:

- I has at most one pd-stuucture.
- if $\gamma_n : I \to I$ are maps, then γ is a pd-structure iff $n!\gamma_n(x) = x^n$.
- I has a pd-structure iff there is a set of generators $\{x_i\}$ of I that $x_i^n \in n!I$.

⌟

Proof: 1 is clear from(5.6.0.3).

2: because $A \subset A \otimes_{\mathbb{Z}} \mathbb{Q}$, we can verify in $A \otimes_{\mathbb{Z}} \mathbb{Q}$, then the verifications are trivial.

3: Use the axioms to extend linearly and additively. □

Prop. (5.6.0.9) [DVR]. If R is a DVR in char 0 with residue field of char p and ramification p and maximal ideal $\mathfrak{m}$, then $\mathfrak{m}$ has a pd-stucture iff $e \leq p-1$. ⌟

Proof: As R has char0, it has at most one pd-structure by(5.6.0.8), and we need to show that $x^n/n!$ is in $\mathfrak{m}$ for any $x \in \mathfrak{m}$. And using(2.6.3.28), we are done. □

Extending PD-Structure

Def. (5.6.0.10) [Extending PD-Structure]. Let (A, I, γ) be a pd-structure and B is an A-algebra, we say that γ extends to B if $A \to B$ extends to a morphism of pd-structures $(A, I, \gamma) \to (B, IB, \gamma')$.

Let $(A, I), (B, J)$ be two pd-structures and B is an A-algebra, then these two pd-structures are said to be compatible iff the pd-structure on A extends to B and the pd-structure on J and IB coincides, or equivalently, there is a pd-structure on $IB + J$ compatible with IB and J, by(5.6.0.4). ⌟

Prop. (5.6.0.11) [Extendability]. Let (A, I) is a pd-structure and B an A-algebra, if any of the following holds:

- $IB = 0$,
- I is principal,
- $B[I] = 0$, (e.g. $A \to B$ is flat).

then γ extends to B. ⌟

Proof: 1 is trivial.

2: if $I = (x)$, we define $\gamma_n(bx) = b^n\gamma_n(x)$. This is well defined: if $(b - b')x = 0$, then $(b^n - (b')^n)\gamma_n(x) = 0$ because $\gamma_n(x) \in (x)$. Verifications of axioms is routine.

3: The condition shows $I \otimes_A B \cong IB$, thus it suffices to define γ on $I \otimes_A B$. For this we define on $I \times B$ and descend: let $\gamma_n((x, b)) = b^n\gamma_n(x)$ and extend by freeness and axioms in(5.6.0.1), then it is easy to show it is bi-additive and A-linear, so descend to $I \otimes B$ by(3.2.4.13). □

Prop. (5.6.0.12) [PD-Structure and Completions]. Let (A, I, γ) be a pd-structure that p is nilpotent in A/I, then each γ_n is continuous in the p-adic topology and extends to a pd-structure $\widehat{\gamma}$ on $\widehat{I}$.

If moreover A is a $\mathbb{Z}_{(p)}$-algebra, then for e large, $p^eA \in I$ is preserved by γ and

$$(\widehat{A}, \widehat{I}, \widehat{\gamma}) = \mathrm{colim}_e(A/p^eA, I/p^eA, \gamma).$$

⌟

Proof: Let $p^t \in I$, then 1 follows from(5.2.3.8). γ_n is clearly continuous, and γ_n preserves p^eA because

$$\gamma_n(p^ea) = p^n\gamma_n(p^{e-1}a) = \frac{p^n}{n!}p^{n(e-1)}a^n \in p^eA.$$

The limit equation follows from(5.6.0.2). □

Prop. (5.6.0.13) [Quotient]. Let (A, I, γ) be a pd-structure and $\mathfrak{a} \subset A$ is an ideal, and $I' = I \cap \mathfrak{a}$, then the following are equivalent:

- δ extends to $A/\mathfrak{a}$.
- I' is preserved by γ.
- There is a set of generator x_i of I' that $\gamma_n(x_i) \in I'$ for all n, i.

⌟

Proof: $1 \to 2 \to 3$ is clear. $2 \to 1$: we can just define $\gamma(x + I) = \gamma(x) + I$, which is well defined by axiom2 of(5.6.0.1). $3 \to 2$ is clear. □

Def. (5.6.0.14) [Free PD-Algebra]. For a pd-structure (A, I, δ), the **free pd-algebra** $A\langle t_1, \ldots, t_n\rangle$ is defined to be the A-algebra generated by symbols $t_i^{[n_i]}$, where $n_i > 0$, modulo the algebraic relations $t_i^{[m]}t_i^{[n]} = \binom{m+n}{n}t_i^{[m+n]}$. Denote by $A\langle t_1, \ldots, t_n\rangle_+$ the ideal generated by $t_i^{[n_i]}$ where $n_i > 0$.

Then the ideal J generated by I and $A\langle t_1, \ldots, t_n\rangle_+$, where $n_i > 0$ has a unique pd-structure that $\gamma_n(t_i) = t_i^{[n]}$ and $(A, I, \delta) \to (A\langle t_1, \ldots, t_n\rangle, J, \gamma)$ is a morphism of pd-structures.

It has a universal property that $\mathrm{Hom}(((A\langle t_1, \ldots, t_n\rangle, J, \gamma), (C, K, \varepsilon)$ is the same as $\mathrm{Hom}((A, I, \delta), (C, K, \varepsilon))$ with specified n elements in K. ⌟

Proof: Because $IA\langle t_i\rangle \cap A\langle t_1, \ldots, t_n\rangle_+ = IA\langle t_i\rangle + A\langle t_1, \ldots, t_n\rangle_+$, by(5.6.0.4), it suffices to construct pd-structures on $IA\langle t_i\rangle$ and $A\langle t_1, \ldots, t_n\rangle_+$. The former is by(5.6.0.11) and for the latter: if A is torsion-free, then we can use(5.6.0.8) because $\gamma_m(x)^n = n!\gamma_n(\gamma_m(x)) = \frac{(mn)!}{(m!)^n}\gamma_{mn}(x) \in n!A\langle t_1, \ldots, t_n\rangle_+$. In general, we write $A = R/\mathfrak{a}$ where R is a torsion-free pd-structure(can choose $\mathbb{Z}\langle A\rangle$), so there is a pd-structure on $R\langle t_i\rangle$, and $R\langle t_i\rangle/\mathfrak{a}\langle t_i\rangle = A\langle t_i\rangle$, then we can use(5.6.0.13) to construct a pd-structure on $A\langle t_i\rangle$ compatible with that of A.

The verification of universal property is omitted. □

PD-Envelopes

Prop. (5.6.0.15)[PD-Envelope]. Let (A, I, γ) be a pd-structure, then there is a **pd-envelope** functor $(B, J) \to (D_B(J), \overline{J}, \overline{\delta})$ from the the category of pairs over (A, I) to the category of pd-structures over (A, I, γ) that is left adjoint to the forgetful functor.

In particular, by the universal property of pd-envelope, there is a morphism $(B, J) \to (D_B(J), \overline{J}) \to (B/J, 0)$ of pairs, so in particular $D/\overline{J} \to B/J$ is surjective. ⌟

Proof: We use adjoint functor theorem(4.1.1.34), the forgetful functor preserves limit by(5.6.0.2), and it satisfies the set-theoretical condition: for any pair (B, J) over (A, I) and a morphism $\psi : (B, J) \to (C, K)$ over (A, I) where $\varphi : (A, I, \gamma) \to (C, K, \delta)$ is a pd-morphism, then we can consider the subring $C' \subset C$ generated by all $\varphi(A), \psi(B)$ and $\delta_m(J)$, and $K' \subset K \cap C'$ the ideal of C' generated by $\varphi(I), \delta_n(\psi(J))$, then $|C'| < |A| \otimes |B|^{\aleph_0}$ and its type is bounded by a cardinal, so does (C, I). □

Prop. (5.6.0.16) [PD-Envelope of Quotients]. Let (A, I, γ) be a pd-structure and $\varphi : B' \to B$ be a surjection of A-algebras with kernel K. Let $IB \subset J \subset B$ an ideal and $J' = \varphi^{-1}(J)$ and $D_{B',\gamma}(J') = (D', \overline{J}', \overline{\gamma})$, then $D_{B,\gamma}(J) = (D'/K', \overline{J}'/K', \overline{\gamma})$ where K' is the ideal generated by all $\overline{\gamma}_n(k)$ for $n \geq 0$ and $k \in K$. ⌟

Proof: There is a pd-structure on $(D'/K', \overline{J}'/K', \overline{\gamma})$ by(5.6.0.13). A map of pais $(B, J) \to (T, I', \gamma)$ is equivalent to a map of pairs $(B', J') \to (T, I', \gamma)$ that vanishes on K, or a map of pd-structures $(D', \overline{J}', \overline{\gamma}) \to (T, I', \gamma)$ that vanishes on $\gamma_n(K)$, thus this is clearly represented by $(D'/K', \overline{J}'/K', \overline{\gamma})$. □

Prop. (5.6.0.17). If (A, I) is a pd-structure and (B, J) is a pair over (A, I), then

$$D_{B[X_i],\gamma}(JB[X_i] + (X_i)) \cong D_{B,\gamma}(J)\langle X_i\rangle$$

⌟

Proof: This follows from the universal property of free pd-structure(5.6.0.14). □

PD-Structures and δ-Rings

Lemma (5.6.0.18). If A is a p-torsionfree $\mathbb{Z}_{(p)}$-δ-ring, denote $\gamma_n(z) = \frac{z^n}{n!}$. If $z \in A$ satisfies $\gamma_p(z) \in A$, then $\gamma_n(z) \in A$ for any n. ⌟

Proof: WARNING: this is not an easy consequence of power counting. We first prove for $n = p^2$: as A is a δ-ring, $\delta(\frac{z^p}{p}) \in A$

$$\delta(\frac{z^p}{p}) = \frac{1}{p}(\frac{\varphi(z)^p}{p} - \frac{z^{p^2}}{p^p}) = \frac{(z^p + p\delta(z))^p}{p^2} - \frac{z^{p^2}}{p^{p+1}} \in A.$$

The first term is in A by assumption, thus the second term is also in A, proving the case for $n = p^2$.

Now for general n, it suffices to prove for $n = kp$. But it can be checked that $\gamma_{nk}(z) = u\gamma_k(\gamma_p(z))$ where u is a unit. Now by what we just proved, we can use induction hypothesis for $z = \gamma_p(z)$, and conclude that $\gamma_{nk}(z) \in A$. □

Prop. (5.6.0.19). The ring $C = \mathbb{Z}_{(p)}\{x, \frac{\varphi(x)}{p}\}$(5.5.4.10) identifies with the pd-envelope $D = D_{\mathbb{Z}_{(p)}\{x\}}(x) = \mathbb{Z}_{(p)}\{x\}[\{\gamma_n(x)\}]$ where $\gamma_n(x) = \frac{x^n}{n!}$. Moreover, it also equals to $\mathbb{Z}_{(p)}[X_1, X_2, \ldots]/(pX_1 - x^p, pX_2 - X_1^p, \ldots)$. ⌟

Proof: It suffices to show that the smallest δ-ring of $\mathbb{Z}_{(p)}\{x\}[\frac{1}{p}]$ containing $\mathbb{Z}_{(p)}\{x\}$ and $\frac{\varphi(x)}{p}$ is the same as the smallest ring of $\mathbb{Z}_{(p)}\{x\}[\frac{1}{p}]$ containing $\mathbb{Z}_{(p)}\{x\}$ and $\frac{\varphi(x)}{n!}$.

$D \subset C$ is immediate from(5.6.0.18). To show $C \subset D$, notice $\frac{x^p}{p} \in D$, it suffices to show φ preserves D, or equivalently, $\varphi(y) - y^n \in pD$ for any $y \in D$. Now

$$\varphi(\frac{x^n}{n!}) = \frac{(x^p + p\delta(x))^n}{n!} = \frac{\sum_{i=0}^n \binom{n}{i}(pi)!p^{n-i}\frac{x^{pi}}{(pi)!}\delta(x)^{n-i}}{n!}$$

The coefficients

$$\frac{\binom{n}{i}(pi)!p^{n-i}}{n!}$$

are all in $p\mathbb{Z}_{(p)}$, thus $\varphi(\frac{x^n}{n!}) \in pD$. On the other hand,

$$(\frac{x^n}{n!})^p = \gamma_p(\gamma_n(x)) = u\gamma_{pn}(x) \cdot p! \in pD$$

where u is a unit in $\mathbb{Z}_{(p)}$ by(5.6.0.1), thus we are done. □

Lemma (5.6.0.20). If A is a p-torsionfree (equivalently, flat) $\mathbb{Z}_{(p)}$-algebra and (a, p) is a regular sequence in A, then $D_A((a)) \cong A \otimes_{\mathbb{Z}_{(p)}\{x\}} D_{\mathbb{Z}_{(p)}}((x)) = A[X_1, X_2, \ldots]/(pX_1 - a^p, pX_2 - X_1^p, \ldots)$. ⌟

Proof: By(5.6.0.19),

$$A \otimes_{\mathbb{Z}_{(p)}\{x\}} D_{\mathbb{Z}_{(p)}}((x)) = A \otimes_{\mathbb{Z}_{(p)}\{x\}} [\{\gamma_n(x)\}] = A[X_1, X_2, \ldots]/(a^p - pX_1, X_1^p - pX_2, X_2^p - pX_3, \ldots)$$

thus there is a natural map from $A \otimes_{\mathbb{Z}_{(p)}\{x\}} D_{\mathbb{Z}_{(p)}}((x))$ to $D_A((a))$ given by

$$X_k \mapsto \frac{a^{p^k}}{p^{\mathrm{ord}_p(n!)}} = \frac{a^{p^k}}{p^{1+p+\ldots+p^{k-1}}} \in D_A((a)).$$

It is surjective, and it is an isomorphism when inverting p. Thus the kernel are all p^∞-torsions. Then to show it is an isomorphism, it suffices to show $A[X_1, X_2, \ldots]/(a^p - pX_1, X_1^p - pX_2, X_2^p - pX_3, \ldots)$ is p-torsion-free. It is a filtered colimit, so it suffices to show $A[X_1, \ldots, X_n]/(a^p - pX_1, X_1^p - pX_2, \ldots, X_{n-1}^p - pX_n)$ is p-torsionfree.

For this, it suffices to prove $A' = A[X_1, \ldots, X_k]/(px_1 - a^k, px_2 - x_1^k, \ldots, px_k - x_{k-1}^p)$ is p-torsion-free. If we denote $K(R) = K(R[X_1, \ldots, X_n], px_1 - a^k, px_2 - x_1^k, \ldots, px_k - x_{k-1}^p)$ for any ring R, then we have a distinguished triangle

$$K(A) \xrightarrow{p} K(A) \to K(Kos(A[X_1, \ldots, X_k], p)) = K(A/p)$$

as A is p-torsionfree. Now we can consider the spectral sequence associated to this distinguished triangle. Notice first that $(px_1 - a^k, px_2 - x_1^k, \ldots, px_k - x_{k-1}^p)$ is a regular sequence in A'/p, which is clear. So the E_1 page looks like

$$\begin{array}{ccccc}
A' & \xrightarrow{p} & A' & \longrightarrow & A'/p \\
\uparrow & & \uparrow & & \uparrow \\
* & \longrightarrow & * & \longrightarrow & 0 \\
\uparrow & & \uparrow & & \uparrow \\
* & \longrightarrow & * & \longrightarrow & 0 \\
\uparrow & & \uparrow & & \uparrow \\
\cdots & \longrightarrow & \cdots & \longrightarrow & \cdots
\end{array}$$

and the E_2 page is of the form

$$\begin{array}{ccccc} A'[p] & \xrightarrow{p} & 0 & \longrightarrow & 0 \\ \uparrow & & \uparrow & & \uparrow \\ * & \longrightarrow & * & \longrightarrow & 0 \\ \uparrow & & \uparrow & & \uparrow \\ * & \longrightarrow & * & \longrightarrow & 0 \\ \uparrow & & \uparrow & & \uparrow \\ \dots & \longrightarrow & \dots & \longrightarrow & \dots \end{array}$$

This spectral sequence converges to 0, so $A'[p] = 0$, we win. □

Prop. (5.6.0.21) [PD-Envelope for Regular Sequence]. Let A be a p-torsionfree δ-ring and $p, f_1, \dots, f_r$ define a regular sequence in A, then $A\{\frac{\varphi(f_1)}{p}, \dots, \frac{\varphi(f_r)}{p}\}$ identifies with the pd-envelope $D_A(I)$ of $I = (f_1, \dots, f_r)$ as a subring of $A[\frac{1}{p}]$. ⌟

Proof: In case $r = 1$, $A\{\frac{\varphi(f_1)}{p}\} = A \otimes_{\mathbb{Z}_{(p)}\{x\}} \mathbb{Z}_{(p)}\{x, \frac{\varphi(x)}{p}\} = A \otimes_{\mathbb{Z}_{(p)}\{x\}} D_{\mathbb{Z}_{(p)}}((x)) \cong D_A((f_1))$ by(5.6.0.20).

The general case follows from this, by considering the tower

$$\begin{aligned}(A, (f_1)) \to (D_A(f_1), (f_2)) &= (A\{\frac{\varphi(f_1)}{p}\}, (f_2)) \\ \to (D_{A\{\frac{\varphi(f_1)}{p}\}}(f_2), (f_3)) &= (A\{\frac{\varphi(f_1)}{p}, \frac{\varphi(f_2)}{p}\}, (f_3)) \\ \to \dots &= A\{\frac{\varphi(f_1)}{p}, \dots, \frac{\varphi(f_r)}{p}\}\end{aligned}$$

The equations are true because (p, f_k) are regular in $A\{\frac{\varphi(f_1)}{p}, \dots, \frac{\varphi(f_{k-1})}{p}\}$:

$$\begin{aligned}A\{\frac{\varphi(f_1)}{p}, \dots, \frac{\varphi(f_{k-1})}{p}\}/p =& A/p[X_{11}, X_{12}, \dots, X_{21}, X_{22}, \dots, \dots, X_{k-1,1}, X_{k-1,2}, \dots]/ \\ & (f_1^p, f_2^p, \dots, f_{k-1}^p, X_{11}^p, X_{12}^p, \dots, X_{21}^p, X_{22}^p, \dots, \dots, X_{k-1,1}^p, X_{k-1,2}^p, \dots)\end{aligned}$$

and f_k is a nonzero-divisor in it because it is a non-zero divisor in $A/(p, f_1^p, \dots, f_{k-1}^p)$, as $(p, f_1^p, \dots, f_k^p)$ is also a regular sequence by(5.3.4.4). then a map of pairs of rings $(A, I) \to (C, J)$ will lift through this tower uniquely by the universal property of pd-envelop.

then we see $A\{\frac{\varphi(f_1)}{p}, \dots, \frac{\varphi(f_r)}{p}\}$ is just the pd-envelop of (A, I), by the universal property. □

Lemma (5.6.0.22). Let A be an $\mathbb{F}_p$-algebra and B an A-algebra. If $(x_1, \dots, x_n) \in B$ is regular w.r.t. A(5.8.3.7), then $D_B((x_1, \dots, x_n))$ is A-flat. ⌟

Proof: By(5.6.0.19) and base change, it is clear that $D_B(I)$ is a free B/I^p-algebra. Thus we need to show that B/I^p is a flat A-module. And this is true as the sequence $x_1^p, \dots, x_n^p$ is also regular w.r.t. A(5.8.3.8). □

Prop. (5.6.0.23) [Flatness of PD-Envelope]. If $A \to B$ is a map of simplicial rings, A is naturally a simplicial pd-structure with $I_\bullet = pA_\bullet$, and B is p-completely flat over A(5.8.3.5), and $(x_1, \dots, x_n) \in \pi_0(B)$ is p-completely regular w.r.t A(5.8.3.7), then the completed pd-envelope $D = D_B((x_1, \dots, x_n))^\wedge$ is p-completely flat over A. ⌟

Proof: By definition(5.8.3.5), to check it is p-completely flat, it suffices to check

$$Kos(A,p) \to Kos(A,p) \otimes^L_A D$$

is flat. and by(5.8.3.4) it suffices to check that

$$\pi_0(Kos(A,p)) \to \pi_0(Kos(A,p)) \otimes^L_A D$$

is flat. The formation of pd-envelope commutes with derived base change by universal property, and tensor with A/p-algebra undoes the completions, so we are reduced to the the case $A' = \pi_0(Kos(A,p))$ and $B' = A' \otimes^L_A B$ is flat over A' and to show that

$$A' \to D_{B'}((x_1,\dots,x_n))$$

is flat. Notice B' is a discrete flat A'-algebra by definition(5.8.3.5), and $(x_1,\dots,x_n)$ is a sequence in B' that $Kos(B,x_1,\dots,x_n)$ is a sequence regular w.r.t. A':

$$\begin{aligned} Kos(B,x_1,\dots,x_n) &= Kos(B' = A' \otimes^L_A B, x_1,\dots,x_n) = A' \otimes^L_A Kos(B,x_1,\dots,x_n) \\ &= A' \otimes^L_{Kos(A,p)} Kos(A,p) \otimes_A Kos(B,x_1,\dots,x_n) \\ &= A' \otimes^L_{Kos(A,p)} Kos(B,p,x_1,\dots,x_n) \end{aligned}$$

is flat because $Kos(A,p) \to Kos(B,p,x_1,\dots,x_n)$ does by definition(5.8.3.7) and(5.8.3.3). So we are done by(5.6.0.22). □

Cor. (5.6.0.24). If A is a p-complete simplicial δ-ring and B is a p-completely flat simplicial δ-A-algebra, and if $x_1,\dots,x_r \in \pi_0(B)$ is p-completely regular w.r.t. A, then

$$C_\bullet = B_\bullet\{\frac{x_1}{p},\dots,\frac{x_r}{p}\}$$

is p-completely flat over A. ⌟

Proof: Let $C'_\bullet = B_\bullet\{\frac{\varphi(x_1)}{p},\dots,\frac{\varphi(x_r)}{p}\}^\wedge$, then $C'_\bullet$ is p-completely flat over A, by(5.6.0.21)(**?** why B is p-torsionfree and $(p,x_1,\dots,x_n)$ is regular sequence) and(5.6.0.23). Now there is a commutative diagram

$$\begin{array}{ccccccccc} A & \longrightarrow & A\{x_1,\dots,x_r\} & \longrightarrow & B & \longrightarrow & B\{\frac{x_1}{p},\dots,\frac{x_r}{p}\} & \longrightarrow & C_\bullet \\ \| & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\psi_B} & & \downarrow{\scriptstyle\psi'} & & \downarrow{\scriptstyle\psi_C} \\ A & \longrightarrow & A\{\varphi(x_1),\dots,\varphi(x_r)\} & \longrightarrow & B' & \longrightarrow & B'\{\frac{\varphi(x_1)}{p},\dots,\frac{\varphi(x_r)}{p}\} & \longrightarrow & C'_\bullet \end{array}$$

where ψ is the relative Frobenius and ψ_B,ψ_C is the derived base change and completed derived base change. Then ψ is f.f. as it is the base change of the Frobenius on the free δ-ring $\mathbb{Z}\{x_1,\dots,x_r\}$(5.5.4.10), thus so does ψ'. Then ψ_C is p-completely flat, because it is the completion(use(5.9.7.2)(5.9.7.4)). Now the conclusion follows, by completely f.f. descent(5.9.7.2). □

1 de Rham Complex

Def. (5.6.1.1) [PD-Differentials]. Let B be an A-algebra and (B,J,δ) be a pd-structure and M a B-module, then a **pd-A-derivation** from B to M is a an element θ of $\mathrm{Der}_A(B,M)$ that $\theta(\delta_n(x)) = \delta_{n-1}(x)\theta(x)$ for $n \geq 1$ and $x \in J$.

As in(5.4.3.4), there is a **pd-differential** $\Omega_{B/A,\delta}$ that

$$\mathrm{Hom}_B(\Omega_{B/A,\delta}, M)$$

is isomorphic to the set of pd-A-derivations of B to M, functorially in M. ⌟

Prop. (5.6.1.2) [PD-Differential of PD-Envelope]. Let (A, I, γ) be a pd-structure and (B, J) be a pair over (A, I), and let $D_{B/A,\gamma}(J) = (D, \overline{J}, \overline{\gamma})$ be the pd-envelope, then $\Omega_{D/A,\overline{\gamma}} = \Omega_{B/A} \otimes_B D$. ⌟

Proof: It suffices to show that for any D-module M, the set of A-derivations $B \to M$ is isomorphic to the set of pd-A-derivations $D \to M$.

Let $D \otimes M$ be the ring that $M^2 = 0$ and a pd-structure on $\overline{J} \oplus M$ is given by $\delta_n(x+m) = \delta_n(x) + \delta_{n-1}(x)m$. Then a pd-$A$-derivations $D \to M$ is equivalent to a pd-ring map $(D, \overline{J}) \to (D \oplus M, \overline{J} \oplus M)$, and an A-derivations $B \to M$ is also equivalent to a map of pairs $(B, J) \to (D \oplus M, \overline{J} \oplus M)$, thus we are done by the universal property of D. □

Prop. (5.6.1.3). Let B be an A-algebra and (B, J, δ) be a pd-structure, then

- if $(B[X], JB[X], \delta')$ is the δ-structure extended from that of (B, J, δ) as in(5.6.0.11), then
$$\Omega_{B[X]/A,\delta'} = \Omega_{B/A,\delta} \otimes_B B[X] \oplus B[X]dx.$$
- Let $B\langle x\rangle$ be the free pd-algebra over B(5.6.0.14), then
$$\Omega_{B\langle x\rangle/A,\delta'} = \Omega_{B/A,\delta} \otimes_B B\langle x\rangle \oplus B\langle x\rangle dx.$$
- Let $K \subset J$ be an ideal preserved by δ and then consider the quotient $(B' = B/K, \overline{J} = J/K, \overline{\delta})$, then $\Omega_{B'/A,\overline{\delta}}$ is quotient of the module $\Omega_{B/A,\overline{\delta}} \otimes_B B'$ by the B'-submodule generated by dk where $k \in K$.

⌟

Proof: These are all somewhat trivial. □

Prop. (5.6.1.4) [PD-Differential and Completion]. Let A be a $\mathbb{Z}_{(p)}$-algebra, B be an A-algebra and (B, J, δ) be a pd-structure and p is nilpotent in B/J, then

$$\lim_e \Omega_{B_e/A,\overline{\delta}} = (\Omega_{B/A,\delta})^\wedge = (\Omega_{\widehat{B}/A,\widehat{\delta}})^\wedge.$$

where $B_e = B/p^e$. ⌟

Proof: By(5.6.0.12), the terms make sense. Now by(5.6.1.3) and the observation $d(p^e) = 0$, we have $\Omega_{B_e/A,\overline{\delta}} = \Omega_{B/A,\delta}/p^e = \Omega_{\widetilde{B}/A,\widetilde{\delta}}/p^e$, thus we are done. □

Def. (5.6.1.5) [PD-de Rham Complex]. Let $\Omega^i_{B/A,\delta} = \wedge^i \Omega_{B/A,\delta}$, then the surjection $\Omega_{B/A} \to \Omega_{B/A,\delta}$ satisfies the condition of(8.2.1.2), thus there is a **pd-de Rham complex** $\Omega^\bullet_{B/A,\delta}$. ⌟

PD-Poincaré Lemma

Lemma (5.6.1.6) [PD-Poincaré Lemma]. Let A be a ring, $P = A\langle X_i\rangle$ is the free PD-algebra over A, then for any A-module, the complex

$$0 \to M \to M \otimes_A P \to M \otimes_A \Omega^\wedge_{P/A,\delta} \to \ldots$$

is exact. And if $D = \widehat{P}$ and let $\Omega^n_D = \Omega^n_{P/A,\delta}$, then for any p-complete A-module M, the complex

$$0 \to M \to M \widehat{\otimes}_A P \to M \widehat{\otimes}_A \Omega^\wedge_{P/A,\delta} \to \ldots$$

is exact. ⌟

Proof: It suffices to show that $0 \to M \to M \otimes_A P \to M \otimes_A \Omega^1_{P/A,\delta} \to \ldots$ is homotopic to 0. For this, notice every element of $\Omega^n_{P/A,\delta}$ is of the form $\sum P \prod_{j=0}^n dx_{i_0} dx_{i_1} \ldots dx_{i_n}$, so we can let

$$f(\omega) = f(\gamma_{n_{i_0}}(x_{i_0}) dx_{i_0} \wedge \omega) = \gamma_{n_{i_0}+1}(x_{i_0})\omega$$

where ω doesn't divides dx_k for $k < i_0$. Then it can be checked that $df + fd = \mathrm{id}$, so we are done. □

Prop. (5.6.1.7). If A is a ring and (B, J, δ) is a is a pd-structure, and let $P = B\langle X_i \rangle$ be the free pd-structure(5.6.0.14). Let M be a B-module endowed with an integrable connection $\nabla : M \to M \otimes_B \Omega^1_{B/A,\delta}$, then the map of de Rham complexes

$$M \otimes_B \Omega^*_{B/A,\delta} \to M \otimes_B \Omega^*_{P/A,\delta}$$

is a quasi-isomorphism. And if we denote D, D' the p-adic completions of B, P, and $\Omega_D, \Omega_{D'}$ the p-adic completion of $\Omega_{B/A,\delta}, \Omega_{P/A,\delta}$, and M is a p-complete B-module endowed with an integrable connection $\nabla : M \to M \otimes_D \Omega_D$, then the map of de Rham complexes

$$M \otimes_D \Omega^*_D \to M \otimes_{D'} \Omega^*_{D'}$$

is a quasi-isomorphism. ⌟

Proof: Consider the filtration F^* on $\Omega^\bullet_{B/A,\delta}$ given by the stupid truncation $\sigma_{\geq i}\Omega^\bullet_{B/A,\delta}$, and consider the filtration on $\Omega^\bullet_{P/A,\delta}$ given by

$$F^*(\Omega^\bullet_{P/A,\delta}) = F^*(\Omega^\bullet_{B/A,\delta}) \wedge \Omega^\bullet_{P/A,\delta}.$$

Notice that we have a split exact sequence

$$0 \to \Omega^1_{B/A,\delta} \otimes_B P \to \Omega^1_{P/A,\delta} \to \Omega^1_{P/B,\delta} \to 0$$

and $\Omega^1_{P/B,\delta}$ is free on X_i over B(pondering the universal property, this is for the same reason as(5.4.3.7).

Then we see that $F^i(\Omega^\bullet_{P/A,\delta}) \to \Omega^\bullet_{P/A,\delta}$ is termwise split injection for any i, and the graded is $\Omega^i_{B/A,\delta} \otimes_B \Omega^\bullet_{P/B,\delta}$. Thus if we let $F^i(M \otimes_B \Omega^\bullet_{P/A,\delta}) = M \otimes F^i(\Omega^\bullet_{P/A,\delta})$, then the graded is $M \otimes_B \Omega^i_{B/A,\delta} \otimes_B \Omega^\bullet_{P/B,\delta}$, which is quasi-isomorphic to $M \otimes_B \Omega^i_{B/A,\delta}$ by(5.6.1.6). Then the original map is a filtered complexes that induces quasi-isomorphism on gradeds, so it induces a quasi-isomorphism, because it induces an morphism between two convergent spectral sequences, by(4.10.7.6) and(4.10.7.5). □

5.7 Almost Ring Theory

References are [Almost Ring Theory Gabber/Ramero] and [Almost Ring Theory Foundations Gabber/Ramero].

Def. (5.7.0.1). The setup of most mathematics is an flat ideal $I \subset R$, that $I^2 = I$. This implies that $I \otimes I \cong I^2 = I$.

Denote $i : R \to R/I$. Then there is a map $i_* : M \mapsto M_R$, which has a left adjoint $i^* : N \mapsto N \otimes_R R/I$, and a right adjoint $i^! : N \mapsto \mathrm{Hom}(R/I, N)$. ┘

1 Homological Theory

Almost Modules

Prop. (5.7.1.1) [Examples].

- If K is a perfectoid field, $R = K^0, I = K^{00}$, then I is flat over R, because if π is a pseudo-uniformizer of K(11.2.8.9), then $I = (\pi^{\frac{1}{p^\infty}})$, which is a colimit of free modules thus flat, and $I^2 = I$ clearly.
- Let R be a ring and f is an arbitrary element with compatible p^n-th roots, let $I = (f^{\frac{1}{p^\infty}})$, then $I^2 = I$. To show I is flat, consider:

$$M_0 \xrightarrow{f^{1-\frac{1}{p}}} M_1 \xrightarrow{f^{\frac{1}{p}-\frac{1}{p^2}}} M_2 \to \ldots \to M_n \xrightarrow{\frac{1}{p^n}-\frac{1}{p^{n+1}}} M_{n+1} \to \ldots$$

where $M_i \cong R$, and $M = \mathrm{colim}\, M_i$, then M is flat, and there is a map $M \to I : 1 \in M_n \to f^{\frac{1}{p^n}}$, then this map is surjective, and it is injective: if α maps to 0, then $\alpha f^{\frac{1}{p^n}} = 0$, so $\alpha^{p^m} f = 0$ for all $m \geq n$, and by perfectness of R, $\alpha f^{\frac{1}{p^m}} = 0$, so in particular, $\alpha = 0 \in M_{n+1}$.

┘

Prop. (5.7.1.2)[The Category of Almost R-Modules in disguise]. Let $\mathcal{A} \subset \mathrm{Mod}_R$ be the category of all R-modules M that the action $I \otimes M \to M$ is an isomorphism(By $I \otimes I = I$ this is equivalent to $M = I \otimes N$ for some N) then:

- The inclusion $j_! : \mathcal{A} \to \mathrm{Mod}_R$ is exact, i.e. the cokernel, kernel of objects in $\mathcal{A}$ are also in $\mathcal{A}$.
- $j_!$ has a right adjoint $j^* : M \mapsto I \otimes M$, and the unit map $N \to j^* j_! N$ is an isomorphism on $\mathcal{A}$.
- j^* has its right adjoint $j_*(M) = \mathrm{Hom}(I, M)$, and the counit $j^* j_* M \to M$ is an isomorphism on $\mathcal{A}$.

┘

Proof: 1: an easy consequence of five-lemma.

2: We need to show for $N \in \mathcal{A}$, $\mathrm{Hom}(N, I \otimes M) \cong \mathrm{Hom}(N, M)$. Notice there is a distinguished triangle

$$I \otimes M \to M \to M \otimes R/I,$$

as $- \otimes_R^L M$ is a derived functor and I is flat. So it suffices to show

$$R\,\mathrm{Hom}_R(N, M \otimes_R^L R/I) = 0 = R\,\mathrm{Hom}_{R/I}(N \otimes_R^L R/I, M \otimes_R^L R/I).$$

And in fact $N \otimes_R^L R/I = 0$, because $N \otimes_R^L R/I = N \otimes_R^L I \otimes_R^L R/I$, and $I \otimes_R^L R/I = I \otimes_R R/I = I/I^2 = 0$ by flatness and hypothesis.

$N \cong j^*j_!N$ is an easy consequence of $I\otimes I = I$.

3: The adjointness is just Tor-Hom-adjunction, and for the isomorphism $I\otimes \mathrm{Hom}(I,M)\cong M$, as I is flat, it suffices to prove the stronger result that $I\otimes^L_R R\,\mathrm{Hom}(I,M) = M[0]$. As there is an exact triangle

$$R\,\mathrm{Hom}(R/I,M)\to M\to R\,\mathrm{Hom}(I,M),$$

so it suffices to show $I\otimes^L R\,\mathrm{Hom}(R/I,M) = 0$, because $I\otimes^L M = M$. But this is because $I\otimes^L R\,\mathrm{Hom}(R/I,M) = I\otimes^L R/I\otimes^L R\,\mathrm{Hom}(R/I,M)$, and $I\otimes^L R/I = 0$ as before. □

Prop. (5.7.1.3) [Category of Almost R-modules].

- The image of the functor $i_*:\mathrm{Mod}_{R/I}\to \mathrm{Mod}_R$ is a Serre subcategory of Mod_R, so the quotient $\mathrm{Mod}^a_R = \mathrm{Mod}_R/\mathrm{Mod}_{R/I}$ exists by(4.8.3.14),
- The quotient $q:\mathrm{Mod}_R\to\mathrm{Mod}^a_R$ admits fully faithful left and right adjoints. In particular, q preserves all limits and colimits.
- The image of i is a 'tensor ideal' of Mod_R, so the quotient Mod^a_R inherits a natural symmetric monoidal $\otimes$-product structure.
- There is a functor $\mathrm{alHom}:(\mathrm{Mod}^a_R)^{op}\times\mathrm{Mod}^a_R\to\mathrm{Mod}^a_R:(X,Y)\to\mathrm{alHom}(X,Y)$ that $\mathrm{alHom}(X,-)$ is right adjoint to $-\otimes X$:

$$\mathrm{Hom}(Z\otimes X,Y)\cong\mathrm{Hom}(Z,\mathrm{alHom}(X,Y)).$$

⌟

Proof: 1: the image of i_* is just the category of modules killed by I, if M is killed by I, then subobjects and quotients of M is killed by I, and if M is an extension of two elements killed by I, then $IM = I^2M = 0$.

2: In fact we show that the category $\mathcal{A}$ in(5.7.1.2) and the functor j^* is just equivalent to Mod^a_R: First: $j^*(\mathrm{Mod}_{R/I}) = 0$, because $I\otimes M = I\otimes_R R/I\otimes_{R/I} M = I/I^2\otimes_{R/I} M = 0$ as $I = I^2$, and j^* is exact because I is flat.

And for any R-module M, consider $I\otimes M\to M$, it has kernels and cokernels, then tensoring I, it becomes $I\otimes M\to I\otimes M$(5.7.0.1). as I is flat, the kernel and cokernels are killed by I, so for any functor q to another category that kills $\mathrm{Mod}_{R/I}$, $q(M) = q(I\otimes M) = qj_!j^*(M)$, so q factors through M, uniquely, as j^* is surjective.

Now the left/right adjoints exist by(5.7.1.2).

3: if $IM = 0$, then $IM\otimes N = 0$, so the tensor products pass to the quotient, and j^* is a map between symmetric monoidal categories.

4: alHom is defined by $\mathrm{alHom}(j^*M,j^*N) = j^*(\mathrm{Hom}(M,N)) = \mathrm{Hom}(M,N)^a$. This is well defined, because if $IM = 0$ or $IN = 1$, then $I\,\mathrm{Hom}(M,N) = 0$. □

Cor. (5.7.1.4).

- $i^*j_! = 0$.
- $i^!j_* = 0$.
- $j^*i_* = 0$, and the kernel of j^* is just $i_*(\mathrm{Mod}_{R/I})$.

⌟

Proof: 1: $R/I\otimes I\otimes M = 0$, because $I\otimes R/I = 0$.

2: $\mathrm{Hom}(R/I,\mathrm{Hom}(I,M)) = 0$, because $I\otimes R/I = 0$.

3: This is by 2 of the proposition(5.7.1.3). □

Remark (5.7.1.5). The construction above can be summarized as the following diagram:

$$\mathrm{Mod}_{R/I} \underset{\xleftarrow{i^!}}{\overset{\xleftarrow{i^*}}{\xrightarrow{i_*}}} \mathrm{Mod}_R \underset{\xleftarrow{j_*}}{\overset{\xleftarrow{j_!}}{\xrightarrow{j^*}}} \mathrm{Mod}_R^a$$

with four adjoint pair and three vanishing. This should be seen as an analogy of the case of topology: X is a space and $i : U \to X$ is open in X, and $j : Z \to X$ is closed, $Z = X - U$, then the defined sheaf operations are the same as written above.

However, one should not consider Mod_R^a as the sheaf of modules on the open subscheme $\mathrm{Spec}\, R_f$ for some pseudo uniformizer, because the map $M \to M \otimes R_f$ factors through Mod_R^a as it vanishes on $\mathrm{Mod}_{R/I}$, but it is not $\mathrm{Mod}_{R/I}^a$. For example, if k is a perfect field, and consider $R = k[t^{\frac{1}{p^\infty}}]$, then the module $M = R/(t)$ is also killed by $\otimes R_f$, but it is not killed by I.

Then one may consider it is the category of Qco sheaves on $D(I)$, but first this is not an affine scheme, and second this is false, anyway. And we should imagine an non-existent open subscheme $\overline{U}$ bigger than U, as it contains any affine opens of U. ⌟

Remark (5.7.1.6). Notice j^* is both left exact and right exact, so it preserves both arbitrary limits and colimits, so almostification nearly loses anything. In particular, the category Mod_R^a has all colimits and limits. ⌟

Def. (5.7.1.7) [Almost Commutative Algebras]. As Mod_R^a has a symmetric monoidal structure, it is possible to define the category of **almost commutative algebras** as the category of commutative unitary monids in Mod_R^a, denoted by $CAlg(\mathrm{Mod}_R^a)$. Notice that its unit object is $I = R^a$.

There is an obvious map

$$(-)^a : \mathrm{Alg}(\mathrm{Mod}_R) \to \mathrm{Alg}(\mathrm{Mod}_R^a),$$

and yet another functor

$$(-)_* : \mathrm{Alg}(\mathrm{Mod}_R^a) \to \mathrm{Alg}(\mathrm{Mod}_R),$$

because $M \to M_*$ is lax symmetric monoidal, i.e. there are natural map $M_* \otimes N_* \to (M \otimes N)_*$. This is a right adjoint of $(-)^a$, as j^* and j_* is adjoint.

Finally there is a functor

$$(-)_{!!} : \mathrm{Alg}(\mathrm{Mod}_R^a) \to \mathrm{Alg}(\mathrm{Mod}_R),$$

whose construction is a little complicated, first notice the functor $(-)_!$ preserves multiplication but it has no units, so in order to give it a unit, consider the module pushout: $(A_! \oplus V)/I$, which has a natural multiplicative structure that can be made into a R-module, and $(-)_{!!}$ is left adjoint to $(-)^a$,Cf.[Almost Ring Theory P22]. ⌟

Prop. (5.7.1.8). $(-)_{!!}$ preserves faithfully flatness. ⌟

Proof: Cf.[Almost Ring theory P52]**?** □

Def. (5.7.1.9). For an almost commutative algebra A, a **left module** is an almost module $M \subset \mathrm{Mod}_R^a$ that has a left action $A \otimes M \to M$ that has natural commutative diagrams as one expects. And for any R-algebra A, there are natural maps $\mathrm{Mod}_A \to \mathrm{Mod}_{A^a}^a$. ⌟

<u>**Almost Homological Algebra**</u>

2 Almost Commutative Algebra

Def. (5.7.2.1) [Almost Notations]. Given a R-module M, an element $f \in M$ is called **almost zero** if $I \cdot f = 0$, and M is called **almost zero** if all $f \in M$ is almost zero.

Denote

$$M^a = j^* M \in \mathrm{Mod}_R^a, \quad M_* = j_* M^a = \mathrm{Hom}(I, M), \quad M_! = j_! M^a = I \otimes M.$$

Then there are morphisms $M_! \to M \to M_*$, which becomes isomorphisms after almostification. ⌟

Prop. (5.7.2.2). If $I = (f^{\frac{1}{p^\infty}})$, then $M_* = \{x \in M[f^{-1}] | f^{\frac{1}{p^n}} x \in A\}$ for all n. ⌟

Prop. (5.7.2.3). If $M \to N$ is almost surjective maps of K^0-algebras that $M/I \to N/I$ is surjective, then $M \to N$ is surjective. ⌟

Proof: As I is flat over K^0, if $M \to N \to Q \to 0$ is the cokernel, tensoring A/I, as $M/I \to N/I$ is surjective, $Q/IQ = 0$, but Q is almost zero thus $IQ = 0$, so $Q = 0$. □

Def. (5.7.2.4) [Almost Properties]. Something is called **almost XXX** if it is XXX when passed to the category of almost R-modules. For example,

- elements of M_* are called **almost elements** of M.
- M is called **almost flat** iff $M^a \otimes -$ is exact on Mod_R^a, which is equivalent to $Tor_{>0}^R(M, N)$ is almost zero for all N.
- M is called **almost projective** iff $\mathrm{alHom}(M, -)$ is exact on Mod_R^a, which is equivalent to $\mathrm{Ext}_R^{>0}(M, N)$ is almost zero for all N.
  Notice this is not equivalent to projective in Mod_R^a, because R is almost projective, but $\mathrm{Hom}_{R^a}(R^a, M^a) = \mathrm{Hom}(I, M)$ is not exact as I is not projective: $\mathrm{Ext}_{R^a}^1(R^a, R^a) = \mathrm{Ext}_R^1(I, R) = \mathrm{Ext}^2(k, R)$, which is not 0 if R is the valuation ring of a non-spherically complete perfectoid field K, like $\widehat{\overline{\mathbb{Q}_p}}$**?**.
- M is called **almost finitely generated/almost finitely presented** if for any $\varepsilon \in I$, there is a f.g./f.p. $M_\varepsilon \to M$ with N_ε generators that the kernel and cokernel are killed by ε. It is called **uniformly almost finitely generated** iff N_ε is independent of ε.
  Notice this definition doesn't depends on M chosen**?**
- If S is of char$p$, it is called **almost perfect** iff S_* is perfect.

⌟

Prop. (5.7.2.5) [Enough Almost Injectives]. The category mod_R^a has enough injectives. In fact j^*, j_* both preserves injectives, because they has exact left adjoints, so I is injective R-module iff I^a is injective R^a-module, and J is injective R^a-module iff J_* is injective R-module. So to construct an injective resolution in R^a, pass to R-modules using either $(-)_*$ or $(-)_!$ and find an injective resolution, then almostificate it. ⌟

Prop. (5.7.2.6) [Derived Functors of $(-)_*$]. Notice that $\mathrm{Hom}_{R^a}(M^a, N^a) = \mathrm{Hom}_R(I \otimes M, N)$ by adjointness, so using(5.7.2.5),

$$\mathrm{Ext}_{R^a}^k(M^a, N^a) = \mathrm{Ext}_R^k(M_*, N) = \mathrm{Ext}_R^k(M, R\,\mathrm{Hom}(I, N)),$$

then as $M_* = \mathrm{Hom}(I, M)$, the derived functor of $(-)_*$ is just $\mathrm{Ext}^k_R(I, M) = \mathrm{Ext}^k_{R^a}(R^a, M^a)$.

Notice that $\mathrm{Ext}^k_{R^a}(M, N)$ are all almost zero, as $j^a j_* = \mathrm{id}$, and use trivial Grothendieck spectral sequence. ⌟

Prop. (5.7.2.7) [(Example) A Quadratic Extension of a Perfectoid Field]. If $K = \widehat{Q_p[p^{\frac{1}{p^\infty}}]}$ and $L = K(\sqrt{p})$ with $p \neq 2$, then L^0 is a uniformly almost f.p. projective K^0-module. ⌟

Proof: It suffices to find for each n a K^0-module R_n of rank 2 that $R_n \to L^0$ is injective with cokernel annihilated by $p^{\frac{1}{p^n}}$. For this, consider $R_n = K^0 \oplus K^0 p^{\frac{1}{2p^n}}$, then $L^0 = \widehat{\mathrm{colim}_n R_n}$.

Notice that the cokernel of $R_n \to R_{n+1}$ is killed by $p^{\frac{1}{p^n}}$, because

$$p^{\frac{1}{p^n}} \cdot p^{\frac{1}{2p^{n+1}}} = p^{\frac{(p+1)/2}{p^{n+1}}} \cdot p^{\frac{1}{2p^n}} \subset R_n.$$

So by killing one by one, the cokernel of $R_n \to \mathrm{colim}_n R_n$ is killed by any p-power with power larger than $\sum \frac{1}{p^n}$, in particular by $p^{\frac{1}{p^{n-1}}}$. So $\mathrm{colim}_n R_n$ is an extension of R_0 by a cokernel killed by p, so it is also p-adically complete, and $L^0 = \mathrm{colim}_n R_n$. Now Consider $0 \to R_n \to \mathrm{colim}_n R_n \to \mathrm{Coker}$, then $\mathrm{Ext}^n(\mathrm{colim}_n R_n, N) = \mathrm{Ext}^n(\mathrm{Coker}, N)$ is killed by $p^{\frac{1}{p^{n-1}}}$ for all n, so it is killed by I, thus $\mathrm{colim}_n R_n$ is almost projective. □

Completions and Closures

Prop. (5.7.2.8) [prc and Completion]. If A is a ring with a nonzero-divisor f that $A \subset A[f^{-1}]$ is p-root closed(prc), then:

- $\widehat{A} \subset \widehat{A}[f^{-1}]$ is p-root closed.
- If f admits a compatible p-power roots, then $A_* \subset A_*[f^{-1}]$ is p-root closed(where almost mathematics is performed w.r.t $(f^{\frac{1}{p^\infty}})$.

⌟

Proof: We first replace A with its maximal separated quotient $A/(\cap_n f^n A = I)$: f is still non-zero-divisor, because if $fg \in I$, then $fg \in f^n A$ for all n, so $g \in f^{n-1}A$ as f is non-zero-divisor. And it is p-root closed, because if $a^p \in A/I[f^{-1}]$, then $a^p = b + f^{-c}d$ for c integer and $d \in I$. Notice $I = fI = f^c I$ by(5.2.2.16), so $f^{-c}d \in I$ as well, so $a \in A$.

Now A is f-separated, in particular, $A \hookrightarrow \widehat{A}$.

1: If $g \in \widehat{A}[f^{-1}]$ and $g^p \in \widehat{A}$, then $f^N g \in \widehat{A}$ for some N and choose a $m \geq N(p-1)$, then by the density, $g = g_0 + f^m g_1$ for some $g_0 \in A[f^{-1}]$, $g_1 \in \widehat{A}$. Notice $f^N g_0 \in \widehat{A}$, now

$$g^p = g_0^p + p g_0^{p-1} f^m g_1 + \ldots + (f^m g_1)^p,$$

By definition of m, all terms except g_0^p are in $\widehat{A}$, so $g_0^p \in A$, so $g_0 \in A$, and $g \in \widehat{A}$.

2: Use the convention(5.7.2.2), if $g \in A_*[f^{-1}]$ that $g^p \in A_*$, then $f^{\frac{1}{p^n}} g^p \in A$ for all n, so $(f^{\frac{1}{p^{n+1}}} g)^p \in A$, thus $f^{\frac{1}{p^{n+1}}} g \in A$, hence $g \in A_*$. □

Prop. (5.7.2.9) [ic and Completion]. Let A be a ring with a non-zero-divisor f, if $A \subset A[f^{-1}]$ is integrally closed, then:

- $\widehat{A} \subset \widehat{A}[f^{-1}]$ is integrally closed.
- If f admits a compatible p-power roots, then $A_* \subset A_*[f^{-1}]$ is integrally closed(where almost mathematics is performed w.r.t $(f^{\frac{1}{p^\infty}})$.

⌟

Proof: We first replace A with its maximal separated quotient $A/(\cap_n f^n A = I)$: f is still non-zero-divisor and I is f-divisible as in the proof of(5.7.2.8). And it is integrally closed, because if g satisfies a monic polynomial $h(X) \in A/I[f^{-1}][X]$, then choose a lifting, $h(g) \in I[f^{-1}] = I \subset A$, so g is integral over A thus $g \in A$, and $g \in A/I$. Now A is f-separated and $A \hookrightarrow \widehat{A}$.

1: If $g \in \widehat{A}[f^{-1}]$ satisfies a polynomial $H \in \widehat{A}[X]$, then $g = f^{-c}h$ for $h \in \widehat{A}$, and then h satisfies a polynomial $H(f^c x)$, and choose an approximation of coefficients of $H(x)$ and h_0 of h mod f^{cn}, then it is clear that $H(f^c h_0) \in f^{cn}\widehat{A} \cap A = f^{cn}A$, so when dividing back, $g_0 = f^{-c}h_0$ is integral over A thus $g_0 \in A$, thus $h_0 \in f^c A$, and $h \equiv h_0 \mod f^{cn}$, thus $h \in f^c\widehat{A}$, and $g \in A$.

2: Use the convention(5.7.2.2), if $g \in A_*[f^{-1}]$ is integral over A_*, then there are polynomial H that $H(g) = 0$, now if $\varepsilon = f^{\frac{1}{p^k}}$ consider another polynomial $H(x/\varepsilon)$, then its coefficients are all in A, thus εg is integral over A thus $\varepsilon g \in A$, and then $g \in A_*$. □

Prop. (5.7.2.10) [tic and Completion]. Let A be a ring with a non-zero-divisor f that admits a compatible system of p-power roots $f^{\frac{1}{p^n}}$ for all $n > 0$, and A is totally integrally closed(tic) in $A[f^{-1}]$, then $\widehat{A}$ is totally integrally closed in $\widehat{A}[f^{-1}]$ and $A = A^*$. ⌟

Proof: 1: Notice totally integrally closed is p-root closed, so $\widehat{A} \subset \widehat{A}[f^{-1}]$ is p-root closed. Now if $f^k g^{\mathbb{N}} \subset \widehat{A}$ for some k, then by prc, $f^{\frac{k}{p^n}} g \in \widehat{A}$ for all n, thus g in an almost zero element in $\widehat{A}[f^{-1}]/\widehat{A} \cong A[f^{-1}]/A$, and then g is totally integrally closed over A, because for any n, let $n < p^k$, then $f^{\frac{1}{p^k}} g \in A$, thus $f^{\frac{n}{p^k}} g \in A$, and $f g^n \in A$.

2: Because $f^{\frac{1}{p^k}} A_* \subset A$ by convention(5.7.2.2), clearly A_* is totally integrally closed in A, thus $A_* \subset A$. □

<u>**Almost Étale Map**</u>

Def. (5.7.2.11). A map $A \to B$ of R^a-algebras is called **almost étale** iff:

- B is almost f.p. projective over A.
- (Unramifiedness(5.4.6.10))There exists a diagonal idempotent $e \in (B \otimes_A B)_*$. i.e. $e^2 = e$ and $\mu_*(e) = 1$, and $\ker(\mu)_* \cdot e = 0$, where $\mu : B \otimes_A B \to B$ is the multiplication map.

⌟

Prop. (5.7.2.12) [Example of Almost Étale Maps]. Let $K = \widehat{Q_p[p^{\frac{1}{p^\infty}}]}$ and $L = K(\sqrt{p})$ with $p \neq 2$, then L^0/K^0 is uniformly almost f.p projective K^0-module, by(5.7.2.7). We show it is finite étale: flatness is clear, as L^0/K^0 is torsion-free and K^0 is a valuation ring and use(5.7.3.3).

For unramifiedness, notice that

$$L \otimes_K L \cong L \times L : (a, b) \mapsto (ab, a\sigma(b)).$$

by(3.2.8.6), the diagonal idempotent e is given by

$$e = \frac{1}{2p^{\frac{1}{2p^n}} \otimes 1}(1 \otimes p^{\frac{1}{2p^n}} + p^{\frac{1}{2p^n}} \otimes 1)$$

for any $n \geq 0$, then we see $p^{\frac{1}{p^n}} e \in L^0 \otimes_{K^0} KL^0$ for all n, thus $e \in (L^0 \otimes_{K^0} L^0)_*$. ⌟

Lemma (5.7.2.13) [Lemma for Almost Purity in Characteristic p]. If $\eta : R \to S$ is an integral map of perfect rings. If $\eta[t^{-1}]$ is finite étale for some $t \in R$, then η is almost finite étale w.r.t the ideal $I = (t^{\frac{1}{p^\infty}})$. ⌟

Proof: Firstly, we may assume R, S are both t-torsion-free, because the t-torsion part $R[t^\infty]$ and $S[t^\infty]$ is almost zero: if $t^c\alpha = 0$, then $t^c\alpha^{p^n} = 0$, so $t^{\frac{c}{p^n}}\alpha = 0$. So we reduce to $R/R[t^\infty] \to S/S[t^\infty]$, which doesn't change anything.

Now we reduce to the case that R, S are integrally closed in $R[t^{-1}]$ and $S[t^{-1}]$: it suffices to show that $R_{int} \subset R_*$, thus they are almost isomorphic. For this, an element $f \in R_{int}$ satisfies $f^{\mathbb{N}}t^k \in R$ for some k, so by perfectness, $ft^{\frac{k}{p^n}} \in R$ for all n, so $f \in R_*$.

Now check unramifiedness: let $e \in (S \otimes_R S)[t^{-1}]$ be a diagonal idempotent, then $t^c e \in S \otimes_R S$ for some c, now $e^2 = e$, so easily $e \in (S \otimes_R S)_*$.

Now check almost finite projective: for $m > 0$, represent $t^{\frac{1}{p^m}} e = \sum a_i \otimes b_i \in S \otimes_R S$, then use the map $S \xrightarrow{\alpha} R^n \xrightarrow{\beta} S$ as in(5.4.7.14), then $\beta\alpha = t^{\frac{1}{p^m}}$ on S, as S is t-torsion free, $R^n \to S$ is injective with $t^{\frac{1}{p^m}}$-torsion cokernel, for any m. So S is almost finite projective. □

Prop. (5.7.2.14) [Almost Purity in Characteristic p]. If R is a perfect ring of char$p$, then using the almost mathematics w.r.t. $I = (t^{\frac{1}{p^\infty}})$, $S \to S_*[t^{-1}]$ gives an isomorphism of categories: $R_{af\acute{e}t} \cong R[t^{-1}]_{f\acute{e}t}$. ⌟

Proof: As in the proof of(5.7.2.13), we may assume R is t-torsion-free. Notice that any integral extension of $R[t^{-1}]$ comes from an integral extension of R(choose the integral closure), so the lemma above(5.7.2.13) tells us the functor is essentially surjective.

Now we construct an inverse functor, $S_*[t^{-1}]$ maps to T^a, where T is the integral closure of R in $S_*[t^{-1}]$. By lemma(5.7.2.15) below, S is almost perfect. So S_* is t-torsion-free, as if $t^c f = 0$, then $t^{\frac{c}{p^n}} f = 0$ for all n, so $f = 0 \in (S_*)_* = S_*$. So now $S_* \subset S_*[t^{-1}]$. Clearly T is also perfect and t-torsion-free. So $R \to T$ is an integral extension that is identified with $R[t^{-1}] \to S_*[t^{-1}]$ after inversion of t.

To show that $T^a = S$, it suffices to show $T_* = S_*$. for $f \in T$, $f^{\mathbb{N}}$ spans a finite module of $T[t^{-1}] = S_*[t^{-1}]$, so $t^c f^{\mathbb{N}} \subset S_*$, then by perfectness, $f \in (S_*)_* = S_*$, so $T_* \in S_*$. Conversely, if $g \in S_*$, then $tg^{\mathbb{N}}$ lies in a f.g. R-module of $S_*[t^{-1}]$, by almost f.g.. So $t^c g^{\mathbb{N}} \subset T$, and then by perfectness $g \in T_*$. □

Lemma (5.7.2.15). Almost finite étale map of rings of char$p$ is almost relatively perfect. ⌟

Proof: Cf.[Bhatt notes on Perfectoid Spaces P28]. □

3 Almost Mathematics on Perfectoid Fields

Prop. (5.7.3.1) [Almost Elements]. If K is a perfectoid field, $R = K^0$ and $I = K^{00}$, M is an R-module, then

- If M is torsion-free, then $M_* = \{m \in M \otimes_{K^0} K | Im \in M\} = \{m \in M \otimes_{K^0} K | t^{\frac{1}{p^n}} m \in M\}$,by(11.2.8.12) and(5.7.2.2).
- $I_* = R_* = R$. More generally, for an ideal $J \subset R$, let $c = \sup\{|x| | x \in J\}$, then $J_* = \{a \in K, |a| \le c\}$.

⌟

Prop. (5.7.3.2). Let K be a perfectoid field with a pseudo-uniformizer π. If $\alpha : M \to N$ is an almost surjective map of K^0-algebras that M is π-adically separated and N is π-torsion-free that $\alpha \mod \pi$ is an almost isomorphism, then α is an almost isomorphism. ⌟

Proof: We may replace N with the image of α as to assume α is surjective. Now if $L = \ker \alpha$, then the π-torsion-freeness of N shows L/π is the kernel of ($\alpha \mod \pi$), and L/π is almost zero, thus L is almost π-divisible, but it is also π-separated, thus it is almost zero(using $t^{\sum_i \frac{1}{p^{a_i}}} m \in \cap_n t^n L$). □

Prop. (5.7.3.3) [Almostification and Completeness]. Let K be a perfectoid field with a pseudo uniformizer t and $R = K^0, I = K^{00}$, let $M \in \mathrm{Mod}_R^a$, then:

- M is almost flat iff M_* is R-flat iff $M_!$ is R-flat.
- Assume M is almost flat, then M is t-adically complete iff M_* does.
- Assume M is almost flat, then for each $f \in K^0$, $fM_* \cong (fM)_*$, and $M_*/fM_* \subset (M/fM)_*$. And for any $\varepsilon \in I$, the image of $(M/f\varepsilon M)_*$ and M_*/fM_* in $(M/fM)_*$ are identical.

⌟

Proof: 1: R is a valuation ring, so M_* is R-flat iff $M_*[t]$ is flat by(5.4.1.12), as t is a pseudo uniformizer. As $(-)_*$ is left exact, $M_*[t] = (M[t])_*$, so if M is almost flat, then $M[t] = 0$ as t is nonzero-divisor, so M_* is R-flat. The converse is true as $M = (M_*)^a$, and the tensor is compatible.

For $(-)_!$, this follows from the observation that $(-)_!$ and $(-)^a$ are both exact and commute with tensor products, and notice $M_! \otimes N = (M \otimes N^a)_!$.

2: As $(-)^a$ commutes with all limits and colimits, if M_* is t-adically complete then so does $M = (M_*)^a$. Conversely, if M is R-flat and t-adically complete, then $M_!, M_*$ are also R-flat, and consider the commutative diagram:

$$\begin{array}{ccc} M_! & \xrightarrow{a} & \lim(M/t^nM)_! = \lim M_!/t^nM_! = \widehat{M_!} \\ \downarrow d & & \downarrow b \\ M_* & \xrightarrow{c} & \lim(M/t^nM)_* \end{array}$$

then d is almost isomorphism by(5.7.1.2) and so does b because $(-)^a$ commutes with all limits, and c is an isomorphism as $(-)_*$ commutes with limits and M is t-adically complete. So a is also almost isomorphism.

Now notice $M_!$ is flat hence t-torsion-free, so the kernel of a, d must be 0, with almost zero cokernels. Now(5.2.3.9) shows first $M_!$ is complete and next M_* is complete.

3: Notice $(fM_*)^a = fM$ as $(-)^a$ is exact, so

$$(fM)_* = \mathrm{Hom}(I, fM_*) = \{y \in M_*[t^{-1}] | Iy \subset fM_*\} = f\{y \in M_*[t^{-1}] | Iy \subset M_*\} = fM_*$$

and $M_*/fM_* \subset (M/fM)_*$ follows from the left exactness of $(-)_*$.

For the last assertion, consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{f} & M & \longrightarrow & M/fM & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & M/\varepsilon M & \xrightarrow{f} & M/f\varepsilon M & \longrightarrow & M/fM & \longrightarrow & 0 \end{array}$$

and apply $(-)_* = \mathrm{Hom}_{R^a}(R^a, -)$ and use(5.7.2.6), then

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_*/fM_* & \xrightarrow{a} & (M/fM)_* & \longrightarrow & \mathrm{Ext}^1_{R^a}(R^a, M)[f] & \longrightarrow & 0 \\ & & \downarrow & & \| & & \downarrow c & & \\ 0 & \longrightarrow & (M/f\varepsilon M)_* & \xrightarrow{b} & (M/fM)_* & \longrightarrow & \mathrm{Ext}^1_{R^a}(R^a, M/\varepsilon M) & & \end{array}$$

To show a, b has the same image, it suffices to show that c is injective. For this, it suffices to show $\mathrm{Ext}^1_{R^a}(R^a, M) \to \mathrm{Ext}^1_{R^a}(R^a, M/\varepsilon M)$ is injective. Consider the exact sequence $0 \to M \xrightarrow{\varepsilon} M \to M/\varepsilon M \to 0$, it suffices to show that $\varepsilon\,\mathrm{Ext}^1_{R^a}(R^a, M) = 0$, and this is obvious as $\varepsilon \in I$(5.7.2.6). □

Prop. (5.7.3.4) [General Completeness and Almostification]. More generally, if $J = (f_1, \ldots, f_r) \subset R$ is a f.g. ideal, then an R^a-module M is J-adically complete iff M_* does. ⌟

Proof: Cf.[Perfectoid Spaces Bhatt P32]. □

<u>**Banach Space**</u>

Prop. (5.7.3.5) [Uniform Banach K-Algebra]. If K is a non-Archimedean perfectoid(perfect) field with a pseudo uniformizer t, then the following categories are equivalent:

- The category of uniform Banach K-algebras.
- The category $\mathcal{D}_{tic}$ of t-adically complete and t-torsionfree K^0-algebras A with A totally integrally closed in $A[t^{-1}]$(5.2.1.1).
- The category $\mathcal{D}_{ic}$ of t-adically complete and t-torsionfree K^0-algebras that A is integrally closed in $A[t^{-1}]$ and $A = A_*$.
- The category $\mathcal{D}_{prc}$ of t-adically complete and t-torsionfree K^0-algebras that A is p-root closed in $A[t^{-1}]$ and $A = A_*$.

⌟

Proof: The last three are equivalent, because if $A \in \mathcal{D}_{tic}$, then $A = A_*$ by(5.7.2.10), as K is perfect by(11.2.8.4). So $\mathcal{D}_{tic} \subset \mathcal{D}_{ic} \subset \mathcal{D}_{prc}$, so it suffices to show that $\mathcal{D}_{prc} \subset \mathcal{D}_{tic}$. Now for any f that $f^{\mathbb{N}} \subset t^{-k}A$, then $t^k f^{p^n} \subset A$, and A is p-root closed, so $t^{\frac{k}{p^n}} f \subset A$ for all n, so $f \in A_*$(5.7.2.3), but $A_* = A$.

The equivalence of $1, 2$ is general, by(14.2.4.8). □

Prop. (5.7.3.6). If K is a perfectoid field, then the category of uniform Banach spaces has all colimits and limits. ⌟

Proof: Cf.[Bhatt P38]. □

5.8 Simplicial Commutative Algebras

Main references are [Model Categories and Simplicial Methods, Paul Goerss and Kristen Schemmerhorn], [Simplicial Commutative Rings, Mathew].

1 Simplicial Groups

Prop. (5.8.1.1). A morphism of simplicial groups, when regarded as simplicial set, is a Kan fibration iff

$$X \to \pi_0 X \otimes_{\pi_0(Y)} Y$$

is surjective. In particular, any simplicial group is a Kan complex. ⌟

Proof: Cf.[Simplicial Homology Theory Jardine P12] □

Def. (5.8.1.2) [Simplicial Modules]. A **simplicial module** over a simplicial ring $R_\bullet$ is a map of simplicial map $R_\bullet \times M_\bullet \to M_\bullet$ that is a ring action. ⌟

2 Simplicial R-Modules and Resolutions

Def. (5.8.2.1) [Moore Complex]. Giving a simplicial object in an Abelian category, we can have a **Moore chain complex** with Čech-like differentials. $\partial_n = \sum_1^n (-1)^i d_i$. And we have $\partial^2 = 0$. ⌟

Proof: Should use $d_i d_j = d_{j-1} d_i$ for $i < j$. □

Def. (5.8.2.2) [Normalized Moore complex of a simplicial R-Module]. The **normlized Moore complex** of a simplicial R-module M is the chain complex

$$NM : \cdots \to NM_n \xrightarrow{(-1)^n d_n} NM_{n-1} \to \cdots$$

where $NM_n = \bigcap_{i=0}^{n-1} \ker(d_i) \in M_n$. This is a chain complex because $d_{n-1} d_n = d_{n-1} d_{n-1}$ is 0 on NM_n. In fact NM is preserved by all injections.

The **homotopy groups** $\pi_*(M)$ of M is defined to be the homology of the normalization of M. And it can be shown that as a set $\pi_n(M)$ is just the n-th homotopy group of the geometrization of the

The **degenerate complex** of a Moore complex DM is the chain complex that $D_n = \sum_{i=0}^{n-1} s_i M_{n-1}$ is a sub chain complex of M by the relation of d_i, s_j. ⌟

Def. (5.8.2.3). A morphism of simplicial Abelian groups is called a **weak equivalence** is it induces an isomorphism on the homotopy groups. ⌟

Prop. (5.8.2.4) [Differential Graded Structures]. For any simplicial commutative R-algebra A, the homotopy groups $\pi_*(A)$ form a graded commutative R-ring. ⌟

Proof: The group structure on $\pi_*(A)$ is given by smash products. Cf.[Simplicial Commutative Algebras, Mathew, P2]. □

Cor. (5.8.2.5) [π_0 is an Algebra]. If Y is a simplicial commutative R-algebra, then $\pi_0(Y) = Y_0/(\mathrm{Im}(d_0 - d_1))$, which is an algebra. ⌟

Proof: It suffices to show $\mathrm{Im}(d_0 - d_1)$ is an ideal of Y_0: If $a \in Y_0$, then

$$(d_0 - d_1)(s_0(a)y) = d_0 s_0(a) d_0(y) - d_1 s_0(a) d_1(y) = a(d_0 - d_1)(y).$$

□

Prop. (5.8.2.6). if $R_\bullet$ is a simplicial ring and $M_\bullet$ is a simplicial $R_\bullet$-ring, then $\pi_*(M)$ is a graded $\pi_*(R)$-module. ⌟

Prop. (5.8.2.7). The simplicial homology of the Moore complex of the bar resolution BG of group homology with coeeficient in R is just the group homology $H_n(G,R)$ for the trivial module R. And it has the same homology with the geometrization $|BG|$. ⌟

Lemma (5.8.2.8). $A_* \cong NA_* \oplus DA_*$ as a complex, $NA_*, A_*, (A/DA_*)$ are all homotopically equivalent. ⌟

Proof: We define similarly $N_k A_*$ and $D_k A_*$ and induct on k, our conclusion is the case $k = n-1$. When $k = 0$, $\mathrm{Im}\, d_0 \oplus \ker s_0 A_n = A_n$ because $d_0 s_0 = id_{n-1}$ thus $A_{n-1} \xrightarrow{s_0} A_n$ is a split injection.

There are two split exact rows by simplicial relations:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N_{k-1}A_{n-1} & \xrightarrow{s_k} & N_{k-1}A_n & \xrightarrow{1-s_k d_k} & N_k A_n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_{n-1}/D_{k-1}A_{n-1} & \xrightarrow{s_k} & A_n/D_{k-1}A_n & \longrightarrow & A_n/D_k A_n & \longrightarrow & 0 \end{array}$$

The first one split because it has a right section, the second one split because it has a left section. So by induction, $N_k A_n \to A_n/D_k A_n$ is an isomorphism, thus $N_k A_n \oplus D_k A_n = A_n$ because it splits.

For the homotopy equivalence, Cf.[Jardine P150]. □

Prop. (5.8.2.9)[Dold-Kan Correspondence]. For $R \in \mathcal{R}\mathrm{ing}$, the normalized Moore complex(5.8.2.2) functor N gives an equivalence of categories:

$$N_* : s\,\mathcal{M}\mathrm{od}_R \cong Ch_{\geq 0}(\mathcal{A}).$$

and the inverse is given by

$$(\sigma C_\bullet)_n = \bigoplus_{[n] \twoheadrightarrow [k]} C_k$$

and a morphism $\sigma_n \to \sigma_m$ for a morphism $[m] \to [n]$ is defined as follows: For $[n] \twoheadrightarrow [k]$, write $[m] \to [n] \to [k]$ as $[m] \twoheadrightarrow [r] \xrightarrow{\psi} [k]$ where φ is injective, thus maps $a \in C_k$ in σC_n to $\psi^*(a) \in C_r$ in σC_m, where ψ^* is zero unless $\psi = d^n : \Delta[n-1] \to \Delta[n]$. And homotopy groups and homology groups correspond via this equivalence, so does weak equivalences. ⌟

Proof: $\sigma(\mathcal{C}_\bullet)$ defines a simplicial Abelian group because of the uniqueness of the the canonical decomposition. There is a natural map from $\sigma(N\mathcal{A})$ to $\mathcal{A}$.

Now the task is to show that $\sigma(NA) \cong A$ and $N(\sigma C) \cong C$. We has $N(\sigma C)_n = C_n$ because $d^i C_n$ is 0 for $i \neq n$ and the other components are all degeneracies thus are not in $N(\sigma C)_n = C_n$ by(5.8.2.8).

Then we prove $\sigma(NA) \cong A$. It is a surjection by(5.8.2.8) and induction. For the injectivity, if $(a_\varphi) \neq 0$ is mapped to 0, a_{id_n} is 0 by(5.8.2.8). And we choose an ordering on the $\varphi : [n] \to [k]$ by dominating, and suppose ψ is a minimal one. Now choose a section ξ of ψ that ξ is the maximal section, thus $\varphi\xi$ cannot by id_k for any other φ. Now by induction we have $a_\psi = 0$, contradiction. □

Cor. (5.8.2.10) [Trivial Simplicial Algebra]. There is a functor form an R-algebra S to a trivial simplicial R-algebra $s(S)$, it is a fully faithful embedding and π_0 is left adjoint to it. ⌟

Proof: This is the adjointness of(4.10.1.12) under the equivalent σ(5.8.2.9). □

Cor. (5.8.2.11) [Model Structure on $s\,\mathcal{M}\mathrm{od}_R$]. By(4.5.4.2) applied to the equivalence with $Ch_{\geq 0}R$, $s\,\mathcal{M}\mathrm{od}_R$ has the structure of a model category where a morphism $X \to Y$ is

- an equivalence if it is a weak equivalence,
- a fibration if $NX_n \twoheadrightarrow NY_n$ for any $n \geq 1$.
- a cofibration if the the maps of the degenerate diagrams is of the form

$$X_n \to Y_n = X_n \oplus \bigoplus_{\varphi:[n]\twoheadrightarrow[k]} \varphi^* P_k$$

  compatible with the differential, and P_k are all projectives.

⌟

Prop. (5.8.2.12) [Fibrations]. A fibration of simplicial R-modules is a fibration iff it is a fibration of simplicial sets. Moreover, by(5.8.1.1), this is equivalent to $X \to \pi_0 X \otimes_{\pi_0(Y)} Y$ is surjective. ⌟

Proof: □

Prop. (5.8.2.13) [Simplicial Model Structure]. $s\,\mathcal{M}\mathrm{od}_R$ admits a simplicial model category structure. ⌟

Proof: Firstly $s\,\mathcal{M}\mathrm{od}_R$ is a simplicial category tensored and cotensored over $\mathcal{S}et_\Delta$(4.2.2.7) by(4.6.1.6), then it suffices to show(4.5.5.3)**?**. □

Prop. (5.8.2.14) [Model Structure on $s\,\mathcal{CR}\mathrm{ing}_R$]. By(4.5.4.2) applied to the forgetful functor to $\mathcal{S}et_\Delta$, Let R be a commutative algebra, then the category of simplicial commutative algebras $sCAlg_R$ has a simplicial model category structure where a morphism is

- a weak equivalence if it is a weak equivalence of simplicial sets.
- a fibration if it is fibration of simplicial sets.

⌟

Proof: □

Cor. (5.8.2.15). For a ring map $R \to S$, the tensor product $S \otimes_R -$ and forgetful functor form a Quillen adjunction between $s\,\mathcal{CR}\mathrm{ing}_R$ and $s\,\mathcal{CR}\mathrm{ing}_S$. ⌟

Def. (5.8.2.16) [Free Morphisms]. A morphism of simplicial R-algebras is called **free** if it is s-free(4.6.1.5) on the a set of objects P_k where P_k are projective R-modules. ⌟

Prop. (5.8.2.17) [Cofibrations in $sAlg_R$]. A morphism in $sAlg_R$ is a cofibration iff it is a retraction of a free morphism(5.8.2.16). In particular, a cofibrant simplicial R-algebra is the symmetrization of a chain of projective R-modules. ⌟

Proof: This follows from(4.5.4.2)(4.2.2.10) and notice the free morphisms just corresponds free commutative algebra applied to the attaching cell morphism in the category of sets. □

Simplicial Resolutions

Def. (5.8.2.18) [Simplicial Resolutions].

- Let $M \in \mathcal{M}od_R$, a **simplicial resolution** of M is a cofibrant replacement of M, or equivalently, it is an augmented simplicial R-module $X \to M$ that $NX \to M$ is a projective resolution.
- Let $M \in \mathcal{CR}ing_R$, a **free resolution** of M is free cofibrant replacement of M, or equivalently, it is an augmented simplicial commutative R-algebras $X \to M$ that $NX \to M$ is a resolution of R-modules, and P_n are all projective(4.1.1.21) in Alg_R. Notice we can always choose a free resolution only only cofibrant resolution by(4.5.8.3) and Dold-Kan complex.

⌟

Def. (5.8.2.19) [Bar Resolution]. Let $\mathcal{C}$ be a category and $T : \mathcal{C} \to \mathcal{C}$ a monad, and X is an algebra over T(4.3.1.2), then we can form a simplicial T-algebras where $B(T, X)_n = T^{n+1}X$ where the simplicial operators come from the action of T on itself and the action of T on X.

Then there is a simplicial morphism $B(T, X) \to X$, which is a simplicial homotopy. ⌟

Remark (5.8.2.20). If $\mathcal{C}$ is the category of sets, R is an algebra and T is a functor that sends a set S to $R[S]$, then a T-algebra is just an R-algebra, and the bar resolution is just the canonical resolution, and it is a cofibrant replacement, by(5.8.2.17). ⌟

Prop. (5.8.2.21). If $f, g : A^\bullet \to B^\bullet$ are two homotopic maps of cosimplicial Abelian groups, then f, g induces an isomorphism between their totalizations. ⌟

Proof: Cf.[[Sta]019S]. □

3 Properties

Def. (5.8.3.1). If A is a ring and $f_1, \ldots, f_n \in A$, the Koszul complex is defined to be

$$Kos(A, f_1, \ldots, f_n) = A \otimes^L_{\mathbb{Z}[X_1,\ldots,X_n]} \mathbb{Z}.$$

We want to extend this definition to the case of simplicial commutative rings.

Now if A is a simplicial ring and $f_1, \ldots, f_n \in \pi_0(A)$, let $g_1, \ldots, g_n$ in A_0 lifting f_i, then we define

$$Kos(A, f_1, \ldots, f_n) = A \otimes^L_{\mathbb{Z}[X_1,\ldots,X_n]} \mathbb{Z}.$$

Then we need to check that this is independent of the lifting: if there is another set of lifting h_i, because we have identities

$$A \otimes^L_{\mathbb{Z}[X_1,\ldots,X_n]} \mathbb{Z} \cong (A \otimes^L_{\mathbb{Z}[X_1,\ldots,X_n]} \mathbb{Z}[X_1]) \otimes^L_{\mathbb{Z}[X]} \mathbb{Z}$$

it suffices to prove for $n = 1$. Then there is a $\gamma \in A_1$ that $d_0(\gamma) = g, d_1(\gamma) = h$. Then we consider the evaluating maps

$$e_0, e_1 : \underline{\mathrm{Hom}}(\Delta_1, A) \to A$$

are weak equivalences?, and then the maps

$$e_0 : \underline{\mathrm{Hom}}(\Delta_1, A) \otimes^L_{\gamma,\mathbb{Z}[X]} \mathbb{Z} \to A \otimes^L_{g,\mathbb{Z}[X]} \mathbb{Z}$$

$$e_1 : \underline{\mathrm{Hom}}(\Delta_1, A) \otimes^L_{\gamma,\mathbb{Z}[X]} \mathbb{Z} \to A \otimes^L_{h,\mathbb{Z}[X]} \mathbb{Z}$$

are also weak equivalences, so we are done.

And if M is a simplicial A-module, then we define

$$Kos(M, f_1, \ldots, f_n) = M \otimes^L_A Kos(A, f_1, \ldots, f_n)$$

⌟

Def. (5.8.3.2) [Flatness]. A map $A \to B$ of simplicial rings is called **(faithfully)flat** if $\pi_0(B)$ is (faithfully)flat over $\pi_0(A)$ and $\pi_i(A) \otimes_{\pi_0(A)} \pi_0(B) \to \pi_i(B)$ is an isomorphism for any i. ⌟

Prop. (5.8.3.3). Flatness is stable under base change. ⌟

Proof: Cf.[Emerton note, completely flatness, P12]. □

Prop. (5.8.3.4). If $\pi_0(A) \otimes^L_A M$ is (faithfully)flat over $\pi_0(A)$, then M is (faithfully)flat over A. ⌟

Proof: Cf.[Emerton note, completely flatness, P12]. □

Def. (5.8.3.5). If A is a simplicial ring and M is a simplicial A-module, if $I = (f_1, \ldots, f_n)$ is an ideal of $\pi_0(A)$, then M is called ***I*-completely flat** over A if $Kos(M, f_1, \ldots, f_n)$ is flat over $Kos(A, f_1, \ldots, f_n)$.

Clearly if M is A-flat, then it is I-completely flat. ⌟

Prop. (5.8.3.6) [Flatness and Derived Completion]. If A is a simplicial ring, M is a flat simplicial A-module, and $I = (f_1, \ldots, f_n)$ is an ideal of $\pi_0(A)$, then its derived I-completion $\widehat{M} = ho\lim_n Kos(M, f_1^N, \ldots, f_n^N)$ is I-completely flat. The proof is similar to that of(5.9.7.4). ⌟

Prop. (5.8.3.7) [Relative Regular Sequence]. If $A \to B$ is a map of simplicial rings, then $x_1, x_2, \ldots, x_n \in \pi_0(B)$ is called **regular with respect to $A_\bullet$** if

$$A \to Kos(B, x_1, \ldots, x_n)$$

is flat. And if $I = (f_1, \ldots, f_m) \in \pi_0(A)$, then it is called ***I*-completely regular** if

$$Kos(A, f_1, \ldots, f_m) \to Kos(A, f_1, \ldots, f_m) \otimes^L_A Kos(B, x_1, \ldots, x_n) = Kos(B, f_1, \ldots, f_m, x_1, \ldots, x_n)$$

is flat. In particular, regular relative to $A_\bullet$ implies I-completely regular relative to $A_\bullet$. ⌟

Prop. (5.8.3.8). If $(f_1, \ldots, f_{r-1}, f)$ is regular w.r.t. A and $(f_1, \ldots, f_{r-1}, g)$ is regular w.r.t A, then $(f_1, \ldots, f_{r-1}, fg)$ is also regular w.r.t A. In particular, for any $n_i > 0$, $f_1^{n_1}, \ldots, f_r^{n_r}$ is also regular w.r.t. A. ⌟

Proof: Similarly as in(5.4.4.6), we have a distinguished triangle

$$Kos(M, f_1, \ldots, f_{r-1}, f) \to Kos(M, f_1, \ldots, f_{r-1}, fg) \to Kos(M, f_1, \ldots, g).$$

Then we can use induction. □

Prop. (5.8.3.9) [Regular and Derived Completion]. If $x_1, \ldots, x_n \in \pi_0(B)$ is regular w.r.t A, then they are I-completely regular w.r.t. A in the derived I-completion $\widehat{B}$. The proof is similar to that of(5.8.3.6). ⌟

4 Non-Abelian Derived Functors

Def. (5.8.4.1) [∞-Category of Chain Complexes]. Let $\mathcal{A}$ be an additive category, then $\mathrm{Ch}(\mathcal{A})$ is enriched over $\mathrm{Ch}(\mathcal{A}\mathrm{b})$, and the Dold-Kan correspondence can be made into a right-lax monoidal functor by ?[S. Schwede and B. Shipley. Equivalences of monoidal model categories.], so $N_*(\mathrm{Ch}(\mathcal{A}))$ is enriched over $s\mathcal{A}\mathrm{b}$, which consists of Kan complexes(5.8.1.1). Thus $N_*(\mathrm{Ch}(\mathcal{A}))$ is Bergner-fibrant, and we can define the **∞-category of chain complexes**

$$\mathrm{Ch}_\infty(\mathcal{A}) = N_\Delta(N_*(\mathrm{Ch}(\mathcal{A}))),$$

which is an ∞-category by(4.6.4.9). ⌟

Prop. (5.8.4.2) [Left Derived Functor]. Let $F : \mathcal{P}\mathrm{oly}_A \to \mathcal{C}$ be a functor where $\mathcal{C}$ is any ∞-category admitting all colimits (e.g. $D_\infty(\mathcal{A}\mathrm{b})$), then there exists a left Kan extension LF of F along $\mathcal{P}\mathrm{oly}_A \subset \mathcal{C}\mathcal{R}\mathrm{ing}_A$ that

- LF commutes with filtered colimit.
- LF commutes with geometric realization of simplicial resolutions: given $B \in \mathcal{C}\mathcal{R}\mathrm{ing}_A$ and a simplicial resolution $P_\bullet \to B$ by A-algebras, the geometric realization $|LF(P_\bullet)|$ is equivalent to $LF(B)$.

which is called the **left derived functor** of F. ⌟

Proof: Cf.[Bhatt, Prism, 7.1.2]. □

5.9 Derived Commutative Algebras

Main references are [Sta].

[Sta]Chap15 contains many beautiful results working on the derived category of rings, and is used heavily in Scholze's Thesis.

The basic construction of Rtensor and RHom should be redone at the level of ringed sites, Cf.[Sta]Chap21.

This section is obsolete and should be redone in the language of ∞-categories.

1 Basics

Prop. (5.9.1.1) [Product in $D(R)$]. Let R be a ring and $K_n \in D(R)$, then the product in $D(R)$ of K_n is given by $\prod I_n$, where I_n are K-injective resolutions of K_n. ⌟

Proof: This is immediate from(4.10.2.7). □

Def. (5.9.1.2) [Homotopy Fiber Square]. A square of Abelian groups is called a **homotopy fiber square** if it is a homotopy fiber square in the derived category, or equivalently, the kernel of the two rows(or the two columns) are isomorphic.

This notion is identical to the notion of pullback square when the rows or the columns are surjective.? ⌟

Prop. (5.9.1.3) [Bockstein Differential]. Let I be an invertible ideal of A, for any $M^\bullet \in D(A)$, we use the Breuil-Kisin Twist notation(8.9.5.1) and consider the exact triangle

$$M^\bullet \otimes^L_A A/I\{i+1\} \to M^\bullet \otimes^L_A I^i/I^{i+2} \to M^\bullet \otimes^L_A A/I\{i\}$$

obtained from the exact triangle

$$I^{n+1}/I^{n+2} \to I^n/I^{n+2} \to I^n/I^{n+1}$$

tensoring $\mathcal{O}_\Delta$. Then we get a Bockstein differential

$$\beta^n : H^n(M^\bullet \otimes^L_A A/I\{n\}) \to H^{n+1}(M^\bullet \otimes^L_A A/I\{n+1\})$$

Then these maps satisfy $\beta^{n+1} \circ \beta^n = 0$. ⌟

Proof: Consider the morphism of distinguished triangles:

$$\begin{array}{ccccc} I^{n+1}/I^{n+3} & \longrightarrow & I^n/I^{n+3} & \longrightarrow & I^{n+1}/I^{n+1} \\ \downarrow & & \downarrow & & \downarrow \\ I^{n+1}/I^{n+2} & \longrightarrow & I^n/I^{n+2} & \longrightarrow & I^{n+1}/I^{n+2} \end{array}$$

then we see for any $M^\bullet \in D(A)$, β^n factors as

$$H^n(M^\bullet \otimes^L_A I^n/I^{n+1}) \to H^{n+1}(M^\bullet \otimes^L_A I^{n+1}/I^{n+3}) \to H^{n+1}(M^\bullet \otimes^L_A I^{n+1}/I^{n+2})$$

and also we consider the distinguished triangle

$$I^{n+2}/I^{n+3} \to I^{n+1}/I^{n+3} \to I^{n+1}/I^{n+2}$$

to see that the composition

$$H^{n+1}(M^\bullet \otimes^L_A I^{n+1}/I^{n+3}) \to H^{n+1}(M^\bullet \otimes^L_A I^{n+1}/I^{n+2}) \xrightarrow{\beta^{n+1}} H^{n+2}(M^\bullet \otimes^L_A I^{n+2}/I^{n+3})$$

is 0, and this two observation gives the result. □

Injective Amplitude

Prop. (5.9.1.4) [Injective Amplitude]. For $K \in D(A)$, the following are equivalent:

- K has finite amplitude in $[a, b]$.
- $\mathrm{Ext}^i(N, K) = 0$ for any $N \in D^0(A)$ and $i \notin [a, b]$.
- $\mathrm{Ext}^i(A/I, K) = 0$ for any ideal I of A.

⌟

Proof: $1 \to 2 \to 3$ is clear. For $3 \to 1$: Notice $\mathrm{Ext}^n(A, K) = H^n(K)$, $H^i(K) = 0$ for any $i \notin [a, b]$. Then K is represented by a complex

$$0 \to I^a \to I^a \to I^{a+1} \to \ldots \to I^b \to \ldots.$$

Let $J = \ker(I^b \to I^{b+1})$, then K is also represented by

$$0 \to I^a \to I^a \to I^{a+1} \to \ldots \to I^b \to J \to 0.$$

Let $K' = (I^a \to \ldots \to I^b) \in D(A)$, then there is an distinguished triangle

$$J[-b] \to K \to K' \to J[1-b],$$

which induces an exact sequence $\mathrm{Ext}^b(R/I, K') \to \mathrm{Ext}^1(R/I, J) \to \mathrm{Ext}^{b+1}(R/I, K)$ for any ideal $I \subset A$. Then by $1 \to 2$, $\mathrm{Ext}^1(R/I, J) = 0$, implying J is injective. □

Prop. (5.9.1.5) [Dedekind Domain]. Let R be a Dedekind domain, then every ideal I is finite torsion-free thus projective over R, so every R-module has injective dimension≤ 1. In particular, $\mathrm{Ext}^i(M, N) = 0$ for any $i \geq 2$ and $M, N \in \mathcal{M}\mathrm{od}_R$. In particular, by(4.10.3.26). any $K \in D^+(R)$ is isomorphic to a direct sum of their cohomology groups. ⌟

Prop. (5.9.1.6). Let $(R, \mathfrak{m}, k)$ be a Noetherian local ring and $K \in D^+(R)$ have finite cohomology modules, then K has finite injective dimension iff $\mathrm{Ext}^i_R(k, K) = 0$ for i large. ⌟

Proof: Cf.[Sta]0AVJ. □

2 Derived Tensor and Tor

Prop. (5.9.2.1) [Differential Graded Structure]. If K is a commutative A-algebra object in $D(A)$ in the monoidal structure defined in(6.3.3.8), then $\oplus_{n\geq 0} H^n(K^\bullet)$ carries a natural graded commutative A-algebra structure. ⌟

Proof: Compare with(5.8.2.4).

We may replace K by a K-flat resolutions L^1(6.3.3.3) that the algebra structure map for K is represented by a morphism $L_1^\bullet \otimes_A L_1^\bullet \to L^2$ of complexes where L^2 is a complex quasi-isomorphic to K, hence the graded A-algebra structure is clear by(4.8.9.2), and it is commutative by(4.8.9.1). (How to check the structure is uniquely determined**?**). □

Tor

Def. (5.9.2.2) [Tor]. Let M, N be A-module, then the torsion group $\mathrm{Tor}_n^A(M,N)$ is defined to be $H^n(M \otimes^L_{\mathcal{O}} N)$, compatible with the definition in(6.3.3.11). ⌟

Def. (5.9.2.3) [Torsion Group]. Let A be a commutative ring, B an A-algebra and I be an ideal, then the ***I*-torsion** of B is defined to be $\mathrm{Tor}_1^A(A/I, B)$, denoted by $B[I]$. In case $I=(f)$, it can be checked that $B[f]$ is the set of elements of B that killed by f.

Also we denote $B[I^\infty] = \mathrm{colim}_{n\to\infty} B[I^n]$. And B is said to have **bounded *f*-torsion** iff $B[f^\infty] = B[f^n]$ for some n. ⌟

Prop. (5.9.2.4). If A is a commutative ring with bounded I-torsions and B is a flat A-module, then B also has bounded I-torsions. (Because tensoring B is exact). ⌟

Prop. (5.9.2.5)[Balancing Tor]. In the category of rings, $\mathrm{Tor}_n(A,B) = \mathrm{Tor}_n(B,A)$. This can be seen using spectral sequence of the double complex of flat resolutions of A and B. Similarly, we have two definitions of $\mathrm{Ext}^i(M,N)$ are compatible. ⌟

Proof: □

Prop. (5.9.2.6)[Base Change]. For a ring extension $R \to S$, using projective resolution and spectral sequence, there is a first quadrant homology spectral sequence:

$$E^2_{pq} = \mathrm{Tor}_p^S(\mathrm{Tor}_q^R(A,S), B) \Rightarrow \mathrm{Tor}^R_{p+q}(A,B).$$

Similarly, for Ext,

$$E_2^{pq} = \mathrm{Ext}^p_S(A, \mathrm{Ext}^q_R(S,B)) \Rightarrow \mathrm{Ext}^{p+q}_R(A,B).$$

⌟

Prop. (5.9.2.7) [Universal Coefficient Theorem]. Let P be a free R-module so $d(P_n)$ are all flat, then $Z(P_n)$ are also flat and

$$0 \to d(P_{n+1}) \to Z_n \to H_n \to 0$$

is a free resolution. we have an exact sequence:

$$0 \to H_n(P)\otimes_R M \to H_n(P\otimes_R M) \to \mathrm{Tor}_1^R(H_{n-1}(P), M).$$

$$0 \to \mathrm{Ext}^1_R(H_{n-1}(P), M) \to H^n(\mathrm{Hom}_R(P,M)) \to \mathrm{Hom}(H_n(P), M) \to 0$$

and these exact sequences non-canonically split because Z_n is a direct summand of P_n, thus $Z_n \otimes M$ is a direct summand of $P_n \otimes M$ and a fortiori $Z_n(P_n\otimes M)$. so $H_n(P)\otimes M$ is a direct summand of $H_n(P\otimes_R M)$. ⌟

Internal Hom and Derived Tensor

Prop. (5.9.2.8). If R is a ring and $K, L, M \in D(R)$, then

$$R\,\mathrm{Hom}_R(K, R\,\mathrm{Hom}(L,M)) = R\,\mathrm{Hom}_R(K\otimes^L_R L, M).$$

⌟

Proof: This is a special case of(6.3.3.29). □

Cor. (5.9.2.9).

$$\mathrm{Hom}_{D(R)}(K, R\,\mathrm{Hom}(L, M)) = \mathrm{Hom}_{D(R)}(K \otimes^L_R L, M),$$

i.e., derived tensor is left adjoint to internal Hom. ⌟

Proof: This follows from taking H^0, by(4.10.3.18). □

Prop. (5.9.2.10) [Derived Base Change Adjunction]. For a ring map $R \to S$ and any $L \subset D(R), M \subset D(S)$, there is an isomorphism

$$\mathrm{Hom}_R(L, M) \cong \mathrm{Hom}_S(L \otimes^L_R S, M)$$

⌟

Proof: This follows from(6.3.3.16). □

3 Rlim

Def. (5.9.3.1) [Rlim]. Rlim is the derived limit(4.10.6.1) in $D(\mathcal{A}\mathrm{b})$ restricted to the inverse systems consisting of discrete complexes. ⌟

Lemma (5.9.3.2). The set of Mittag-Leffler Complexes in $\mathcal{A}\mathrm{b}(\mathbb{N})$ is adapted for $R\lim$. ⌟

Proof: Firstly, for any complex (A_n), we can associate to it the complex (B_n) where $B_n = A_n \oplus A_{n-1} \oplus \ldots \oplus A_1$, then (B_n) is a Mittag-Leffler complex and $(A_n) \hookrightarrow (B_n)$. So ML complexes are sufficiently large.

Now for any exact sequence of complexes $0 \to (A_n) \to (B_n) \to (C_n) \to 0$, if A_n is ML, then $\lim B_i \to \lim C_i$ is surjective: for an element $(c_i) \in \lim C_i$, let $E_i = \pi_i^{-1}(c_i) \in B_i$, then (E_i) is an inverse system of nonempty sets, and it suffices to show (E_i) is ML, because then(4.1.1.45) will show there is a element $(e_i) \in \lim E_i \subset \lim B_i$ that maps to (c_i).

For this, Cf.[Sta]0598. □

Prop. (5.9.3.3) [Rlim].

- If (A_n) is Mittag-Leffler, then $R^1\lim((A_n)) = 0$.
- $R\lim((A_n))$ is represented by the complex in degree $0, 1$:

$$\prod_n A_n \to \prod_n A_n : (x_n) \mapsto (x_n - f_{n+1}(x_{n+1}))$$

.

- for any $(A_n) \in Ab(\mathbb{N})$ we have $R^p\lim((A_n)) = 0$ for $p > 1$.

⌟

Proof: 1 follows from(5.9.3.2) and(4.10.3.2).

2, 3: We use(4.10.3.2) again. Notice the complex (B_n) where $B_n = A_n \oplus A_{n-1} \oplus \ldots \oplus A_1$ and the complex (C_n) where $C_n = A_{n-1} \oplus A_{n-2} \oplus \ldots \oplus A_1$ form an exact sequence of complexes

$$0 \to (A_n) \to (B_n) \to (C_n) \to 0$$

where $B_n \to C_n : (x_i) \mapsto (x_i - f_{i+1}(x_{i+1}))$, and $(B_n), (C_n)$ are both ML, so we are done. □

4 Lifting Complexes

Prop. (5.9.4.1) [Lifting Projective Complex Along Thickening]. Let R be a ring and I be a nilpotent ideal, and $K \in D(R)$. Now if $K \otimes_R^L R/I$ is represented by a bounded above complex of projective R/I-modules, then there is a complex P of bounded above complex of projective R-modules that $P \cong K \in D(R)$, and $P \otimes_R R/I \cong E$. ⌟

Proof: Cf.[[Sta]09AR]. □

5 Pseudo-Coherent and Perfect Modules

Def. (5.9.5.1) [Pseudo-Coherent Modules]. Let R be a ring, $m \in \mathbb{Z}$, then $K \in D(R)$ is called an m**-pseudo-coherent module** iff there exists a complex $E^\bullet \in K^b(R)$ and a morphism $\alpha : E^\bullet \to K^\bullet$ where $K^\bullet$ represents K, s.t. $H^i(\alpha)$ is an isomorphism for $i > m$, and surjective for $i = m$.

$K \in D(R)$ is called a **pseudo-coherent module** if it is represented by a bounded above complex of finite free R-modules. ⌟

Prop. (5.9.5.2). If A is Noetherian and $C^\bullet$ is a complex of A-modules bounded above that every cohomology group H^i is a finite A-module, then there is a complex $L^\bullet$ of finite free A-modules, that $g : L^\bullet \to C^\bullet$ is a quasi-isomorphism.

Moreover, if C^i are all flat A-modules, then $L^\bullet \otimes_A M \to C^\bullet \otimes_A M$ is quasi-isomorphism for every M. ⌟

Proof: $C^\bullet$ is bounded above so we choose $L^n = 0$, and use induction to construct L^n that $H^i(L) \to H^i(C)$ is isomorphism for $i > n+1$ and surjection for $i = n+1$. For this, choose a generator $x_1, \ldots, x_r$ of $H^n(C)$ in $Z^n(C)$, and let $y_{r+1}, \ldots, y_s$ be a generator of $g^{-1}(B^{n+1}(C))$(Noetherian used), and let $g(y_i) = dx_i$ for $x_i \in C^n$.

Now let L^n be freely generated by $e_1, \ldots, e_s$ and $de_i = 0$ for $i \leq r$ and $de_i = y_i$ for $i > r$, and let $g : L^n \to C^n$ be $ge_i = x_i$. Then it can be verified to be a quasi-isomorphism.

If C^i are all flat, we check isomorphism for all f.g. modules M, because $\otimes$ and cohomology all commutes with direct limits. Use induction, for n large, both are 0, and if we write $0 \to R \to F \to M \to 0$, for F finite free, then there is a commutative diagram of long exact sequences, and for F, H^i are obviously isomorphism, so I can use five lemma. □

Def. (5.9.5.3)[Perfect Complexes of Modules]. Let R be a ring, then $K \in D(R)$ is called a **perfect module** if K is quasi-isomorphic to a bounded complex of finite projective R-modules. An R-module M is called perfect iff $M[0]$ is perfect. ⌟

Prop. (5.9.5.4) [Perfectness and Pseudo-Coherence]. An object $K \in D(R)$ is perfect iff it is pseudo-coherent and has finite Tor amplitude. ⌟

Proof: Cf.[Sta]0658. □

Prop. (5.9.5.5). If R is a regular ring of finite dimension, then an object $K \in D(R)$ is perfect iff $K \in D^b(R)$ and each $H^i(K)$ is a finite R-module. ⌟

Proof: Cf.[Sta]066Z. □

Prop. (5.9.5.6) [Duality of Perfect Complexes]. Let K be a perfect complex of $D(A)$, then the **dual complex** $K^\vee = R\operatorname{Hom}(K, A)$ is also a perfect complex and $(K^\vee)^\vee \cong K$. Also, there is a functorial isomorphism

$$L \otimes_A^L K^\vee = R\operatorname{Hom}_A(K, L)$$

⌟

Proof: Cf.[Sta]07VI. □

Prop. (5.9.5.7). If A is a ring and K_n is a system of perfect objects in $D(A)$, then for any $E \in D(A)$, there is an isomorphism

$$R\operatorname{Hom}_A(ho\operatorname{colim} K_n, E) \cong R\lim E \otimes^L_A K_n^\vee$$

⌟

Proof: By(5.9.5.6), $R\lim E \otimes^L_A K_n^\vee = R\lim R\operatorname{Hom}(K_n, E)$ which fits into a distinguished triangle

$$R\lim R\operatorname{Hom}(K_n, E) \to \prod \operatorname{Hom}(K_n, E) \to \prod \operatorname{Hom}(K_n, E)$$

. So it suffices to show that

$$\prod \operatorname{Hom}(K_n, E) \cong R\operatorname{Hom}_A(\oplus K_n, E).$$

This follows from Yoneda lemma and(6.3.3.28)(6.3.3.29). □

Prop. (5.9.5.8) [Perfectness and Thickening]. If R is a ring, $I \subset R$ is a nilpotent ideal, and $K \in D(R)$. If $K \otimes^L_R R/I$ is perfect in $D(R/I)$, then K is perfect in R. Moreover, if $K \otimes^L_R R/I = 0$, then $K = 0$. ⌟

Proof: Let $\overline{P}^\bullet \cong K \otimes^L_R R/I$ where P is a complex of finite projective R/I-modules, then by(5.9.4.1) there is a complex of projective R-modules P that $P/IP \cong \overline{P}$. Then it follows from Nakayama that P is bounded. □

Pseudo-Coherent Modules

Def. (5.9.5.9) [Pseudo-Coherent Complexes of Modules]. Let $R \in \mathcal{CA}\mathrm{lg}$, $K \in D(R)$ is called an m**-pseudo-coherent module** if there exists a perfect object $E \in D(R)$ and a morphism $E \to K$ that induces isomorphisms on H^i for $i > m$ and surjection on H^m.

$K \in D(R)$ is called a **pseudo-coherent module** if it is represented by a bounded above complex of finite free R-modules. ⌟

6 Derived Completeness

Cf.[Sta]Chap15.90.

Def. (5.9.6.1). For a ring A, $f \in A$ and a complex $K \in D(A)$, we denote by $T(K, f)$ a derived limit of the system

$$\ldots \to K \xrightarrow{f} K \xrightarrow{f} K$$

⌟

Prop. (5.9.6.2) [Properties of $T(K, f)$]. For a ring $A, f \in A$ and $K \in D(A)$, the following are equivalent:

1. $T(K, f) = 0$.
2. $R\operatorname{Hom}_A(A_f, K) = 0$.
3. $\operatorname{Ext}^n_A(A_f, K) = 0$ for all n.

4. $\mathrm{Hom}_{D(A)}(E, K) = 0$ for all $E \in D(A_f)$.
5. For any $p \in \mathbb{Z}$, $\mathrm{Hom}_A(A_f, H^p(K)) = 0$ and $\mathrm{Ext}^1_A(A_f, H^p(K)) = 0$.
6. For any $p \in \mathbb{Z}$, $T(H^p(K), f) = 0$.

⌟

Proof: $2, 3$ is clearly equivalent.

$4 \to 3$ is clear, and for $3 \to 4$: Let $I^\bullet$ be a complex representing K, then 3 says $\mathrm{Hom}_A(A_f, I^\bullet)$ is acyclic, and $\mathrm{Hom}_{D(A)}(E, K) = \mathrm{Hom}_{K(A)}(E, I^\bullet) = \mathrm{Hom}_{K(A_f)}(E, \mathrm{Hom}_A(A_f, I^\bullet))$. As $\mathrm{Hom}_A(A_f, I^\bullet)$ is both acyclic and K-injective(4.8.9.6), we get it is homotopic to 0 by(4.10.2.1), thus we get 4.

$1 \iff 3$: There is a free resolution of A_f given by

$$0 \to \oplus_n A \to \oplus_n A \to A_f \to 0$$

where the first map is $(a_n) \mapsto (a_n - f a_{n-1})$, and the second map is $(a_n) \mapsto \sum a_i/f^i$. Applying $\mathrm{Hom}_A(-, I^\bullet)$, we get a distinguished triangle

$$R\,\mathrm{Hom}_A(A_f, K) \to \prod K \to \prod K.$$

So this shows $R\,\mathrm{Hom}_A(A_f, K)$ is just $T(K, f)$, so we get $1 \iff 3$.

$1 \iff 5 \iff 6$: There is a spectral sequence convergence(choose a finite free resolution of A_f then rotate and use(4.10.7.10)):

$$E_2^{p,q} = \mathrm{Ext}^q_A(A_f, H^p(K)) \Rightarrow: \mathrm{Ext}^{p+q}(A_f, K)$$

This spectral sequence degenerates at E_2 because A_f has a length 1 resolution by free A-modules hence the E_2 page has only 2 rows. So there is an exact sequence

$$0 \to \mathrm{Ext}^1_A(A_f, H^{p-1}(K)) \to \mathrm{Ext}^1_A(A_f, K) \to \mathrm{Hom}_A(A_f, H^p(K)) \to 0.$$

Then we are done. □

Lemma (5.9.6.3). Let A be a ring, $K \in D(A)$, then the set I of f that $T(K, f) = 0$ is a radical ideal of A. ⌟

Proof: If $T(K, f) = 0$ and $g \in A$, then A_{gf} is a A_f-module, then

$$\mathrm{Ext}^n_A(A_{gf}, K) = \mathrm{Hom}_{D(A)}(A_{gf}[-n], K)(6.3.3.32) = 0$$

by(5.9.6.2) item4. Then $T(K, gf) = 0$ by(5.9.6.2) again. And if $f, g \in I$, there is an exact sequence

$$0 \to A_{f+g} \to A_{f(f+g)} \oplus A_{g(f+g)} \to A_{fg(f+g)} \to 0$$

by(5.4.2.3) and a easy check that the last term is surjective. Then from the long exact sequence of Ext, we get $\mathrm{Ext}^n(A_{f+g}, K) = 0$ for any n. Finally if $f^n \in I$, then $f \in I$, because $A_f = A_{f^n}$. □

Def. (5.9.6.4) [Derived Completeness]. Let A be a ring, $K \in D(A)$, I is an ideal of A, then K is said to be **derived complete** w.r.t I if $T(K, f) = 0$ for any $f \in A$. Let $D_{comp}(A, I)$ denote the subcategory consisting of derived I-complete objects in $D(A)$.

Let M be an A-module, then M is called **derived complete** w.r.t I if $M[0] \in D(A)$ is derived complete w.r.t I. ⌟

Prop. (5.9.6.5). A $\aleph_0$-filtered colimit of derived I-complete rings is also derived I-complete. ⌟

Proof: Cf.[Bhatt, Prism, 5.4.3]. □

Prop. (5.9.6.6) [Complete and Derived Complete]. Let A be a ring and I be an ideal, M an A-module, then

- If M is I-adically complete, then $T(M,f)=0$ for any $f\in I$.
- If $T(M,f)=0$ for all $f\in I$ and I is f.g., then $M\to\lim M/I^nM$ is surjective.

In particular, if I is f.g., M is I-adically complete iff M is derived I-adically complete and $\cap I^nM=0$.

In particularly, when M is f.g. over A Noetherian and $I\subset\mathrm{rad}(A)$, derived I-complete is equivalent to I-complete(5.2.2.14). ⌟

Proof: If M is I-adically complete, by(5.9.6.2), it suffices to show that $\mathrm{Hom}(A_f,M)=0$ and $\mathrm{Ext}^1(A_f,M)=0$. But $M=\varprojlim_n M/I^nM$, and $\mathrm{Hom}(A_f,M/I^nM)=0$, because $f\in I$. For Ext, use(4.10.3.24), for any extension

$$0\to M\to E\to A_f\to 0,$$

chose arbitrary e_n that maps to $1/f^n$. Then $\delta_n=fe_{n+1}-e_n\in M$. We consider

$$e_n'=e_n+\delta_n+f\delta_{n+1}+f^2\delta_{n+2}+\ldots,$$

which exist because M is I-adically complete. Then $fe_{n+1}'=e_n'$, so this gives a splitting of the extension.

Conversely, if $I=(f_1,\ldots,f_r)$ and $T(M,f_i)=0$ for any i, then by(5.2.3.16), we can assume $I=(f)$. Then consider the extension

$$0\to M\to E\to A_f\to 0$$

where $E=(M\oplus\bigoplus Ae_n)/(x_n-fe_{n+1}+e_n)\to A_f$ that maps M to 0 and e_n to $1/f^n$. This extension splits by(5.9.6.2) and(4.10.3.24), thus there is an element $x+e_0$ that generate a copy of A_f in E.

But then $x+e_0=x-x_0+fe_1=x-x_0-fx_1+f^2e_2\ldots$, which implies $x-x_0-fx_1-f^2x_2-\ldots-f^{n-1}x_{n-1}\in f^nE+A_f$ for any n. Then $x-x_0-fx_1-f^2x_2-\ldots-f^{n-1}x_{n-1}\in f^nM$, because $E=M\oplus A_f$. Then we are done. □

Prop. (5.9.6.7). If $M\in D(A/I)\subset D(A)$, then M is derived-I-complete. (This follows from the definition of $T(M,f)$). ⌟

Prop. (5.9.6.8)[Category of Derived Complete Modules]. Let I be an ideal of A, then the derived I-complete A-modules form a weak Serre subcategory of Mod_A. In particular, $D_{comp}(A,I)$ is also a weak Serre subcategory. ⌟

Proof: If $f:M\to N$ is a map of derived I-complete A-modules, then we consider the complex $K=(M\to N)$, then there is an exact sequence $0\to M[1]\to K\to N\to 0$, so we have $\mathrm{Ext}^n(A_f,K)=0$ for any $f\in I,n\in\mathbb{Z}$ because M,N does(5.9.6.2), so K is derived I-complete by(5.9.6.2) again. Then we have $\ker(f),\mathrm{Coker}(f)$ are derived I-complete, by(5.9.6.2) again. Extension is also clear. □

Lemma (5.9.6.9). If R is ring, I is an ideal, and $K\in D(R)$ that $K\otimes_R^L R/I=0$, then $K\otimes_R^L M$ for any $M\in D^b(R)$ with all the cohomology groups I-power torsions. ⌟

Proof: We use the truncation(4.8.6.6), then it suffices to prove for M discrete. Now $M=\cup M[I^n]$, and we have $K\otimes_R^L M=ho\operatorname{colim}K\otimes_R^L M[I^n]$, so we may assume $I^nM=0$ for some n. Consider the R-algebra $R'=R/I^n\oplus M$, where $M^2=0$, then it suffices to show $K'=K\otimes_R^L R'=0$. Now $0=K\otimes_R^L R/I=K'\otimes_{R'}^L R/I$, so by(5.9.5.8) $K'=0$. □

Prop. (5.9.6.10) [Derived Nakayama]. the derived tensor product $-\otimes_A^L A/I$ reflects isomorphism on $D_{comp}(A,I)$, i.e. if $M\otimes_A^L A/I=0$, then $M=0$. ⌟

Proof: Let $I=(f_1,\ldots,f_r)$, by(5.9.6.9), $M\otimes_A^L K_n=0$ for any $K_n=Kos(A,f_1^n,\ldots,f_r^n)$, so $K=R\lim K\otimes_A^L K_n=0$. □

Cor. (5.9.6.11). If I is f.g. and M is a derived I-complete A-module that $M/IM=0$, then $M=0$. ⌟

Proof: ?This should be an immediate corollary.

Let $I=(f_1,\ldots,f_r)$, if $M\neq 0$, let i be the largest integer that $M/(f_1,\ldots,f_i)M\neq 0$, then N is also derived I-complete by(5.9.6.8). But $f_{i+1}:N\to N$ is surjective, so $T(N,f_{i+1})\neq 0$, contradiction. □

Prop. (5.9.6.12). If A is derived I-complete, then (A,I) is a Henselian pair. ⌟

Proof: Cf.[[Sta]0G3H]?. □

Prop. (5.9.6.13) [Derived I-Completion]. If $I=(f_1,\ldots,f_n)$ is f.g. in A, the inclusion of categories $D_{comp}(A,I)\subset D(A)$ has a left adjoint, which maps K to

$$\widehat{K}=R\operatorname{Hom}((A\to\prod_{i_0}A_{f_{i_0}}\to\prod_{i_0<i_1}A_{f_{i_0}f_{i_1}}\to\ldots\to A_{f_1,\ldots f_r}),K).$$

called the **derived I-completion** of K.

Moreover, this construction is identical to $K\mapsto K^\bullet=R\lim(K\otimes_A^L K_n^\bullet)$, by(5.9.5.7) and(5.4.4.7). ⌟

Proof: There is a map $(A\to\prod_{i_0}A_{f_{i_0}}\to\prod_{i_0<i_1}A_{f_{i_0}f_{i_1}}\to\ldots\to A_{f_1,\ldots f_r})\to A$, which induces a morphism $K\to\widehat{K}$. Now by(6.3.3.28), $R\operatorname{Hom}(A_f,\widehat{K})$ is isomorphic to

$$R\operatorname{Hom}((A_f\to\prod_{i_0}A_{ff_{i_0}}\to\prod_{i_0<i_1}A_{ff_{i_0}f_{i_1}}\to\ldots\to A_{ff_1,\ldots f_r}),K)$$

as A_f is A-flat. Now this one is 0 for any $f\in I$, by(5.4.4.7), so $\widehat{K}$ is derived I-complete.

Conversely, if $\widehat{K}$ is derived I-complete, then $R\operatorname{Hom}(A_f,K)=0$ for any $f\in I$, thus $K\to\widehat{K}$ is an isomorphism is we inductively use the stupid truncation(4.8.6.6). □

Cor. (5.9.6.14). If M is an A-module, then $H^0(\widehat{M})$ is the derived-I-completion in the category of modules, by(4.10.1.12). ⌟

Cor. (5.9.6.15). (5.9.6.2) show the notion of derived I-complete and derived I-completion only depends on $\operatorname{rad} I$. ⌟

Principal Ideal Case

Prop. (5.9.6.16) [Bounded Torsion and Derived Completion]. Let A be a commutative ring and $f\in A$. If M is an A-module that has bounded f^∞-torsion, then the derived f-completion of M as a complex is a module and coincides with the classical f-adic completion. ⌟

Proof: The derived f-completion is defined to be

$$\widehat{M} = R\lim_n (M \otimes^L_{\mathbb{Z}[X]} \mathbb{Z}[X]/(x^n)) = R\lim_n (M \xrightarrow{f^n} M).$$

So by(4.10.6.5), there are exact sequences

$$R^1 \lim_n M/f^n M \cong H^1(\widehat{M})$$

$$0 \to R^1 \lim M[f^n] \to H^0(\widehat{M}) \to \lim_n M/f^n \to 0$$

$$H^{-1}(\widehat{M}) \cong \lim_n M[f^n]$$

Now the hypothesis implies that $(M[f^n])$ is Mittag-Leffler and $\lim_n M[f^n] = 0$, so we have the desired result. □

Cor. (5.9.6.17). Let R be a perfect $\mathbb{F}_p$-algebra, then the derived p-completion and p-adic completion of R coincide. ⌟

7 Derived Completely Properties

Def. (5.9.7.1)[Derived Completely Properties]. Let A be a commutative ring and I is a f.g. ideal, then $M \subset D(A)$ is called **I-completely (faithfully)flat/smooth/étale/**... iff $M \otimes^L_A A/I$ is discrete and is a (faithfully)flat A/I-module.

M is said to have **finite I-completely Tor amplitude** if $M \otimes^L_A A/I$ is is a bounded complex in $D(A/I)$.

Clearly, any flat/smooth/étale A-module M is I-completely flat/smooth/étale/... for any I. And M has finite I-completely amplitude if M has a finite resolution of flat A-modules. ⌟

Prop. (5.9.7.2)[I-Completely F.F. Descent]. If $A \to B \to B'$ are ring maps and I is an ideal of A,

1. If C is a B-algebra and B is I-completely f.f. over A, then C is I-completely (f.)f. over A iff C is I-completely (f.)f. over B.
2. If $B \to B'$ is I-completely flat, M is a B-module, then M is I-completely flat over A iff $M \otimes^L_B B'$ is I-completely flat over A.

⌟

Proof: 1: One direction is easy, for the other, if C is I-completely (f.)f. over A, then

$$C \otimes^L_A A/I = C \otimes^L_B B \otimes^L_A A/I = (C \otimes^L_B B/I) \otimes_{B/I} (B \otimes^L_A A/I)$$

is a discrete and (f.)f. C/I-module iff $(C \otimes^L_B B/I)$ does, as $(B \otimes^L_A A/I)$ is f.f. over B/I.

2: This is because $(B' \otimes^L_B M) \otimes^L_A A/I \cong B' \otimes^L_B (M \otimes^L_A A/I)$. □

Prop. (5.9.7.3). If I is generated by a Koszul-regular sequence, then any A-module M has finite I-completely Tor amplitude. ⌟

Proof: This is because $A/i \cong A \otimes^L_{\mathbb{Z}[X_1,\ldots,X_r]} \mathbb{Z}$ in this case, so $M \otimes^L A/I \cong M \otimes^L_{\mathbb{Z}[X_1,\ldots,X_r]} \mathbb{Z}$, which has f.m. homology groups because $\mathbb{Z}$ has a finite free $\mathbb{Z}[X_1,\ldots,X_n]$-resolution(5.4.4.1). □

Prop. (5.9.7.4)[I-Completely Flatness and Derived Completion]. Let A be a commutative ring and I be f.g., then the derived I-completion of a I-completely (faithfully)flat/étale M is I-completely (faithfully)flat/étale, both the complex and the module. In fact, $H^0(\widehat{M}) \otimes^L_A A/I \cong \widehat{M} \otimes^L_A A/I \cong M \otimes^L_A A/I$. ⌟

Proof: Because objects in the image of $D(A/I) \to D(A)$ are all derived I-complete, by(5.9.6.7), so there is an isomorphism $M \otimes_A^L A/I \cong \widehat{M} \otimes_A^L A/I$ for any M, because they are both left adjoint to $\mathcal{M}od_{A/I} \subset D(A)$, by the definition of derived I-completion and(5.9.2.10). So $\widehat{M} \otimes_A^L A/I \cong M \otimes_A^L A/I = M \otimes_A A/I$, which is a flat A/I-module. □

Prop. (5.9.7.5) [Flatness and Completed Derived Tensor]. The completed derived tensor of a I-completely flat/étale module is discrete and I-completely flat/étale. ⌟

Proof: If M is an I-completely flat A-module, then $M\widehat{\otimes}_A^L B$ is I-complete and I-completely flat by(5.9.7.4), and $(M\widehat{\otimes}_A^L B) \otimes_B^L B/I = H^0(M\widehat{\otimes}_A^L B) \otimes_B^L B/I = M \otimes_A^L B/I$, because they are both left adjoint of the forgetful functor $\mathcal{M}od_{B/I} \subset D(A)$. Then we have $M\widehat{\otimes}_A^L B \cong H^0(M\widehat{\otimes}_A^L B)$ is discrete, as they are both I-complete, by(5.9.6.2) and derived Nakayama. □

Prop. (5.9.7.6). A is derived I-completely flat iff A is I^n-completely flat for any $n > 0$. Moreover, in this case, A is derived J-completely flat for any ideal J that $I \subset \operatorname{rad} J$. ⌟

Proof: The exact sequence

$$0 \to I/I^2 \to A/I^2 \to A/I \to 0$$

induces distinguished triangles

$$(M \otimes_A^L A/I) \otimes_{A/I}^L I/I^2 \to M \otimes_A^L I/I^2 \to M \otimes_A^L A/I^2 \to M \otimes_A^L A/I$$

which shows $M \otimes_A^L I/I^2$ is discrete, $= N$. Then N is an A/I^2-module that $N \otimes_{A/I^2}^L A/I = M/IM$ is A/I-flat. Then N is A/I^2 flat: for any A/I^2-module L, let $L' = IL$ and $L'' = L/IL$ which are both A/I-modules, then there is a distinguished triangle

$$N \otimes_{A/I^2}^L L' \to N \otimes_{A/I^2}^L L \to N \otimes_{A/I^2} L''$$

and

$$N \otimes_{A/I^2}^L L' = (N \otimes_{A/I^2}^L A/I) \otimes_{A/I}^L L' = (M/IM) \otimes_{A/I} L'$$
$$N \otimes_{A/I^2}^L L'' = (N \otimes_{A/I^2}^L A/I) \otimes_{A/I}^L L'' = (M/IM) \otimes_{A/I} L''$$

are both discrete, hence so does $N \otimes_{A/I^2}^L L$, implying it is A/I^2-flat.

In a similar fashion, we can show M is I/I^n-flat for any n. And if $I \subset \operatorname{rad} J$, then $I^n \subset J$, so $M \otimes_A^L A/J = (M \otimes_A^L A/I^n) \otimes_{A/I^n}^L A/J$ is discrete and A/J-flat. □

Prop. (5.9.7.7). Let A be a ring and I be an invertible ideal, then any derived (p, I)-complete and (p, I)-completely flat A-complex $M \in D(A)$ is discrete and (p, I)-complete. Moreover, for any $n \geq 0$, we have $M[I^n] = 0$ and $M/I^n M$ has bounded p^∞-torsion. ⌟

Proof: M is (I^n, p)-completely flat by(5.9.7.6), so we fine $M \otimes_A^L A/I^n$ is p-completely flat in $D(A/I^n)$. Notice that A/I^n has bounded p^∞-torsion by induction(I invertible used), (5.9.7.11) says $M \otimes_A^L A/I^n$ is discrete in $D(A/I^n)$ and has bounded p^∞-torsion, and is p-adically complete. In particular,

$$M \otimes_A^L A/I^n = (M \otimes_A^L A/I^{n+1}) \otimes_{A/I^{n+1}}^L A/I^n$$

So if we denote $M \otimes_A^L A/I^n = M_n$, then $M_n = M_{n+1}/I^n M_{n+1}$, as M is derived I-complete, we have $M = R\lim(M \otimes^L A/I^n)$, so clearly M is discrete. And then we have $M \otimes^L AA/I^n = M/I^n M$, which means $M[I^n] = 0$, and $M/I^n M$ has bounded p^∞-torsion. Now because M is derived (p, I)-complete,

$$M = R\varprojlim_{m,n}((M \otimes_A I^n \to M) \otimes_{A/I^n} (A/I^n \xrightarrow{p^m} A/I^n)) = R\varprojlim_{m,n}(M/I^n \xrightarrow{p^m} M/I^n) = R\varprojlim_{m,n}(M/(I^n, p^n))$$

is (p, I)-complete. □

Lemma (5.9.7.8). Let C be a commutative ring with a f.g. ideal J, and D a C-algebra that has finite J-complete Tor amplitude, then the J-completed base change operator $-\widehat{\otimes}_C^L D$ commutes with totalization in $D^{\geq 0}(C)$ and $D^{\geq 0}(D)$, i.e. if $M^\bullet$ is a cosimplicial object with in $D^{\geq 0}(C)$ with totalization M, then

$$\mathrm{Tot}(M^\bullet)\widehat{\otimes}_C^L D \cong \mathrm{Tot}(M^\bullet \widehat{\otimes}_C^L D)$$

via the natural map. ⌟

Proof: Cf.[Scholze, Prism, 4.22].**?** □

Prop. (5.9.7.9)[Elkik's Algebrization Theorem]. Let A be a commutative ring and I is a f.g. ideal, then an A-algebras is derived I-completely étale/smooth iff it is the derived I-completion of some étale/smooth A-algebra. ⌟

Proof: if it is the derived I-completion of some étale/smooth algebra, then it is derived I-completely étale/smooth by(5.9.7.4). Converse, Cf.[A. Arabia, "Relèvements des algèbres lisses et de leurs morphismes", Commentarii Mathematici Helvetici 76 (2001), 607–639.]. □

Lemma (5.9.7.10). Let A be a ring, if M is an A-module with bounded f^∞-torsion, i.e. $M[f^\infty] = M[f^c]$ for some $c > 0$, then there are maps

$$(M \xrightarrow{f^n} M) \to M/f^n M, \quad M/f^{n+c} \to (M \xrightarrow{f^n} M)$$

in $D(A)$ inducing an equivalence between two pro-objects $\{M \xrightarrow{f^n} M\}$ and $\{M/f^n\}$. ⌟

Proof: The first map is obvious, for the second map, use the following commutative diagram:

$$\begin{array}{ccc} M/M[f^c] & \xrightarrow{f^{n+c}} & M \\ \downarrow{\scriptstyle f^c} & & \downarrow \\ M & \xrightarrow{f^n} & M \end{array}$$

the upper row is injective thus isomorphic to $M/f^{n+c}M$, then this gives the map. It can be checked that this is an equivalence of pro-objects**?**. □

Prop. (5.9.7.11). Let A be a commutative ring that has bounded f^∞-torsion, then for a $M \in D(A)$, the following is equivalent:

- M is derived f-complete and f-completely flat.
- M is discrete and is represented by a f-adically complete module that $M/f^n M$ is A/f^n-flat for any $n > 1$ and M has bounded f^∞-torsion.

Furthermore, in this case, $M \otimes_A A[f^\infty] = M[f^\infty]$. ⌟

Proof: By(5.9.7.10), $\{A/f^n A\}$ and $\{Kos(A, f^n)\}$ are two equivalence pro-objects in $D(A)$. So if 1 or 2 holds, then M is derived f-complete, so

$$M = R\lim(M \otimes_A^L Kos(A, f^n)) = R\lim(M \otimes_A^L A/f^n A).$$

Now if 1 holds, then $M_n = M \otimes_A^L A/f^n A$ is discrete by(5.9.7.6), and $M_n = M_{n+1}/f^n M_{n+1}$ is surjective:

$$M \otimes^L AA/f^n A = (M \otimes_A^L A/f^{n+1}A) \otimes_{A/f^{n+1}}^L A/f^n.$$

So $M = R\lim(M \otimes^L_A A/f^n A)$ is discrete. Then $M \otimes_A A/f^n = M \otimes^L_A A/f^n$ is flat over A/f^n.

Next we prove $M \otimes_A A[f^\infty] = M[f^\infty]$: There is an exact sequence

$$0 \to (A[f^n])[1] \to Kos(A, f^n) \to A/f^n \to 0$$

Then tensoring $M\otimes^L_A$ gives a distinguished triangle

$$(M \otimes^L_A A[f^n])[1] \to Kos(M, f^n) \to M \otimes^L_A A/f^n.$$

Notice that

$$M \otimes^L_A A[f^n] = (M \otimes^L_A A/f^n) \otimes^L_{A/f^n} A[f^n] = (M \otimes_A A/f^n) \otimes^L_{A/f^n} A[f^n] = M \otimes_A A[f^n]$$

by flatness, so the distinguished triangle shows $M \otimes_A A[f^n] \cong H^{-1}(Kos(M, f^n)) = M[f^n]$.

Conversely, if 2 holds, then there are equivalences of pro-objects

$$\{M \otimes^L_A A/f^n\} \cong \{M \otimes^L_A Kos(A, f^n)\} = \{Kos(M, f^n)\} \cong \{M/f^n M\}$$

by(5.9.7.10) as M has bounded f^∞-torsion. So

$$\widehat{M} = R\lim\{M \otimes^L_A Kos(A, f^n)\} = R\lim\{M/f^n M\} = M[0]$$

so M is derived p-complete. And the constant system

$$\{M \otimes^L_A A/f\} = \{M \otimes^L_{A/f^n} A/f^n \otimes^L_{A/f^n} A/f\} \cong \{M/f^n M \otimes^L_{A/f^n} A/f\} = \{M/fM\}$$

where we used $M/f^n M$ is A/f^n-flat. So $M \otimes^L_A A/f \cong M/fM$ is flat over A/f. □

8 Duality

Def. (5.9.8.1) [Dualizing Complexes]. Let A be a Noetherian ring, then a **dualizing complex** for A is a complex $\omega_A \in D(A)$ s.t.

- ω_A has finite injective dimension.
- $H^i(\omega_A)$ are all finite A-modules.
- $A[0] \to R\operatorname{Hom}(\omega_A, \omega_A)$ is a quasi-isomorphism.

⌟

Prop. (5.9.8.2) [Dualizing Complex is Local]. Let A be a Noetherian ring,

- If $B = S^{-1}A$ and $\omega_A \in D(A)$ is a dualizing complex for A, then $\omega_A \otimes^{\mathrm{L}}_A B$ is a dualizing complex for B.
- If $(f_1, \ldots, f_n) = (1) \in A$, and $\omega_A \in D(A)$ satisfies $(\omega_A)_{f_i}$ are dualizing complexes for A_{f_i} for any i, then ω_A is a dualizing complex for A.

⌟

Proof: Cf.[Sta]0A7G, 0A7H. □

Def. (5.9.8.3) [Dualizing Modules]. Let $(A, \mathfrak{m}, k)$ be a Noetherian local ring and ω_A a normalized dualizing complex for A, then $[\omega_A] = H^{-\dim A}(\omega_A)$ is called a **dualizing module** for A. ⌟

Def. (5.9.8.4) [Relative Dualizing Complex]. Cf.[Sta]0E9M. ⌟

Quasi-Finite Case

Cf.[Sta]Chap49.4.

Prop. (5.9.8.5). ⌟

6 Algebraic Geometry I: Scheme Theory

6.1 Sites, Sheaves, Topoi and Stacks

References are [Sta], [Ols16], [Vis08] and [Fibered Category to Algebraic Stacks Lamb].

1 Sites

Def. (6.1.1.1) [Sites]. A **site** is given by a category $\mathcal{C}$ and a set $\mathrm{Cov}(\mathcal{C})$ of families of morphisms with fixed target, called the **coverings** of $\mathcal{C}$ that:

- An isomorphism is a covering.
- Coverings of covering is a covering.
- Base change of a covering is a covering.

Sometimes A site is wrongly called a **topology**, the difference is that the morphism of site is looks like a reverse of a morphism of topology(6.1.1.5). We never talk about the category of sites, but we use $\mathcal{C} \in \mathcal{S}\mathrm{ite}$ to mean that $\mathcal{C}$ is a site. ⌟

Def. (6.1.1.2) [Discrete Topology]. A **discrete topology** or chaotic topology is a site that the only coverings are identies. In this way, we can regard any category as a site. ⌟

Def. (6.1.1.3) [Noetherian Topology]. An object U in a site $\mathcal{C}$ is called **quasi-compact** if for each covering of U, f.m. of them still forms a covering of U. The site $\mathcal{C}$ is called **Noetherian** if each object of $\mathcal{C}$ is quasi-compact.

Given a site $\mathcal{C}$, we can define a new site $\mathcal{C}^f$ whose coverings are coverings of $\mathcal{C}$ that are finite. Then this is truly a site and it is Noetherian. ⌟

Def. (6.1.1.4) [Comma Topology]. For a site $\mathcal{C}$ and an object S, we have the comma category $\mathcal{C}/S$(4.1.1.17), and we can define a topology on it where the coverings are coverings of $\mathcal{C}$ that is compatible over S. ⌟

Def. (6.1.1.5) [Continuous Functor]. A **continuous functor** between sites $\mathcal{C} \to \mathcal{D}$ is a functor that preserves covering and any base change by morphisms in a covering.

A **morphism of sites** $\mathcal{C} \to \mathcal{D}$ is given by a continuous functor $u : \mathcal{D} \to \mathcal{C}$ that u_s(6.1.2.11) is exact.

This exact condition is easy to be satisfied, by(6.1.2.14). ⌟

Def. (6.1.1.6) [Cocontinuous functors]. A **cocontinuous functor** between sites $u : \mathcal{C} \to \mathcal{D}$ is a functor that for any $U \in \mathcal{C}$ and any covering $\{V_i \to u(U)\}$ in $\mathcal{D}$, there is a covering $\{U_i \to U\} \in \mathcal{C}$ that refines $\{V_i \to u(U)\}$ after the functor u. ⌟

Topologies and Sieves

Def. (6.1.1.7) [Sieves]. For a covering $\mathcal{U} = \{U_i \to U\}$ in a category $\mathcal{C}$, define a subfunctor $h_{\mathcal{U}} \subset h_U$, where for each X $h_{\mathcal{U}}(X)$ consists of elements in $\mathrm{Hom}(X, U)$ that factor through some $U_i \to U$.

A **sieve** $\mathcal{S}$ on U is a subfunctor of h_U. Notice that any sieve must by of the form $h_{\mathcal{U}}$, by choosing $\mathcal{U}$ to consist of all arrows in $\{S(T)\}_{T \in \mathcal{C}}$. ⌟

Def. (6.1.1.8). If $\mathcal{T}$ is a Grothendieck topology on a category $\mathcal{C}$, then a sieve $S \subset h_U$ over U is said to **belong to** $\mathcal{T}$ or just a sieve of the site $\mathcal{C}$ if there exists a covering $\mathcal{U}$ of U that $h_{\mathcal{U}} \subset S$. ⌟

G-Spaces

Def. (6.1.1.9) [G-Spaces]. A **G-space** is a set X with a family of subsets of X that they form a site w.r.t inclusions and that covering are all set-theoretic coverings(but not necessarily conversely). These subsets are called **admissible opens** of X and covers are called **admissible covers**. (In other words, a G-topological space is a "topological space without unions"). Morphisms of G-spaces is simultaneously a continuous map and a morphism of sites. ⌟

Def. (6.1.1.10) [Completeness]. The completeness of a G-topological space X:

- G0: $\varnothing$ and X are admissible open.
- G1: Let $\{U_i \to U\}$ be an admissible cover, then a subset $V \subset U$ is admissible if $V \cap U_i$ are all admissible.
- G2: Let $\{U_i \to U\}$ be a cover of admissible opens for U admissible, then the cover is admissible if it has an admissible cover as a refinement.

⌟

Lemma (6.1.1.11) [Admissible is Local]. If G_2 is satisfied for a G-topological space X, then for an admissible covering $\{X_i \to X\}$ and another covering $\{U_i \to X\}$ between admissible opens, it is admissible iff $U_i \cap X_j$ is an admissible covering for X_j for each j. (By composition, $\{U_i \cap X_i \to X\}$ is admissible, and it refines $\{U_i \to X\}$). ⌟

Prop. (6.1.1.12) [Glue of Complete G-topological spaces]. For sets $\cup X_i = X$, if there are Grothendieck category $\mathcal{I}_i$ on X_i making X_i into a G-topological space, and they all satisfies the completeness conditions G_0, G_1, G_2 of(6.1.1.10). Assume that $X_i \cap X_j$ is $\mathcal{I}_i$-open in X_i and $\mathcal{I}_i, \mathcal{I}_j$ restrict to the same topology on $X_i \cap X_j$, then there is a unique Grothendieck category $\mathcal{I}$ on X making X a G-topological space that:

- X_i is $\mathcal{I}$-open and $\mathcal{I}$ restricts to $\mathcal{I}_i$ on X_i,
- $\mathcal{I}$ satisfies the completeness conditions G_0, G_1, G_2.
- X_i is a $\mathcal{I}$-covering of X.

⌟

Proof: By(6.1.1.10) and(6.1.1.11), the uniqueness is straightforward, for the existence,

- check Grothendieck first: Composition, base change.
- check condition 1: by hypothesis, and(6.1.1.10) applied to $X_i \cap X_j \to X_i$(this is admissible because id_{X_i} refined it).
- check condition 2: G_0 obvious, G_1 by if $V \cap U_i \cap X_i$ admissible, then $V \cap X_i$ admissible by admissibility of $U_i \to U$, then V is admissible, G_2: obvious

- check condition 3: because $X_i \cap X_j \to X_i$ is admissible.

□

Def. (6.1.1.13). A G-topological space is called **connected** iff there isn't two nonempty admissible open subset X_1, X_2 that $X_1 \cap X_2 = \varnothing$ and $\{X_1, X_2 \to X\}$ is an admissible cover. ⌟

$\mathcal{G}$-torsor

Def. (6.1.1.14) [Torsors]. Let $\mathcal{C}$ be a site and $\mathcal{G} \in \mathcal{S}\mathrm{h}^{\mathcal{G}\mathrm{rp}}(\mathcal{C})$, then a **pseudo $\mathcal{G}$-torsor** is a sheaf of sets $\mathcal{F}$ over $\mathcal{C}$ endowed with an action $\mathcal{G} \times \mathcal{F} \to \mathcal{F}$ that $\mathcal{G} \times \mathcal{F} \to \mathcal{F} \times \mathcal{F} : (g, f) \mapsto (gf, f)$ is an isomorphism.

A pseudo $\mathcal{G}$-torsor is called a **$\mathcal{G}$-torsor** if for any $U \in \mathcal{C}$, there is a covering $\{U_i \to U\}$ that $\mathcal{F}(U_i)$ is non-empty for each i. ⌟

Prop. (6.1.1.15). A $\mathcal{G}$-torsor on a site is trivial iff $\Gamma(\mathcal{C}, \mathcal{F}) \neq 0$(6.3.1.1). ⌟

Proof: This is because the transitive action of $\mathcal{G}$ on the global section induces an isomorphism $\mathcal{G} \to \mathcal{F}$. □

Prop. (6.1.1.16). If $\mathcal{C}$ is a subcanonical site, and $\mathcal{G}$ a sheaf of groups over $\mathcal{C}$, then a sheaf of sets $\mathcal{F}$ together with an action $\alpha : \mathcal{G} \times \mathcal{F} \to \mathcal{F}$ is a G-torsor iff for any $U \in \mathcal{C}$, there is a covering $\{U_i \to U\}$ that the restrictions to U_i are trivial torsors, i.e. $\alpha|_{\mathcal{C}/U_i} = \pi_2 : \mathcal{G}|_{U_i} \times \mathcal{F}|_{U_i} \to \mathcal{F}|_{U_i}$. ⌟

Proof: If $\mathcal{F}$ is a $\mathcal{G}$-torsor, then the restrictions of the torsor on U_i are trivial because they have global sections in $\Gamma(\mathcal{C}/U_i, \mathcal{F}) = \mathcal{F}(U_i)$, by(6.1.1.15). Conversely, if there is a covering $\{U_i \to U\}$ that the restrictions to U_i are trivial torsors, then the map $\mathcal{G} \times \mathcal{F} \to \mathcal{F} \times \mathcal{F} : (g, f) \mapsto (gf, f)$ are isomorphisms when restricted to U_i, which means $\mathcal{G}(U) \times \mathcal{F}(U) \to \mathcal{F}(U) \times \mathcal{F}(U)$ is an isomorphism for any U, because they are sheaves, so it is an isomorphism, and $\mathcal{F}$ is a $\mathcal{G}$-torsor. □

Cor. (6.1.1.17) [Representable G-Torsor]. If $\mathcal{C}$ is a site and G is a group object in $\mathcal{C}$, then

- $X \to Y$ is a G-torsor in the category $\mathcal{C}/Y$ iff $X \to Y$ is a G-equivariant map(where the action of G on Y is trivial), $G \times X \to X \times_Y X : (g, x) \mapsto (gx, x)$ is an isomorphism, and $\{X \to Y\}$ is refined by a covering of Y.
- If $\mathcal{C}$ is a subcanonical site, then $X \to Y$ is a G-torsor in the category $\mathcal{C}/Y$ iff $X \to Y$ is a G-equivariant map(where the action of G on Y is trivial), and there exists a covering $\{Y_i \to Y\}$ that each $Y_i \times_Y X \to Y_i$ is a trivial torsor, i.e. G-equivariantly isomorphic to $G \times Y_i \to Y_i$.

⌟

Cor. (6.1.1.18). If $\mathcal{C}$ is a site and G is a group object in $\mathcal{C}$, $X \to Y$ is a G-torsor in the category $\mathcal{C}/Y$, then the map $G \times G \times X \to X \times_Y X \times_Y X : (g, h, x) \mapsto (ghx, hx, x)$ is an isomorphism. ⌟

Presheaves

Def. (6.1.1.19) [Presheaves]. Let $\mathcal{C}, \mathcal{D} \in \mathcal{C}\mathrm{at}$, then a **presheaf** of objects in $\mathcal{D}$ on $\mathcal{C}$ is a functor $\mathcal{C}^{op} \to \mathcal{D}$. The category of presheaves of objects in $\mathcal{D}$ on $\mathcal{C}$ is denoted by $\mathcal{PS}\mathrm{h}(\mathcal{C}; \mathcal{D})$. For any $U \in \mathcal{C}$, $\Gamma(U, -)$ is the functor $\mathcal{PS}\mathrm{h}(\mathcal{C}; \mathcal{D}) \to \mathcal{D} : F \mapsto F(U)$. ⌟

Prop. (6.1.1.20). If $\mathcal{D}$ is complete or cocomplete, and the same is true for $\mathcal{PS}\mathrm{h}(\mathcal{C}; \mathcal{D})$. ⌟

Def. (6.1.1.21) [Coherent Sheaves]. For $\mathcal{C} \in \mathcal{C}\mathrm{at}$, denote $\mathcal{PS}\mathrm{h}_\infty(\mathcal{C}) = \mathcal{PS}\mathrm{h}(\mathcal{C}; \mathcal{G}\mathrm{rpd}_\infty)$(4.7.2.5), called the category of **coherent sheaves** on $\mathcal{C}$. It is complete and cocomplete. ⌟

Def. (6.1.1.22) [Points]. A **point of a site** is a Cf.[Sta]00Y3. ⌟

2 Sheaves and Topoi

Def. (6.1.2.1) [Sheaves]. Let $\mathcal{C}$ be a site and $\mathcal{D} \in \mathcal{C}at_\infty$, then $\mathcal{F} \in \mathcal{PS}h(\mathcal{C};\mathcal{D})$ is called a **sheaf** of objects in $\mathcal{D}$ on $\mathcal{C}$ iff for any sieve $\mathcal{S}$ on U belong to $\mathcal{C}$, the natural map

$$\mathrm{Map}(h_U, \mathcal{F}) \to \mathrm{Map}(h_{\mathcal{U}}, \mathcal{F})$$

is an equivalence?. ⌟

Def. (6.1.2.2) [Separate Presheaves]. Let $\mathcal{C}$ be a site, then $\mathcal{F} \in \mathcal{PS}h^{\mathcal{S}et}(\mathcal{C})$ is called a **separated presheaf** if $F(U) \hookrightarrow \prod_i F(U_i)$ is injective for any covering $\mathcal{U} = \{U_i \to U\} \in \mathrm{Cov}(\mathcal{C})$. ⌟

Def. (6.1.2.3)[Effective Epimorphisms]. An epimorphism $\{U_i \to V\}$ in a category is called a **family of effective epimorphisms** if

$$\mathrm{Hom}(V, Z) \to \prod \mathrm{Hom}(U_i, Z) \rightrightarrows \prod \mathrm{Hom}(U_i \times_V U_j, Z)$$

is exact for each Z. Similarly for a **family of universal effective epimorphisms**. ⌟

Prop. (6.1.2.4) [Subcanonical Site]. The class of all families of universal effective epimorphisms in a category forms a Grothendieck topology, called the **canonical topology**. It is the finest topology that all representable presheaves are sheaves.

Topologies that are coarser than the canonical topology are called **subcanonical topology**. Equivalently, a subcanonical topology is a topology that every representable presheaf is a sheaf. ⌟

Proof: We only need to verify that family of universal effective epimorphisms is closed under composition. For this, first prove epimorphism, then use epimorphism to prove effectiveness. Universal follows routinely. Cf.[Tamme]. □

Prop. (6.1.2.5). For a subcanonical topology on a site $\mathcal{C}$, its restriction on a localizing category $\mathcal{C}/S$ is subcanonical. ⌟

Proof: The only nontrivial part is that the glued morphism is a morphism over S. For this, consider its composition that maps to S, then the uniqueness of the exact sequence(6.1.2.3) will show that it is truly a S-morphism. □

Prop. (6.1.2.6). Let $\mathcal{C}$ be a subcanonical site, and $f : X \to Y$ is an arrow in $\mathcal{C}/S$, suppose there is a covering $\{S_i \to S\}$ that the pullback of f to $\mathcal{C}/S_i$ are all isomorphisms, then f is an isomorphism. ⌟

Proof: This follows from(6.1.3.6) and(6.1.3.8). □

Prop. (6.1.2.7) [Sheafification]. Let $\mathcal{C}$ be a site, consider the functor

$$(\cdot)^+ : \mathcal{PS}h^*(\mathcal{C}) \to \mathcal{S}h^*(\mathcal{C}) : F^+(U) = \varinjlim \ker(\prod_i F(U_i) \rightrightarrows \prod_{i,j} F(U_i \times_U U_j)) = \check{H}^0(U, F).$$

Then

- For $F \in \mathcal{PS}h^*(\mathcal{C})$, F^+ is separated.
- If $F \in \mathcal{PS}h^*(\mathcal{C})$ is separated, $F \to F^+$ is injective and $F^+ \in \mathcal{S}h^*(\mathcal{C})$. (The problem of separated is that the cover may not be identical in $U_i \times_U U_j$ but only on a cover of it).
- $(\cdot)^+$ is left exact.

- **sheafification functor** $(\cdot)^{\#} : \mathcal{PSh}^* \to \mathcal{Sh}^* : F \mapsto F^{\#} = F^{++}$ is exact and it is left adjoint to the forgetful functor.

So the forgetful functor is left exact and it preserves injectives. Thus the sheaf cokernel is the shification of the presheaf kernel, the sheaf kernel is the presheaf kernel. ⌟

Proof: The separatedness is simple. For sheaf condition, an element of $F^+(U_i)$ is represented by a covering $\{V_{ij} \to U_i\}$, and there restriction to $U_i \times_U U_j$ coincide by separatedness hence the covering $\{V_{ij} \to U\}$ is an element of $F^+(U)$.

Sh is left exact because $(-)^+$ is left exact from $\mathcal{PSh}^*$ to $\mathcal{PSh}^*$ by(6.3.2.4) checked on every element U. It is right exact trivially, hence it is exact. □

Def. (6.1.2.8) [Constant Sheaves]. The **constant sheaf** $\underline{S}$ for a set S is the sheafification of the constant presheaf $U \mapsto S$. ⌟

Transfer of Sheaves under Morphisms of Sites

Def. (6.1.2.9) [Functoriality of Presheaves]. Given a functor of sites $u : \mathcal{C} \to \mathcal{C}'$, which should be regarded as an inverse map, there are maps

$$u^p F'(U) = F'(u(U)) : \mathcal{PSh}(\mathcal{C}') \to \mathcal{PSh}(\mathcal{C}), \quad u_p(F)(U') = \varinjlim_{U_i | U' \to u(U_i)} F(U_i) : \mathcal{PSh}(\mathcal{C}) \to \mathcal{PSh}(\mathcal{C}')$$

Then u_p is left adjoint to u^p.

We can also define a functor

$${}_pu : {}_pu(F)(U') = \varprojlim_{\{U_i | u(U_i) \to U'\}^{op}} F(U_i) : \mathcal{PSh}(\mathcal{C}) \to \mathcal{PSh}(\mathcal{C}').$$

Then this functor is right adjoint to u^p, by duality. ⌟

Proof: A map $f \in \mathrm{Mor}(u_p(F), G)$ is represented by compatible maps

$$\varinjlim_{U_i : U' \to u(U_i)} F(U_i) \to G(U'),$$

and this is represented by compatible maps $F(U_i) \to G(U')$ which is indexed over $\prod_{U' \in \mathcal{C}'} \mathcal{I}_{U'}$, where $\mathcal{I}_{U'} = \{U_i : U' \to u(U_i)\}$. Now this is equivalent to compatible maps $F(U_i) \to G(u(U_i))$, which is a map $g \in \mathrm{Mor}(F, u^p(G))$. □

Cor. (6.1.2.10). u^p is exact. ⌟

Def. (6.1.2.11) [Functoriality of Sheaves].

- Given a continuous functor $u : \mathcal{C} \to \mathcal{C}'$ between sites, there are maps

$$u_s = \sharp \circ u_p \circ \iota : \mathcal{S} \to \mathcal{S}', \quad u^s = u^p \circ \iota : \mathcal{S}' \to \mathcal{S}.$$

  u_s is left adjoint to u^s, by adjointness of u_p, u^p and $\sharp, \iota$.

- Given a cocontinuous functor $u : \mathcal{C} \to \mathcal{C}'$ between sites, there are maps

$$u^s = \sharp \circ u^p \circ \iota : \mathcal{S}' \to \mathcal{S}, \quad {}_su = {}_pu \circ \iota : \mathcal{S} \to \mathcal{S}'.$$

  u^s is left adjoint to ${}_su$, by adjointness of $u^p, {}_pu$ and $\sharp, \iota$. Moreover, u^s is exact.

⌟

Proof: 1: Notice if $\mathcal{F}$ is a sheaf, then $u^s\mathcal{F}$ is also a sheaf, by continuity(6.1.1.5).

2: ${}_pu\mathcal{F}$ is a sheaf by [Sta]00XK**?**. u^p is clearly right exact, and it is left exact because $\iota, \sharp$ do, and u^p is exact by(6.1.2.10). □

Cor. (6.1.2.12). When u is continuous, $(u_p(G))^\sharp \cong (u_p(G^\sharp))^\sharp$ for any presheaf G on T.
When u is cocontinuous, $(u^pG)^\sharp \cong (u^p(G^\sharp))^\sharp$ for any presheaf G on T. ⌟

Proof: Use Yoneda lemma. □

Prop. (6.1.2.13). For $Z \in T$, $u_p h_Z = h_{u(Z)}$. ⌟

Proof: Use the adjointness of u_p, u^p(6.1.2.9), then for any presheaf F,

$$\mathrm{Hom}(u_p h_Z, F) = \mathrm{Hom}(h_Z, u^p F) = f^p(F)(Z) = F(f(Z)),$$

thus we are done by Yoneda lemma. □

Prop. (6.1.2.14) [When is u_s Exact]. If $f : \mathcal{C} \to \mathcal{C}'$ is a continuous functor between sites that $\mathcal{I}_{U'}$ is cofiltered for any $U' \in \mathcal{C}'$, where $\mathcal{I}_{U'}$ is the category of all pairs (U, φ) where $U \in \mathcal{C}$ and $\varphi : U' \to u(U)$, then u_s is exact.

In particular, this is the case when $\mathcal{C}, \mathcal{C}'$ both have weakly final objects and finite fiber products and u preserves them. Notice the condition of weakly final objects can be released if we can show $\mathcal{I}_{U'}$ is nonempty for any U'. ⌟

Proof: It suffices to show the left exactness of u_p. By definition, $u_p(U') = \varinjlim_{\mathcal{I}_{U'}^{op}} F_{U'}$ where $F_{U'}$ is the covariant functor $(U, \varphi) \to F(U)$. Because $\mathcal{I}_{U'}^{op}$ is filtered, this colimit process is exact form $\mathrm{Hom}(\mathcal{I}_{U'}^{op}, \mathcal{A}b)$ to $\mathcal{A}b$ and u_p is exact. Now shifification is also exact(6.1.2.7), so we conclude.

The last assertion is clear.(Notice the weakly-final object are used to assure $\mathcal{I}_{U'}$ is nonempty.) □

Prop. (6.1.2.15) [Localization Site]. For a site T and $Z \in T$, there is a site T/Z as objects over T, and $i : T/Z \to T$ is continuous. Then i^s is exact. ⌟

Proof: $R^q i^s(F) = (i^p(\mathcal{H}^q(F)))^\sharp$(6.3.1.7), and $(\mathcal{H}^q(F))^\sharp = 0$(6.3.2.14), so it suffices to show i^p and $\sharp$ commutes. But i^s and $^+$ commutes obviously. □

Prop. (6.1.2.16) [Sheaf Condition is Local]. To check sheaf condition for presheaf w.r.t. a topology, it suffice to show that for any covering, there is a refinement covering of it that sheaf condition hold, because by the definition of sheafification functor, $F^+ = F$, so F is a sheaf. ⌟

Cor. (6.1.2.17). For two topology on a same category that $\mathcal{I}'$ is finer than $\mathcal{I}$, then any $\mathcal{I}'$-sheaf is a $\mathcal{I}$-sheaf. And if any covering in $\mathcal{I}'$ can be refined by a covering in $\mathcal{I}$, then $\mathcal{S} \to \mathcal{S}'$ is an equivalence of categories. In particular, if T is Noetherian, $\mathcal{S}(T)$ and $\mathcal{S}(T^f)$(6.1.1.3) are equivalent. ⌟

Topoi

Def. (6.1.2.18) [Topoi]. A **topos** is an Abelian category that is equivalent to the category of sheaves $\mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C})$ on a site $\mathcal{C}$. A **morphism of topoi** $f : \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C}) \to \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{D})$ is an adjunction

$$f^{-1} : \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{D}) \rightleftharpoons \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C}) : f_*$$

s.t. f^{-1} is exact. Compositions of morphisms of topoi are defined routinely. A **2-morphism of topoi** between two morphisms of topoi $f, g : \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C}) \to \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{D})$ is a natural transformation $t : f_* \to g_*$.
⌟

Prop. (6.1.2.19) [Presheaves and Topoi]. $\mathcal{C} \in \mathcal{C}at$ is a Grothendieck category iff it is a left exact, reflective accessible localization(4.1.2.10) of $\mathcal{PS}h^{\mathcal{S}et}(\mathcal{A})$ for some $\mathcal{A} \in \mathcal{C}at$. ⌟

Sites and Topoi

Prop. (6.1.2.20) [Continuous Maps and Topoi]. A morphism of sites $f : \mathcal{D} \to \mathcal{C}$ consists of a continuous functor $u : \mathcal{C} \to \mathcal{D}$ that u_s is exact, so it induces a functor of topoi $f : \mathcal{S}h^{\mathcal{S}et}(\mathcal{C}) \to \mathcal{S}h(\mathcal{D})$, if we define $f^{-1} = u_s, f_* = u^s$, by(6.1.2.11). ⌟

Prop. (6.1.2.21) [Cocontinuous Maps and Topoi]. Let $u : \mathcal{C} \to \mathcal{D}$ be a cocontinuous functor between sites, then this defines a morphism of topoi $g : \mathcal{S}h^{\mathcal{S}et}(\mathcal{C}) \to \mathcal{S}h^{\mathcal{S}et}(\mathcal{D})$, if we define $g^{-1} = u^s$ and $g_* = {}_s u$, by(6.1.2.11). ⌟

Prop. (6.1.2.22) [Cocontinuous Map with a Right Adjoint]. Let $u : \mathcal{C} \to \mathcal{D}$ be a cocontinuous functor between sites with a right adjoint $v : \mathcal{D} \to \mathcal{C}$, then the morphism of topoi $g : \mathcal{S}h^{\mathcal{S}et}(\mathcal{C}) \to \mathcal{S}h^{\mathcal{S}et}(\mathcal{D})$ is pretty simple,

$$g^{-1}\mathcal{G}(U) = \mathcal{G}(u(U)), \quad g_*\mathcal{F}(V) = \mathcal{F}(v(V)).$$

This holds in particular for localization of sites. ⌟

Proof: It follows from adjunction that $u^p h_V = h_{v(V)}$, so $g^{-1}(h_V^\sharp) = (u^p h_V^\sharp)^\sharp = (u^p h_V)^\sharp = h_{v(V)}^\sharp$, and

$$(g_*\mathcal{F})(V) = \mathrm{Hom}(h_V^\sharp, g_*\mathcal{F}) = \mathrm{Hom}(g^{-1}h_V^\sharp, \mathcal{F}) = \mathrm{Hom}(h_{v(V)}^\sharp, \mathcal{F}) = \mathcal{F}(v(V)).$$

The other identity is clear. □

Prop. (6.1.2.23) [Continuous and Cocontinuous Maps and Topoi]. Let $u : \mathcal{C} \to \mathcal{D}$ be a functor between sites that satisfies

- u is continuous and cocontinuous,
- u is fully faithful,
- $\mathcal{C}$ has final objects and fiber products and u preserves them.

then there are two maps of topoi: $f = (u_s, u^s) : \mathcal{S}h^{\mathcal{S}et}(\mathcal{D}) \to \mathcal{S}h^{\mathcal{S}et}(\mathcal{C}), g = (u^s, {}_s u) : \mathcal{S}h^{\mathcal{S}et}(\mathcal{C}) \to \mathcal{S}h^{\mathcal{S}et}(\mathcal{D})$ induced by u(6.1.2.20)(6.1.2.14)(6.1.2.21). They satisfy $f \circ g = \mathrm{id}_{\mathcal{S}h^{\mathcal{S}et}(\mathcal{C})}$, and $f^{-1} = u_s$ is fully faithful.

In particular, if we define $g_! = u_s$, then there are two adjunctions

$$(g_!, g^{-1}) : \mathcal{S}h(\mathcal{C}) \rightleftharpoons \mathcal{S}h(\mathcal{D}), \quad (g^{-1}, g_*) : \mathcal{S}h(\mathcal{D}) \rightleftharpoons \mathcal{S}h(\mathcal{C}).$$

⌟

Proof: We need to show that for any $\mathcal{F} \in \mathcal{S}h^{\mathcal{S}et}(\mathcal{C})$, $\mathcal{F} \cong g^{-1}g_!\mathcal{F}$ and $g^{-1}g_*\mathcal{F} \cong \mathcal{F}$. For this, Cf.[Sta]00XT.**?**

Then $f^!$ is fully faithful follows from the equality $\mathcal{F} \cong g^{-1}g_!\mathcal{F}$. □

Prop. (6.1.2.24) [Special Cocontinuous Maps and Topoi]. A functor $u : \mathcal{C} \to \mathcal{D}$ between sites is called a **special cocontinuous functor** if:

- u is continuous and cocontinuous,
- Given any $a, b : U' \to U \in \mathcal{C}$ s.t. $u(a) = u(b) : u(U') \to u(U)$, there is a covering $\{f_i : U_i' \to U'\}$ that $af_i = bf_i$.

- Given any $U', U \in \mathcal{C}$ and a morphism $c : u(U') \to u(U) \in \mathcal{D}$, there exists a covering $\{f_i : U'_i \to U'\} \in \mathcal{C}$ and morphisms $c_i : U'_i \to U$ that $u(c_i) = c \circ u(f_i)$.
- Given any $V \in \mathcal{D}$, there is a covering of the form $\{u(U_i) \to V\}$ in $\mathcal{D}$.

Then the induced morphism of topoi $g : \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C}) \cong \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{D})$(6.1.2.21) is an equivalence of topoi. ⌟

Proof: Cf.[Sta]03A0.**?** □

Cor. (6.1.2.25) [Comparing Topologies]. Let $\mathcal{C}'$ be a fully subcategory of $\mathcal{C}$, and
- $i : \mathcal{C}' \to \mathcal{C}$ is continuous, i.e. $\mathrm{Cov}(\mathcal{C}') \to \mathrm{Cov}(\mathcal{C})$.
- $i : \mathcal{C}' \to \mathcal{C}$ is cocontinuous, i.e. any covering $\{U_i \to U'\} \in \mathrm{Cov}(\mathcal{C})$ s.t. $U' \in \mathcal{C}'$ has a refinement $\{U'_j \to U'\} \in \mathrm{Cov}(\mathcal{C}')$.
- Each $U \in \mathcal{C}$ has a covering $\{U_i \to U\} \in \mathrm{Cov}(\mathcal{C})$ with $U_i \in T'$.

then $i : \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C}') \to \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C})$ is an equivalence of topoi. i^{-1} is just the restriction functor, and i_* is called the **extension functor of sheaves**.

In particular, this applies to the case $i : \mathcal{C}' = \mathcal{C}/Z \to \mathcal{C}$, the localization category, in with case for $Z' \in \mathcal{C}/Z$, $i^{-1}F(Z') = F(Z')$ is called the **restriction sheaf**. ⌟

Prop. (6.1.2.26) [Localizing at Sheaves]. Let $\mathcal{C}$ be a site and $\mathcal{F}_i$ be a set of topos on $\mathcal{C}$, then there is an equivalence $\mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C}) \cong \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{C}')$ induced by a special cocontinuous functor $\mathcal{C} \to \mathcal{C}'$(6.1.2.24) s.t.
- $\mathcal{C}'$ has the subcanonical topology,
- A family of morphisms $\{V_i \to V\}$ are a covering of $\mathcal{C}'$ iff $\coprod h_{V_I} \to h_V$ is surjective.
- $\mathcal{C}'$ has fiber products and a final object.
- Every subsheaf of a representable sheaf is representable,
- Each $g_*\mathcal{F}_i$ is a representable sheaf.

⌟

Proof: Cf.[Sta]03CI. □

3 Stacks

Def. (6.1.3.1) [Stacks]. Let $\mathcal{F} \to \mathcal{C}$ be a fibered category on a site $\mathcal{C}$. Then $\mathcal{F}$ is called a **prestack** over $\mathcal{C}$ if for each covering $\{U_i \to U\}$ in $\mathcal{C}$, the functor $\mathrm{Hom}(h_U, \mathcal{F}) \to \mathrm{Hom}(h_{\mathcal{U}}, \mathcal{F})$(6.1.1.7) is fully faithful. It is called a **stack** over $\mathcal{C}$ if it is moreover an equivalence of categories. ⌟

Def. (6.1.3.2) [Category of Descent Datum]. Let $\mathcal{F} \to \mathcal{C}$ be a fibered category on a site $\mathcal{C}$, $U \in \mathcal{C}$ and $\mathcal{U}$ is a covering of U. Given a choice of fibered products U_{ij}, U_{ijk} in $\mathcal{C}$, we can define the **category of descent datum** $\mathcal{F}_{desc}(\mathcal{U})$ to be the category of tuples $(\xi_i, \xi_{ij}, \xi_{ijk})$ where $\xi_\alpha \in \mathcal{F}(U_\alpha)$ with Cartesian morphisms between them that are commutative. A morphism in $\mathcal{F}_{desc}(\mathcal{U})$ is a family of morphisms $(\varphi_i, \varphi_{ij}, \varphi_{ijk})$ commuting with the Cartesian morphisms.

Then there is an equivalence of categories $\mathrm{Hom}(h_{\mathcal{U}}, \mathcal{F}) \cong \mathcal{F}_{desc}(\mathcal{U})$. ⌟

Proof: For any $F : h_{\mathcal{U}} \to \mathcal{F}$, $U_i \to U \in h_{\mathcal{U}}(U_i)$, applying F to the arrows $\mathrm{id}_{U_i}, U_{ij} \to U_i, U_{ijk} \to U_{ij} \in h_{\mathcal{U}}$, we get an element in $\mathcal{F}_{desc}(\mathcal{U})$. Also a natural transformation $F \to G$ maps to a morphism in $\mathcal{F}_{desc}(\mathcal{U})$, so we get a functor $T : \mathrm{Hom}(h_{\mathcal{U}}, \mathcal{F}) \to \mathcal{F}_{desc}(\mathcal{U})$.

Conversely, choose an arbitrary choice of pullbacks(that coincide with $\xi_{ij} \to \xi_i$), for any arrow $f : T \to U \in h_{\mathcal{U}}(T)$, we choose a U_i that $T \to U$ factors as $T \to U_i \to U$(also for $f = \mathrm{id}_{U_i}$, choose

U_i), then define $F(f)$ as the pullback of ξ_i along $T \to U_i$. For any morphisms $T' \to T \to U \in h_{\mathcal{U}}$ and their choice of U_i, U_j that $T' \to U$ factors through $U_j \to U$ and $T \to U$ factors as $U_i \to U$, then $T' \to U_j$ factors through U_{ij}, i.e. we have a commutative diagram

$$\begin{array}{ccccc} T' & \longrightarrow & U_{ij} & \longrightarrow & U_j \\ \downarrow & & \downarrow & & \downarrow \\ T & \longrightarrow & U_i & \longrightarrow & U \end{array} .$$

Then by Cartesian properties, we get a unique map $F(T') \to F(T)$, which is Cartesian by(4.2.3.8). It can be shown these maps make F a functor, using Cartesian property and the existence of ξ_{ijk}. And also for any map of descent datum, we get a natural transformation in $\mathrm{Hom}(h_{\mathcal{U}}, \mathcal{F})$. Thus we get a functor $S : \mathcal{F}_{desc}(\mathcal{U}) \to \mathrm{Hom}(h_{\mathcal{U}}, \mathcal{F})$.

The construction of S shows T is essentially surjective and full, and also faithful, so (S, T) is an equivalence of categories. □

Def. (6.1.3.3) [Everyday Descent Datums]. Let $\mathcal{F}/\mathcal{C}$ be a fibered category on a site $\mathcal{C}$, $U \in \mathcal{C}$ and $\mathcal{U}$ is a covering of U. Given a choice of fibered products U_{ij}, U_{ijk} in $\mathcal{C}$ and a cleavage of $\mathcal{F}/\mathcal{C}$, let $\mathcal{F}(\mathcal{U})$ be the category of tuples (ξ_i, φ_{ij}) where $\xi_i \in \mathcal{F}(U_i)$ and φ_{ij} are isomorphisms $\varphi_{ij} : \mathrm{pr}_1^* \xi_i \cong \mathrm{pr}_2^* \xi_j \in \mathcal{F}(U_{ij})$ s.t.

$$\mathrm{pr}_{13}^* \varphi_{ik} = \mathrm{pr}_{23}^* \varphi_{jk} \circ \mathrm{pr}_{12}^* \varphi_{ij} : \mathrm{pr}_1^* \xi_i \cong \mathrm{pr}_3^* \xi_k.$$

WARNING: Notice this doesn't make sense unless we insect three isomorphisms such as $\mathrm{pr}_{12}^* \mathrm{pr}_1^* \xi_i \cong \mathrm{pr}_{13}^* \mathrm{pr}_1^* \xi_i$.

Then there is a (non-canonical!)equivalence of categories $\mathcal{F}_{desc}(\mathcal{U}) \to \mathcal{F}(\mathcal{U})$. ⌟

Proof: For $(\xi_i, \xi_{ij}, \xi_{ijk}) \in \mathcal{F}_{desc}(\mathcal{U})$, there are isomorphisms $\xi_{ij} \cong \mathrm{pr}_1^* \xi_i$ and $\xi_{ij} \cong \mathrm{pr}_2^* \xi_j$, which gives an isomorphism $\varphi_{ij} : \mathrm{pr}_1^* \xi_i \to \mathrm{pr}_2^* \xi_j$. This gives an element of $\mathcal{F}(\mathcal{U})$, by comparison with ξ_{ijk}.

Conversely, given $(\xi_i, \varphi_{ij}) \in \mathcal{F}(\mathcal{U})$, choose an ordering on I, for $i < j$, let $\xi_{ij} = \mathrm{pr}_1^* \varphi_i$, and $\mathrm{pr}_2^* \circ \varphi_{ij} : \xi_{ij} \to \xi_j$ is Cartesian. And for $i < j < k$, let $\xi_{ijk} = \mathrm{pr}_1^* \xi_i$, then there are Cartesian morphisms $\xi_{ijk} \to \xi_{ij}, \xi_{ijk} \to \xi_{ik}, \xi_{ijk} \to \xi_{jk}$ by Cartesian properties, and it can be verified that the cocycle condition guarantees the diagram can be completed. □

Cor. (6.1.3.4) [Cocycle Conditions]. If $\mathcal{F}/\mathcal{C}$ is a rigid fibered category, then there is no need to check the cocycle condition, because every automorphism over id_U is trivial. ⌟

Cor. (6.1.3.5) [Stacks and Sheaves]. A rigid (pre)stack over a site $\mathcal{C}$ is equivalent to a (pre)sheaf on $\mathcal{C}$, by(4.2.3.28). ⌟

Cor. (6.1.3.6). A site is subcanonical iff any representable fibered category $h_U \to C$ is a stack. ⌟

Prop. (6.1.3.7) [Equivalence Categories and Stacks]. Let $\mathcal{F} \to \mathcal{G}$ be an equivalence of fibered categories over a site $\mathcal{C}$, then $\mathcal{F}$ is a prestack/stack(in groupoid) iff $\mathcal{G}$ is. ⌟

Proof: There is a strict commutative diagram of categories

$$\begin{array}{ccc} \mathrm{Hom}(h_U, \mathcal{F}) & \longrightarrow & \mathrm{Hom}(h_{\mathcal{U}}, \mathcal{F}) \\ \downarrow & & \downarrow \\ \mathrm{Hom}(h_U, \mathcal{G}) & \longrightarrow & \mathrm{Hom}(h_{\mathcal{U}}, \mathcal{G}) \end{array}$$

that the vertical arrows are equivalences of categories, then we are done. □

Prop. (6.1.3.8) [Prestack and Hom Functor]. Let $\mathcal{F}$ be a fibered category over a site $\mathcal{C}$, then $\mathcal{F}$ is a prestack iff for any object S of $\mathcal{C}$ and two objects $\xi,\eta\in\mathcal{F}(S)$, the presheaf $\underline{\mathrm{Hom}}_S(\xi,\eta):(\mathcal{C}/S)^{op}\to\mathcal{S}et$(4.2.3.19) is a sheaf in the comma site $\mathcal{C}/S$(6.1.1.4). ⌟

Proof: By(6.1.3.7), it suffices to show $\mathcal{H}om_S(\xi,\eta)$ is a stack in the comma topology $\mathcal{C}/S$. Then it can be shown that $\mathrm{Hom}(h_U,\underline{\mathrm{Hom}}_S(\xi,\eta))\to\mathrm{Hom}(h_{\mathcal{U}},\underline{\mathrm{Hom}}_S(\xi,\eta))$ is an equivalence of categories iff $\mathrm{Hom}(h_U,\mathcal{F})\to\mathrm{Hom}(h_{\mathcal{U}},\mathcal{F})$ is fully faithful. □

Lemma (6.1.3.9). Let $\mathcal{F}$ be a prestack over a site $\mathcal{C}$, S,S' be sieves belonging to the topology of $\mathcal{C}$ that $S'\subset S$, then the restriction functor

$$\mathrm{Hom}_{\mathcal{C}}(S,\mathcal{F})\to\mathrm{Hom}_{\mathcal{C}}(S',\mathcal{F})$$

is faithful. ⌟

Proof: it suffices to show for $S'=h_{\mathcal{U}}$ for some covering $\mathcal{U}$. Let $F,G\in\mathrm{Hom}_{\mathcal{C}}(S',\mathcal{F})$ and φ,ψ be two natural transformations from F to G that induce the same natural transformation from the restriction of F to $h_{\mathcal{U}}$ to the restriction of G to $h_{\mathcal{U}}$, then $\varphi=\psi$. For this, just notice there are commutative diagrams

$$\begin{array}{ccc} F(T\times_U U_i/U) & \xrightarrow{\varphi_{T\times_U U_i/U}} & G(T\times_U U_i/U) \\ \downarrow & & \downarrow \\ F(T/U) & \xrightarrow{\varphi_{T/U}} & G(T/U) \end{array},$$

where the vertical arrows are Cartesian, and the hypothesis implies $\varphi_{T\times_U U_i/U}=\psi_{T\times_U U_i/U}$. Then we deduce $\varphi_{T/U}=\psi_{T/U}$ as $\underline{\mathrm{Hom}}_T(F(T/U),G(T/U))$ is a sheaf, as $\mathcal{F}$ is a presheaf(6.1.3.8). □

Prop. (6.1.3.10) [Stack and Sieves]. A prestack $\mathcal{F}\to\mathcal{C}$ is stack iff for any $U\in\mathcal{C}$ and any sieve $\mathcal{S}$ on U belonging to $\mathcal{T}$,

$$\mathrm{Hom}(h_U,\mathcal{F})\to\mathrm{Hom}(\mathcal{S},\mathcal{F})$$

is an equivalence of categories. ⌟

Proof: Let $\mathcal{S}$ be a sieve on U belong to $\mathcal{C}$, choose a covering $\mathcal{U}$ of U that $h_{\mathcal{U}}\subset\mathcal{S}\subset h_U$, then there is a factorization

$$\mathrm{Hom}(h_{\mathcal{U}},\mathcal{F})\to\mathrm{Hom}(\mathcal{S},\mathcal{F})\to\mathrm{Hom}(h_U,\mathcal{F}).$$

Then we are done by(6.1.3.9). □

Cor. (6.1.3.11). let $\mathcal{T},\mathcal{T}'$ be two topologies on a category $\mathcal{C}$ that T' is subordinate to $\mathcal{T}$ and $\mathcal{F}\to C$ is a fibered category, then if $\mathcal{F}$ is a prestack/stack relative to $\mathcal{T}$, it is also true for $\mathcal{T}'$. ⌟

Prop. (6.1.3.12)[2-Fiber Products of Stacks]. There is a natural 2-category of stacks over $\mathcal{C}$ defined as a sub-2-category of the 2-category of fibered-categories over $\mathcal{C}$, and the $(2,1)$-category of stacks over $\mathcal{C}$ has 2-fibered products, which coincides with that of(4.2.3.15). ⌟

Proof: Let $\mathcal{X}\to\mathcal{S},\mathcal{Y}\to\mathcal{S}$ be morphisms of stacks over $\mathcal{C}$, then the category $\mathcal{X}\times_{\mathcal{S}}\mathcal{Y}$ is a fibered category over $\mathcal{C}$, by(4.2.3.15). It remains to show that the morphism presheaves sheaves and descent datum are effective.

For this, Cf.[Sta]026G. □

Prop. (6.1.3.13) [Associated Stack in Groupoids]. Let $\mathcal{C}$ be a site and $\mathcal{F}$ be a prestack, and $\mathcal{F}_{cart}$ is the associated category fibered in groupoids(4.2.3.24), then $\mathcal{F}_{cart}$ is also a prestack. And in this case, $\mathcal{F}$ is a stack iff $\mathcal{F}_{cart}$ is a stack. ⌟

Proof: The categories $\mathcal{F}(\mathcal{U})$ and $\mathcal{F}_{cart}(\mathcal{U})$ have the same isomorphism classes of objects, as isomorphisms are Cartesian, so it suffices to show $\mathcal{F}$ is a prestack iff $\mathcal{F}_{cart}$ is a prestack. For this, use(6.1.3.8) and consider $\xi, \eta \in \mathcal{F}(U)$ and a covering $\{U_i \to U\}$, if there are arrows $\alpha_i : \xi_i \to \eta_i$ that are compatible, then there is a unique arrow $\alpha : \xi \to \eta$ restricting to α_i, thus it suffices to show α is Cartesian. But since $\mathcal{F}_{cart}$ is a category fibered in groupoids, each α_i is invertible, and their inverses glue together to a morphism $\beta : \eta \to \xi$ which is the inverse of α, so α is also an isomorphism thus Cartesian. □

Prop. (6.1.3.14) [2-Fibered Products of Stacks Fibered in Groupoids]. Let $\mathcal{C}$ be a category, the 2-category of stacks fibered in groupoids over $\mathcal{C}$(automatically a $(2,1)$-category) has 2-fiber products, and coincide with that of(6.1.3.12). ⌟

Proof: This is clear from(6.1.3.12) and(4.2.3.26). □

Prop. (6.1.3.15) [Equivalence of Stacks]. Let $F : \mathcal{S}_1 \to \mathcal{S}_2$ be a morphism of stacks over a site $\mathcal{C}$. If F is fully faithful, then F is an equivalence iff for any $x \in \mathcal{S}_{2,U}$, there exists a covering $\{f_i : U_i \to U\}$ s.t. $f_i^* x$ is in the essential image of the functor $F : \mathcal{S}_{1,U} \to \mathcal{S}_{2,U}$. ⌟

Proof: Easy. □

Prop. (6.1.3.16) [Subcanonical Site Prestack]. If $\mathcal{C}$ is a subcanonical site(6.1.2.4) and $\mathcal{P}$ is a class of arrows in $\mathcal{C}$ stable under base change, then the corresponding fibered category $\mathcal{P} \to \mathcal{C}$ is a prestack. ⌟

Proof: By(6.1.3.8), we need to prove for any covering $\{U_i \to U\}$ and arrows $X \to U, Y \to U$, $X_i = U_i \times_U X$, and $X_{ij} = U_{ij} \times_U X$ and analogous for Y, if there are arrows $f_i : X_i \to Y_i$ over U_i that the arrows $X_{ij} \to Y_{ij}$ induced by f_i and f_j coincide, then there is a unique arrow $f : X \to Y$ over U that induces f_i.

Notice that the composite $X_i \xrightarrow{f_i} Y_i \to Y$ give sectiosn $g_i \in h_Y(X_i)$, and the pullback of g_i, g_j to X_{ij} coincide by hypothesis. Now h_Y is a sheaf by hypothesis, so there is an arrow $f : X \to Y$ that pulls back to f_i on X_i. Finally f is compatible over U because $(Y \to U) \circ f$ and $(X \to U)$ coincide when composed with $X_i \to X$, and h_U is a sheaf. □

Prop. (6.1.3.17) [Category of Sheaves is a Stack]. Let $\mathcal{C}$ be a site, we denote $(\mathcal{S}\mathrm{h}/\mathcal{C})(X) = \mathcal{S}\mathrm{h}(\mathcal{C}/X)$, then $\mathcal{S}\mathrm{h}/\mathcal{C}$ is a stack over $\mathcal{C}$. ⌟

Proof: To show $Sh/\mathcal{C}$ is a prestack, by(6.1.3.8), it suffices to show for any $F, G \in \mathcal{S}\mathrm{h}(\mathcal{C}/X)$, $\underline{\mathrm{Hom}}_X(F, G)$ is a sheaf. For this, let $\{U_i \to U\}$ be a covering, and $\varphi_i : F_{U_i} \to G_{U_i}$ be morphisms of sheaves that their restrictions to $F_{U_{ij}} \to \mathcal{G}_{U_{ij}}$ are compatible, then for any $T \to U$, there are commutative diagrams

$$\begin{array}{ccccc} F(T) & \longrightarrow & \prod_i F_i(T_i) & \longrightarrow & \prod_{i,j} F_{ij}(T_{ij}) \\ \downarrow & & \downarrow & & \downarrow \\ G(T) & \longrightarrow & \prod_i G_i(T_i) & \longrightarrow & \prod_{i,j} G_{ij}(T_{ij}) \end{array}$$

where $\varphi_T : F(T) \to G(T)$ is the unique function of sets that makes the diagram commutative. And it can be shown that these φ_T defines a natural transformation $F_U \to G_U$.

Now for any covering $\{U_i \to U\}$ and a descent datum (F_i, F_{ij}), we need to show it is effective. We define a function F on $\mathcal{C}/U$: $F(T) = \mathrm{equal}(\prod_i F(T_i) \rightrightarrows \prod_{ij} F(T_{ij}))$, then it can be shown that this is a sheaf by spectral seqence.

Then it suffices to check $F_{U_k} = F_k$. For any $T \to U_k$, T_i maps to U_{ik}, so $F_i(T_i) = F_k(T_i)$, thus for any $s \in F_k(T)$, we can produce an element $(s_{T_i}) \in \prod_i F_i(T_i)$ that satisfies compatibility conditions, which gives us an element of $F(T)$. It can be shown this is a natural transformation $F_k \to F_{U_k}$, and it is an isomorphism of sheaves. □

Prop. (6.1.3.18)[Descent Along Torsors]. Let $\mathcal{C}$ be a site, G a group object and $X \to Y$ a G-torsor, $\mathcal{F} \to \mathcal{C}$ a stack. Then there exists a canonical equivalence of categories between $\mathcal{F}(Y)$ and the category of G-equivariant objects $\mathcal{F}^G(X)$(4.2.3.17). ⌟

Proof: By(6.1.1.17) $X \to Y$ is refined by a covering, thus by(6.1.3.10), $\mathcal{F}(Y)$ is equivalent to $\mathcal{F}(X \to Y)$. And we check $\mathcal{F}(X \to Y) \cong \mathcal{F}^G(X)$. Then by(6.1.1.18), $\mathcal{F}(X \to Y)$ consists of elements $\xi \in \mathcal{F}(X), \eta \in \mathcal{F}(G \times X)$ and Cartesian arrows φ_1, φ_2 over α, π_2. Cf.[Vis08]P106.**?** □

Stackifications

Prop. (6.1.3.19)[Stackification]. Let $\mathcal{C}$ be a site and $p : \mathcal{F} \to \mathcal{C}$ a fibered category over $\mathcal{C}$, then there exists a stack $p' : \mathcal{F}' \to \mathcal{C}$ and a morphism $G : \mathcal{F} \to \mathcal{F}'$ of fibered categories over $\mathcal{C}$ s.t. for any stack $\mathcal{X} \to \mathcal{C}$, a morphism $F : \mathcal{F} \to \mathcal{X}$ of fibered categories over $\mathcal{C}$ factors through G 2-commutatively and uniquely up to 2-isomorphisms. In other words, there is a canonical equivalence of categories:

$$\mathrm{Mor}_{Fib/\mathcal{C}}(\mathcal{F}, \mathcal{X}) \cong \mathrm{Mor}_{\mathfrak{Sta}/\mathcal{C}}(F', \mathcal{X}).$$

In particular, such a stack $\mathcal{F}'$ is determined up to unique 2-isomorphisms, and is called the **stackification** of $\mathcal{F}$. ⌟

Proof: By(4.2.3.20), we may assume $\mathcal{F}$ is split, thus $\mathcal{F}$ corresponds to the functor $\mathcal{C}^{op} \to Cat : U \mapsto \mathrm{Hom}(h_U, \mathcal{F})$. Then we define a functor

$$\mathcal{F}' : \mathcal{C}^{op} \to \mathfrak{Cat} : U \mapsto \varinjlim_{\mathcal{U} \in \mathrm{Cov}(U)} \mathrm{Hom}(h_{\mathcal{U}}, \mathcal{F}).$$

then there is a natural map of fibered categories $\mathcal{F} \to \mathcal{F}'$. For any stack $\mathcal{X} \to C$, because $\mathrm{Hom}(h_U, \mathcal{X}) \to \mathrm{Hom}(h_{\mathcal{U}}, \mathcal{X})$ is an isomorphism for any covering $\mathcal{U}$ of U, we get the desired equivalence of categories. □

Cor. (6.1.3.20). Let $G : \mathcal{S} \to \mathcal{S}'$ be the stackification of a fibered category over $\mathcal{C}$, then

- For any $U \in \mathcal{C}$ and $x, y \in \mathcal{S}_U$, the map

$$\mathcal{H}om(x, y) \to \mathcal{H}om(G(x), G(y))$$

  identifies the RHS as the shifification of the LHS.
- For any $U \in \mathcal{C}$ and $x \in \mathcal{S}'_U$, there exists a covering $\{U_i \to U\}$ that for any i, $x|_{U_i}$ is in the essential image of $G_U : \mathcal{S}_U \to \mathcal{S}'_U$.

⌟

Proof: Cf.[Sta]0435. □

Prop. (6.1.3.21) [Stackifications Commute with 2-Fibered Products]. Stackifications commute with 2-fibered products. ⌟

Proof: Cf.[Sta]04Y1. □

Prop. (6.1.3.22). If $\mathcal{F}, \mathcal{G}$ are prestacks over a topological space X, if there is a morphism $\eta : \mathcal{F} \to \mathcal{G}$ that satisfies:

- $\mathcal{F}$ is a stack and $\mathcal{G}$ is a prestack.
- η induces isomorphisms on stalks.
- $\eta(U) : \mathcal{F}(U) \to G(U)$ is fully faithful.

Then η is an equivalence of prestacks. In particular, $\mathcal{G}$ is also a stack. ⌟

Proof: Let $\mathcal{H}$ be the stackification of $\mathcal{G}$, then $\mathcal{F} \to \mathcal{G} \to \mathcal{H}$ is a morphism of stacks that is isomorphism on the stalk, so it is an isomorphism?. But G is separated, so for any open U, $\mathcal{F}(U) \to \mathcal{G}(U)$, $\mathcal{G}(U) \to \mathcal{H}(U)$ is fully faithful, and their composition is an equivalence, thus both of them are equivalences. □

Gerbes

Def. (6.1.3.23) [Gerbe]. Let $\mathcal{C}$ be a site, a **gerbe** over $\mathcal{C}$ is a stack in groupoids over $\mathcal{C}$ s.t.

- For any $U \in \mathcal{C}$, there is a covering $\{U_i \to U\}$ that S_{U_i} is nonempty for any i.
- For any $U \in \mathcal{C}$ and $x, y \in \mathcal{S}_U$, there exists a covering $\{U_i \to U\}$ that $x|_{U_i} = y|_{U_i}$ for any i.

⌟

Prop. (6.1.3.24). Let $p : \mathcal{S} \to \mathcal{C}$ be a gerbe over a site $\mathcal{C}$, assume that for all $U \in \mathcal{C}$ and $x \in \mathcal{S}_U$, the sheaf of groups $\mathrm{Aut}(x)$ on $\mathcal{C}/U$ is Abelian, then there exists a sheaf of Abelian groups over $\mathcal{C}$ and for any $x \in \mathcal{S}_U$ an isomorphism $\mathcal{G}|_U \to \mathrm{Aut}(x)$ that for any morphism $\varphi : x \to y \in \mathcal{S}_U$, the diagram

$$\begin{array}{ccc} \mathcal{G}|_U & = & \mathcal{G}|_U \\ \downarrow & & \downarrow \\ \mathrm{Aut}(x) & \xrightarrow{\alpha \mapsto \varphi\circ\alpha\circ\varphi^{-1}} & \mathrm{Aut}(y) \end{array}$$

is commutative. ⌟

Proof: It can be checked by using the fact $\mathrm{Aut}(x)$ is Abelian that there are canonical morphisms $\mathrm{Aut}(x) \to \mathrm{Aut}(y)$ induced by any morphism $\varphi : x \to y$.

If there is no morphism from x to y, then we can use the condition of gerbe to obtain morphisms $\mathrm{Aut}(x)|_{U_i} \to \mathrm{Aut}(y)|_{U_i}$ locally, and then glue together. Similarly, if $\mathcal{S}_U$ is empty, then we can restrict to a covering and then glue.

Finally, notice this gives an Abelian sheaf $\mathcal{G} = \mathrm{Aut}$ on $\mathcal{C}$. □

Bands

4 Sites over Schemes

Prop. (6.1.4.1). Fiber products exist in the category of schemes, by(6.2.7.15). ⌟

Zariski Topology

Def. (6.1.4.2) [Zariski Topology]. The **Zariski topology** has the the covering of a scheme T as classes of open immersions $\{T_i \to T\}$ that their images cover T.

The **Zariski site** $\mathcal{S}\text{ch}_{\text{Zar}}/S$ has the objects as all schemes over S.

The **small Zariski site** S_{Zar} has the objects as all open subschemes over S.

The **restricted Zariski site** $S_{\text{Zar}\,fp}$ has the objects as all schemes that are qcqs open subschemes of S.

The **big affine Zariski site** $\mathcal{A}\text{ff}_{\text{Zar}}/S$ has the objects as all schemes affine over S.

These are all topologies because open immersions satisfies base change trick(6.4.4.60).

In particular when the cover has only one element and is affine, the descent datum is equivalent to compatible isomorphisms

$$\varphi_{13} : N \otimes_A B \otimes_A B \xrightarrow{\varphi_{12}} B \otimes_A M \otimes_B \xrightarrow{\varphi_{23}} B \otimes_A B \otimes_A M.$$

⌟

Def. (6.1.4.3) [Zariski Stacks]. The category of sheaves on $\mathcal{S}\text{ch}_{\text{Zar}}/S$ is denoted by $\mathcal{S}\text{h}_{\text{Zar}}/S$. The category of stacks on $\mathcal{S}\text{ch}_{\text{Zar}}/S$ is denoted by $\mathcal{S}\text{ta}_{\text{Zar}}/S$. ⌟

Prop. (6.1.4.4) [Affine and Full Sites]. The inclusion functor $\mathcal{A}\text{ff}_{\text{Zar}}/S \to \mathcal{S}\text{ch}_{\text{Zar}}/S$ is a special cocontinuous functor, so by(6.1.2.24), it induces an equivalence of topoi $\mathcal{S}\text{h}(\mathcal{A}\text{ff}_{\text{Zar}}/S) \cong \mathcal{S}\text{h}_{\text{Zar}}/S$. ⌟

Def. (6.1.4.5) [Restriction to Small Sites]. The inclusion functor $S_{\text{Zar}} \to \mathcal{S}\text{ch}_{\text{Zar}}/S$ satisfies the hypothesis of(6.1.2.23), thus induces morphisms of topoi

$$\pi_S : \mathcal{S}\text{h}_{\text{Zar}}/S \to \mathcal{S}\text{h}(S_{\text{Zar}}), \quad i_S : \mathcal{S}\text{h}(S_{\text{Zar}}) \to \mathcal{S}\text{h}_{\text{Zar}}/S$$

that satisfies $\pi_S \circ i_S = \text{id}_{S_{\text{Zar}}}$. In particular, $i_S^{-1}\mathcal{F}$ is called the **restriction to small sites** of $\mathcal{F}$. ⌟

Prop. (6.1.4.6). A sheaf w.r.t the small Zariski topology is equivalent to a sheaf on S, trivially, so the sheaf cohomology on $\mathcal{A}\text{ff}_{\text{Zar}}/S$ is equivalent to usual sheaf cohomology on S. ⌟

Prop. (6.1.4.7) [Transfer of Big Sites]. Let $f : T \to S \in \mathcal{S}\text{ch}_{\text{Zar}}/S$, then $\mathcal{S}\text{ch}_{\text{Zar}}/T \to \mathcal{S}\text{ch}_{\text{Zar}}/S$ is a localization, so by(6.1.2.22) it induces a morphism of topoi

$$f : \mathcal{S}\text{h}_{\text{Zar}}/T \to \mathcal{S}\text{h}_{\text{Zar}}/S : f^{-1}\mathcal{G}(U/T) = \mathcal{G}(U/S), \quad f_*\mathcal{F}(U/S) = \mathcal{F}(U \times_S T/T).$$

⌟

Prop. (6.1.4.8) [Transfer of Small Sites]. Let $f : T \to S \in \mathcal{S}\text{ch}_{\text{Zar}}/S$, then the base change functor $S_{\text{Zar}} \to T_{\text{Zar}}$ is continuous, and by(6.1.2.14) induces a morphism of topoi

$$f : \mathcal{S}\text{h}_{\text{Zar}}/T \to \mathcal{S}\text{h}_{\text{Zar}}/S.$$

⌟

Prop. (6.1.4.9). By(6.3.1.15), if X is qs, then $\mathcal{S}\text{h}(X_{\text{Zar}}) \to \mathcal{S}\text{h}(X_{\text{Zar}\,fp})$ is an equivalence by i_s and i^s. ⌟

Étale Topology

Def. (6.1.4.10) [Étale Topology]. The **étale topology** has the covering of a scheme T as classes of étalemorphisms that their images cover T.

The **étale site** $\mathcal{S}\mathrm{ch}_{\text{ét}}/S$ has the objects as all schemes over S.

The **small étale site** $S_{\text{ét}}$ has the objects as all schemes that are étale over S.

The **restricted étale site** $S_{\text{ét}\,fp}$ has the objects as all schemes that are étale and qcqs over S.

The **big affine étale site** $\mathcal{A}\mathrm{ff}_{\text{ét}}/S$ has the objects as all schemes affine over S.

These are truly topologies because étale is stable under base change and composition. ⌟

Prop. (6.1.4.11). Zariski covering is étale , because open immersions are étale. ⌟

Prop. (6.1.4.12). For a family of maps in $S_{\text{ét}}$ to be a covering, it suffices to check their image is adjointly surjective, by(6.6.6.4). ⌟

Prop. (6.1.4.13) [Affine and Full Sites]. The inclusion functor $\mathcal{A}\mathrm{ff}_{\text{ét}}/S \to \mathcal{S}\mathrm{ch}_{\text{ét}}/S$ is a special cocontinuous functor, so by(6.1.2.24), it induces an equivalence of topoi $\mathcal{S}\mathrm{h}(\mathcal{A}\mathrm{ff}_{\text{ét}}/S) \cong \mathcal{S}\mathrm{h}_{\text{ét}}/S$. ⌟

Def. (6.1.4.14) [Restriction to Small Sites]. The inclusion functor $S_{\text{ét}} \to \mathcal{S}\mathrm{ch}_{\text{ét}}/S$ satisfies the hypothesis of(6.1.2.23), thus induces morphisms of topoi

$$\pi_S : \mathcal{S}\mathrm{h}_{\text{ét}}/S \to \mathcal{S}\mathrm{h}(S_{\text{ét}}), i_S : \mathcal{S}\mathrm{h}(S_{\text{ét}}) \to \mathcal{S}\mathrm{h}_{\text{ét}}/S$$

that satisfies $\pi_S \circ i_S = \mathrm{id}_{S_{\text{ét}}}$. In particular, $i_S^{-1}\mathcal{F}$ is called the **restriction to small sites** of $\mathcal{F}$. ⌟

Prop. (6.1.4.15). Any étale covering of a qc scheme can be refined a finite covering by affine étale schemes, this is because étale map are open(6.6.6.3). ⌟

Def. (6.1.4.16) [Étale Stacks]. The category of sheaves on $\mathcal{S}\mathrm{ch}_{\text{ét}}/S$ is denoted by $\mathcal{S}\mathrm{h}_{\text{ét}}/S$. The category of stacks on $\mathcal{S}\mathrm{ch}_{\text{ét}}/S$ is denoted by $\mathcal{S}\mathrm{ta}_{\text{ét}}/S$. ⌟

Prop. (6.1.4.17). For a qc scheme X, $X_{\text{ét}\,fp}$ is a Noetherian topology, because étale map is open, and any object in $X_{\text{ét}\,fp}$ is qc. ⌟

Prop. (6.1.4.18) [Transfer of Big Sites]. Let $f : T \to S \in \mathcal{S}\mathrm{ch}_{\text{ét}}/S$, then the functor $u : \mathcal{S}\mathrm{ch}_{\text{ét}}/T \to \mathcal{S}\mathrm{ch}_{\text{ét}}/S$ is cocontinuous, and has base change as a right adjoint, so by(6.1.2.22) it induces a morphism of topoi

$$f : \mathcal{S}\mathrm{h}_{\text{ét}}/T \to \mathcal{S}\mathrm{h}_{\text{ét}}/S : f^{-1}\mathcal{G}(U/T) = \mathcal{G}(U/S), \quad f_*\mathcal{F}(U/S) = \mathcal{F}(U \times_S T/T).$$

⌟

Prop. (6.1.4.19) [Transfer of Small Sites]. Let $f : T \to S \in \mathcal{S}\mathrm{ch}_{\text{ét}}/S$, then the base change functor $S_{\text{ét}} \to T_{\text{ét}}$ is continuous, and by(6.1.2.14) induces a morphism of topoi

$$f : \mathcal{S}\mathrm{h}(T_{\text{ét}}) \to \mathcal{S}\mathrm{h}(S_{\text{ét}})$$

⌟

Prop. (6.1.4.20). If X is qs, then $\mathcal{S}\mathrm{h}(X_{\text{ét}}) \to \mathcal{S}\mathrm{h}(X_{\text{ét}\,fp})$ is an equivalence by i_s and i^s. ⌟

Proof: Want to use(6.1.2.25), one condition is satisfied by(6.1.4.15), so it suffice to check any $X' \in X_{\text{ét}}$ has an étale covering by schemes étale and qcqs over X. For any point $p \in X'$, there is an affine nbhd U' that maps to an affine nbhd U' of X, so $U' \to U$ is étaleand qcqs, and $U \to X$ is open immersion and qs, it is qc because X is qs and U is qc(6.4.4.27). So these affine nbhds U' cover X'. □

Prop. (6.1.4.21) [Cohomology Big and Small Sites]. The inclusion of small sites to the big sites has no infection on the sheaf cohomology, by(6.3.1.4). This is applicable to all topologies τ considered here. ⌟

Prop. (6.1.4.22) [Topological Invariance of Étale Sites]. If $f : S' \to S$ is universally homeomorphism, then $f : S'_{\text{ét}} \to S_{\text{ét}}$ is an equivalence of sites.

In particular this applies to $S' = S_{\text{red}}$. ⌟

Proof: Cf.[Étale Cohomology Conrad P18]. □

Smooth Topology

This topology will be shown to be identical to the étale topology, so it is not so important.

Def. (6.1.4.23)[Smooth Topology]. The **smooth topology** has the covering of a scheme T as classes of smooth morphisms that their images cover T.

The **big smooth site** $\mathcal{S}\text{ch}_{\text{sm}}/S$ has the objects as all schemes over S.

The **small smooth site** S_{sm} has the objects as all schemes that are smooth over S.

The **restricted smooth site** $S_{\text{ét}\,fp}$ has the objects as all schemes that are smooth and qcqs over S.

The **big affine smooth site** $\mathcal{A}\text{ff}_{\text{ét}}/S$ has the objects as all schemes affine over S.

These are truly topologies because smoothness is stable under base change and composition. ⌟

Syntomic Topology

Def. (6.1.4.24) [Syntomic Topology]. The **syntomic topology** has the covering of a scheme T as classes of syntomic morphisms that their images cover T. ⌟

fppf Topology

Def. (6.1.4.25)[Fppf Topology]. The **fppf topology** has the covering of a scheme T as classes of flat locally of finite presentation morphisms that their images cover T. (f.f.+locally of f.p.).

The **big Zariski site** $\mathcal{S}\text{ch}_{\text{fppf}}/S$ has the objects as all schemes over S.

The **big affine Zariski site** $\mathcal{A}\text{ff}_{\text{fppf}}/S$ has the objects as all schemes affine over S.

They are all topologies because flatness and finite presentedness satisfy base change trick by(6.6.2.1) and(6.6.1.1). ⌟

Prop. (6.1.4.26) [Syntomic Covering is Fppf]. A syntomic covering is fppf by definition(5.4.4.18). ⌟

Prop. (6.1.4.27). A fppf covering of an affine scheme can be refined a finite affine fppf covering, because fppf map are open(6.6.2.10). ⌟

Def. (6.1.4.28) [Fppf Stacks]. The category of sheaves on $\mathcal{S}\text{ch}_{\text{fppf}}/S$ is denoted by $\mathcal{S}\text{h}_{\text{fppf}}/S$. The category of stacks on $\mathcal{S}\text{ch}_{\text{fppf}}/S$ is denoted by $\mathcal{S}\text{ta}_{\text{fppf}}/S$. ⌟

fpqc Topology

Def. (6.1.4.29) [Fpqc Topology]. The **fpqc topology** has the covering of a scheme T as classes of flat morphisms s.t. their images cover T and for any affine open $U \subset T$, the restriction on T can be refined by a finite affine cover of open affine subschemes of the covering(f.f.+qc). It is a topology by(6.6.2.1) and(6.4.4.25).

When the covering consists of affine schemes, it is called a **standard fpqc covering**. ⌟

Def. (6.1.4.30) [Fpqc Stacks]. Defining fpqc sites has inescapable set-theoretic difficulties, thus we don't consider fpqc sites and fpqc cohomologies. Cf.[Sta]0BBK.

Nevertheless, we will denote the category of presheaves on $\mathcal{S}\mathrm{ch}/S$ satisfying the sheaf condition w.r.t. the fpqc topology by $\mathcal{S}\mathrm{h}_{\mathrm{fpqc}}/S$, and denote the category of fibered categories over $\mathcal{S}\mathrm{ch}/S$ satisfying the sheaf condition w.r.t. the fpqc topology by $\mathcal{S}\mathrm{ta}_{\mathrm{fpqc}}/S$. ⌟

Prop. (6.1.4.31) [fppf is fpqc]. Fppf coverings are fpqc. ⌟

Proof: Use(6.6.2.10), we see that fppf covering consists of open morphisms, thus it is qc because affine scheme is quasi-compact. □

Prop. (6.1.4.32). A covering consisting of flat morphisms refined by a fpqc covering is a fpqc covering.

Hence being fpqc is local on the target, because a Zariski cover is a fpqc covering.

If U is a covering consisting of flat morphisms that there is a fpqc covering V that $U \times V \to V$ is a fpqc covering, then U is fpqc, because $U \times V$ does and it refines U. ⌟

Lemma (6.1.4.33) [Checking Sheaf Condition]. Let $S \in \mathcal{S}\mathrm{ch}$, $F \in \mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}((\mathcal{S}\mathrm{ch}_S)_{\mathrm{fpqc}})$ is a sheaf iff it is a sheaf w.r.t the Zariski topology and satisfies sheaf property w.r.t the single covering $V \to U$ f.f. between affine schemes. ⌟

Proof: This follows from(6.1.3.5)(6.1.3.6) and(6.1.5.7). □

Prop. (6.1.4.34) [fpqc Site is Subcanonical]. The coverings in $(\mathcal{S}\mathrm{ch}_S)_{\mathrm{fpqc}}$ are families of universal effective epimorphisms. In other words, $(\mathcal{S}\mathrm{ch}_X)_{\mathrm{fpqc}}$ is subcanonical.

In particular, for any covering $\mathcal{U} = \{U_i \to X\} \in \mathrm{Cov}((\mathcal{S}\mathrm{ch}_S)_{\mathrm{fpqc}})$ and $\{V_{ijk} \to U_i \times_X U_j\} \in \mathrm{Cov}((\mathcal{S}\mathrm{ch}_S)_{\mathrm{fpqc}})$,

$$X = \mathrm{Coeq}(\coprod_{i,j,k} V_{ijk} \rightrightarrows \coprod_i U_i) \in \mathcal{S}\mathrm{ch}_S\,.$$

⌟

Proof: By(6.1.4.33), it suffices to show that any representable presheaf is a sheaf w.r.t Zariski topology and f.f. affine morphisms. The Zariski case follows from(6.1.5.3), for the second, $\mathrm{Spec}\,B \to \mathrm{Spec}\,Z$, for any scheme X, the morphism corresponds to $0 \to \mathrm{Hom}(R, A) \to \mathrm{Hom}(R, B) \to \mathrm{Hom}(R, B \otimes_A B)$, but this follows immediately from(5.4.2.2), with $M = A$. □

Cor. (6.1.4.35). For $f : Y \to X$ a morphism of schemes, if $Z \in X_\tau$ for the above topologies τ, then $f^*(\mathrm{Hom}_X(-, Z)) \cong \mathrm{Hom}(-, Z \otimes_X Y)$, in other words, the inverse sheaf of a representable sheaf is representable. ⌟

Proof: By definition, $f^*(\mathrm{Hom}_X(-, Z))$ is the sheaf associated to the presheaf $f_p(\mathrm{Hom}_X(-, Z))$, which by(6.1.2.13) is just the presheaf represented by $Z \otimes_X Y$, but by the proposition, it is already a sheaf. □

Prop. (6.1.4.36) [Coherent Sheaves on $\mathcal{S}\mathrm{ch}_{\mathrm{fpqc}}/X$]. Let $\mathcal{F} \in \mathfrak{QCoh}(X)$, then the functor $X' \to \Gamma(X', \mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_{X'})$ satisfies the the axiom for Abelian sheaves on $\mathcal{S}\mathrm{ch}_{\mathrm{fpqc}}/X$, by(6.1.5.13). ⌟

Prop. (6.1.4.37) [Qco Sheaves on Sites]. For $X \in \mathcal{S}\mathrm{ch}, \tau \in$ {fppf, étale, smooth, syntomic, Zariski}, restriction defines an equivalence of categories

$$\mathfrak{QCoh}(X) \cong \mathfrak{QCoh}(\mathcal{S}\mathrm{ch}_\tau/X).$$

And if $\tau \in$ {Zariski, étale}, restriction defines an equivalence of categories

$$\mathfrak{QCoh}(X) \cong \mathfrak{QCoh}(X_\tau).$$

⌟

Proof: Cf.[Sta]03DX. □

PH-Covering

Def. (6.1.4.38) [Standard PH-Covering]. ⌟

Def. (6.1.4.39) [PH-Topology]. ⌟

Prop. (6.1.4.40) [Zariski Covering is PH-Covering]. A Zariski covering is a PH-covering. ⌟

Proof: Cf.[[Sta]0DBH]. □

Prop. (6.1.4.41). A proper surjective morphism is a ph-covering. ⌟

Proof: Cf.[[Sta]0DES]. □

V-Topology

Def. (6.1.4.42) [Standard V-Covering]. A finite family of morphisms morphism $T_i \to X$ of affine schemes is a covering in the **standard v-topology** if for any morphism $\mathrm{Spec}\, V \to X$ where V is a valuation ring, there is an extension of valuation rings(11.2.2.11) $V \to W$ and a morphism $\mathrm{Spec}\, W \to \mathrm{Spec}\, V \times_X T_i$ for some i. ⌟

Def. (6.1.4.43) [V-Topology]. A family of morphisms $\{T_i \to T\}$ is called a **v-covering** in the **v-topology** if for any open affine subscheme U of T, the base change is refined by a standard v-covering of U.

The v-coverings form a topology, by[[Sta]0ETJ]. ⌟

Lemma (6.1.4.44). A standard fpqc covering is a standard v-covering. ⌟

Proof: Cf.[[Sta]022E]. □

Prop. (6.1.4.45) [fpqc Covering is v-Covering]. A fpqc covering is a v-covering. ⌟

Proof: This follows immediately from(6.1.4.44). □

Prop. (6.1.4.46). A standard ph-covering is a standard v-covering. ⌟

Proof: Cf.[[Sta]0ETD] □

Prop. (6.1.4.47) [ph-Covering is V-Covering]. A ph-covering is a v-covering. ⌟

Proof: This follows immediately from(6.1.4.46). □

Cor. (6.1.4.48). A proper and surjective map is a v-covering, by(6.1.4.47) and(6.1.4.41). ⌟

Arc-Topology

Def. (6.1.4.49) [Arc-Topology]. A finite family of morphisms $\{T_i \to X\}$ of schemes is a covering in the **arc-topology** if for any morphism $\operatorname{Spec} V \to X$ where V is a rank1-valuation ring, there is a rank1-valuation ring W and a morphism $\operatorname{Spec} W \to \operatorname{Spec} V \times_X T_i$ for some i that $V \to W$ is f.f.. ⌟

Prop. (6.1.4.50). V-coverings are arc coverings. ⌟

Proof: This is by the definition and(11.2.2.11). □

5 Descent for Algebraic Spaces

Main references are [Sta]Chap34, 10.158.

General Principal

Prop. (6.1.5.1). A property of schemes is called **local** in a topology if for any covering $\{U_i \to S\}$, S has P iff U_i has P. A property of morphisms is called **local** in a topology if for any covering $\{U_i \to S\}$, $X \to S$ has P iff $X \times_S U_i \to U_i$ has P. ⌟

Prop. (6.1.5.2) [Twists and Čech Cohomology]. Let ξ be an object of a stack $\mathcal{F}$ over a site $\mathcal{C}$ lying over an object U of $\mathcal{C}$, we call an object $\xi' \in \mathcal{F}(U)$ a **twist** of ξ if there is some covering $\{U_i \to U\}$ that the pullback of ξ and ξ' to $U_i \to U$ are isomorphic.

Then there is a natural bijection between $\mathcal{F}(U)$-isomorphism classes of twists of ξ with $\check{H}^1(U, \underline{\operatorname{Aut}}(\xi))$. ⌟

Proof: Cf.[Appendix of Lamb]. □

Zariski Descent

Lemma (6.1.5.3) [Zariski Descent of Qco Sheaves]. The fibered category $X \mapsto (\mathcal{QC}oh/X)$ is a stack over $\mathcal{S}ch_{\mathrm{Zar}}/S$. ⌟

Proof: This is a consequence of(6.1.3.17) and the fact quasi-coherentness is a Zariski local property. □

Prop. (6.1.5.4) [Zariski Descent of Schemes]. The fibered category $X \mapsto \mathcal{S}ch/X$ is in $\mathcal{S}ta_{\mathrm{Zar}}/S$. ⌟

Proof: Firstly it is a prestack by(6.1.3.16) and(6.1.4.34).

To show any descent datum of effective, let $\{U_i \to U\}$ be a Zariski covering, and $X_i \to U_i$ be schemes with descent datum $\varphi_{ij} : X_i \times_{U_i} U_{ij} \cong X_j \times_{U_j} U_{ij}$, then we define $X = \coprod X_i/\sim$, where $x_i \sim x_j$ if $x_i \in Uij, x_j \in U_{ji}$ and $\varphi_{ij}(x_i) = \varphi_{ji}(x_j)$. It can be shown this is an equivalence relation. Denote $\varphi_i : X_i \to X$ the natural map, and $U_i = \varphi_i(X_i)$. Define the topology on X as the quotient topology. In particular, φ_i is a homeomorphism onto the image. Then we can use(6.1.3.17) to glue the sheaves of rings $(\varphi_i)_*(\mathcal{O}_{X_i})$ to a sheaf of rings $\mathcal{O}_X$ on X that $\varphi_i^*\mathcal{O}_X = \mathcal{O}_{X_i}$. Also we have a map $f : X \to U$ by set-theoretical and topological consideration. For the structure map $f^{-1}(\mathcal{O}_U) \to \mathcal{O}_X$, use(6.1.3.17). □

Cor. (6.1.5.5). If $\mathcal{P}$ is a subclass of arrows of schemes that is stable under base change and local on the target, then $\mathcal{P}/S$ is a stack over $(\mathcal{S}ch/S)_{Zar}$. ⌟

Cor. (6.1.5.6) [Zariski Descent of Schemes with a Qco Sheaf]. The fibered category $X \mapsto$ {Schemes over X with a Qco sheaf $\mathcal{F}$} is a stack in the Zariski topology $\mathcal{S}ch_{Zar}/S$. ⌟

Proof: This is a combination of(6.1.5.4) and(6.1.5.3). □

Fpqc Descent

Prop. (6.1.5.7) [Reduction to Affine Case]. Let S be a scheme and $\mathcal{F}$ be a fibered category over $\mathcal{S}\mathrm{ch}\,/S$. Suppose that

- $\mathcal{F}$ is a stack w.r.t. the Zariski topology.
- When $V \to U$ is a f.f. morphism of affine S-schemes, $\mathcal{F}(U) \to \mathcal{F}(V \to U)$ is an equivalence of categories.

then $\mathcal{F}$ is a stack w.r.t the fpqc topology. ⌟

Proof: Firstly, to show $\mathcal{F}$ is a prestack, using(6.1.3.8), it suffices to show for an S-scheme $T \to S$ and objects $\xi, \eta \in \mathcal{F}(T)$, the functor

$$\underline{\mathrm{Hom}}_T(\xi, \eta) : (\mathcal{S}\mathrm{ch}\,/T)^{op} \to \mathcal{S}\mathrm{et}$$

is a sheaf. But then we can use(6.1.4.33) to achieve this.

Next, according to(4.2.3.20) and(6.1.3.7), we may assume $\mathcal{F}$ is splitting.

Notice that $\mathcal{F}(\varnothing)$ is equivalent to the category pt. This is because $\mathcal{F}(\varnothing)$ is equivalent to $\mathcal{F}(\mathcal{U})$, where $\mathcal{U}$ is the null Zariski covering of $\varnothing$(with no mapping or obejcts at all!). Then for any disjoint union of open subschemes $U = \coprod U_i$, there is a natural isomorphism of categories $\mathcal{F}(U) \cong \prod_i \mathcal{F}(U_i)$.

Thus for any covering $\mathcal{U} = \{U_i \to X\}$, to show $\mathcal{F}(X) \to \mathcal{F}(\mathcal{U})$ is an equivalence of categories, it suffices to show that $\mathcal{F}(X) \to \mathcal{F}(\coprod U_i \to X)$ is an equivalence of categories: this is because $\coprod U_i \times_X \coprod U_i \cong \coprod U_i \times_X U_j$, so $\mathcal{F}(\coprod U_i \to X) \to \mathcal{F}(\mathcal{U})$ is an equivalence of categories.

If $\mathcal{U} = \{V \to U\}$ is a covering of F with a single morphism that is qc and U is affine, then by the proof of(6.1.3.10), we can choose a finite affine cover of V reduce to the case of covering of f.m. affine maps, then we finish by the case above.

If $\mathcal{U} = \{V \to U\}$ is a covering of F with a single morphism and U is affine, then we can find a Zariski covering $\{V_i \to V\}$ that each V_i is qc. and surjects onto U. Then there are maps of categories $\mathcal{F}(U) \to \mathcal{F}(\{V \to U\}) \to \mathcal{F}(\{V_i \to V\})$, where $\mathcal{F}(U) \to \mathcal{F}(\{V_i \to V\})$ is an equivalence and $\mathcal{F}(U) \to \mathcal{F}(\{V \to U\})$ is fully faithful. Thus to show $\mathcal{F}(U) \to \mathcal{F}(\{V \to U\})$ is an equivalence, it suffices to show $\mathcal{F}(\{V \to U\}) \to \mathcal{F}(\{V_i \to V\})$ is faithful, which is true by(6.1.3.9).

For general case, Cf.[Vis08]P88. □

Prop. (6.1.5.8). $\mathrm{Mor}\,/S : X \mapsto \mathcal{S}\mathrm{ch}\,/X$ is a prestack over $\mathcal{S}\mathrm{ch}_{\mathrm{fpqc}}\,/S$, by(6.1.4.34) and(6.1.3.16). ⌟

Def. (6.1.5.9) [Affine Fpqc Descent Datum]. For $A \to B \in \mathcal{CA}\mathrm{lg}$, define a category $\mathcal{M}\mathrm{od}_{A\to B}$ as follows: its objects are pairs (N, ψ), where $N \in \mathcal{M}\mathrm{od}_B$ and $\psi : N \otimes_A B \to B \otimes_A N$ is an isomorphism of $B \otimes_A B$-modules s.t. that

$$\psi_{12} \circ \psi_{01} = \psi_{02} : N \otimes_A B \otimes_A B \to B \otimes_A B \otimes_A N$$

where ψ_{ij} is permuting the i, j-parts using ψ. The morphisms in $\mathcal{M}\mathrm{od}_{A\to B}$ are maps in $\mathcal{M}\mathrm{od}_B$ that is compatible with ψ.

There is a natural functor $\mathcal{M}\mathrm{od}_{A\to B} \to \mathcal{M}\mathrm{od}_B$. ⌟

Lemma (6.1.5.10) [Affine Fpqc Descent]. For $A \to B \in \mathcal{CA}\mathrm{lg}$, there is a functor $F : \mathcal{M}\mathrm{od}_A \to \mathcal{M}\mathrm{od}_{A\to B}$, where M is mapped to $(B \otimes_A M, \psi_M)$ with

$$\psi_M : (B \otimes_A M) \otimes_A B \to B \otimes_A (B \otimes_A M) : b \otimes m \otimes b' \mapsto b \otimes b \otimes m.$$

Then when $A \to B$ is f.f., this is an equivalence of categories. ⌟

Proof: We construct an inverse T that maps (N,ψ) to $\{n|\psi(n\otimes 1)=1\otimes n\}$. Then $TF\cong \mathrm{id}$ because of the first exactness of(5.4.2.2).

And for $FT\cong\mathrm{id}$, let $T((N,\psi))=M$. Notice if $\psi(n\otimes 1)=\sum_i b_i\otimes n_i$, then by cocycle condition,

$$\sum_i b_i\otimes 1\otimes n_i=\sum_i b_i\otimes\psi(n_i\otimes 1).$$

so $\psi(N\otimes 1)\subset \ker(\mathrm{id}_B\otimes(n\mapsto\psi(n\otimes 1)-1\otimes n))=B\otimes M$ because B/A is flat.

So we defined a map $N\xrightarrow{\Psi}B\otimes_A M\in\mathcal{M}\mathrm{od}_B$, and the composition $B\otimes_A M\xrightarrow{\text{mul.}}N\xrightarrow{\Psi}B\otimes_A M$ is identity, because

$$\psi(bm\otimes 1)=(b\otimes 1)\psi(m\otimes 1)=(b\otimes 1)(1\otimes m)=b\otimes m.$$

This shows Ψ is surjective. And Ψ is injective because $n\mapsto n\otimes 1$ is injective as B/A is f.f., and ψ is an isomorphism. So Ψ is an isomorphism of $N\cong FT(N)$.

Finally, to show $\psi=\psi_M$, as now $B\otimes_A M\xrightarrow{\text{mul.}}N$ is an isomorphism, we check

$$\psi((bm)\otimes b')=(b\otimes b')\psi(m\otimes 1)=(b\otimes b')(1\otimes m)=b\otimes(b'm).$$

□

Remark (6.1.5.11). In fact, a descent datum is always effective iff $A\to B$ is universally injective. Cf.[Sta]. And f.f. extension is u.i.(5.4.1.28). ⌟

Prop. (6.1.5.12) [fpqc Descent for Qco Sheaves]. Let S be a scheme, then $\mathcal{QC}\mathrm{oh}/\mathcal{S}\mathrm{ch}\in\mathcal{S}\mathrm{ta}_{\mathrm{fpqc}}/S$. ⌟

Proof: We use(6.1.5.7), the first condition is satisfied by(6.1.5.3), and for the second condition, let $\mathrm{Spec}\,B\to\mathrm{Spec}\,A$ be a f.f. morphism of affine schemes, then $\mathcal{QC}\mathrm{oh}(\mathrm{Spec}\,B\to\mathrm{Spec}\,A)$ is equivalent to $\mathrm{Mod}_{A\to B}$, and $\mathcal{QC}\mathrm{oh}(\mathrm{Spec}\,A)$ is equivalent to Mod_A, so the conclusion follows from(6.1.5.10). □

Cor. (6.1.5.13). For any $\mathcal{F}\in\mathcal{QC}\mathrm{oh}(S)$, the functor $(\mathcal{S}\mathrm{ch}/S)^{op}\to\mathcal{A}\mathrm{b}:T\to\Gamma(T,f^*\mathcal{F})\in\mathcal{S}\mathrm{ta}_{\mathrm{fpqc}}/S$, hence are also sheaves w.r.t. the fppf, étale, Zariski topologies. ⌟

Proof: Because this functor is just $\underline{\mathrm{Hom}}_S(\mathcal{O}_S,\mathcal{F})$, and it is a sheaf(6.1.3.8). □

Cor. (6.1.5.14). If $\mathcal{P}$ is a property of Qco sheaves that is stable under base change and fpqc local, then $\mathcal{QC}\mathrm{oh}_{\mathcal{P}}/S\in\mathcal{S}\mathrm{ta}_{\mathrm{fpqc}}/S$. ⌟

Prop. (6.1.5.15) [Descending Affine Morphisms]. For a scheme S, let $\mathcal{P}$ be the class of affine arrows in $\mathcal{S}\mathrm{ch}/S$ that denote by $\mathrm{Mor}_S^{\mathcal{A}\mathrm{ff}}$ the resulting fibered category, then $\mathrm{Mor}_S^{\mathcal{A}\mathrm{ff}}\in\mathcal{S}\mathrm{ta}_{\mathrm{fpqc}}/S$. ⌟

Proof: Firstly $\mathrm{Mor}^{\mathcal{A}\mathrm{ff}}/S\in\mathcal{S}\mathrm{ta}_{\mathrm{Zar}}/S$, and it satisfies the affine fpqc descent condition of(6.1.5.7)(Notice the $\{n|\psi(n\otimes 1)=1\otimes n\}$ is now a ring, because ψ is a ring homomorphism), so we are done by(6.1.5.7). □

Cor. (6.1.5.16). If $\mathcal{P}$ is a subclass of affine arrows stable under base change and fpqc local on the target, then $\mathrm{Mor}^{\mathcal{P}}/S\in\mathcal{S}\mathrm{ta}_{\mathrm{fpqc}}/S$. ⌟

Prop. (6.1.5.17) [Descent via Ample Invertible Sheaves]. Let S be a scheme and $\mathcal{P}$ be a class of flat proper morphisms of f.p. in $\mathcal{S}\mathrm{ch}/S$ that is local in the fpqc topology. Assume that for each object $\xi:X\to U\in\mathcal{P}$, we have an invertible sheaf $\mathcal{L}_\xi$ on X that is ample relative to $X\to U$, and for an arrow $f:(X\xrightarrow{\xi}U)\to(Y\to\eta V)$, we have an isomorphism $\rho_f:f^*\mathcal{L}_\eta\cong\mathcal{L}_\xi$ that satisfies $\rho_{gf}=\rho_f\circ f^*\rho_g$, then $\mathrm{Mor}^{\mathcal{P}}/S\in\mathcal{S}\mathrm{ta}_{\mathrm{fpqc}}/S$. ⌟

Proof: Cf.[Vistoli, P96].**?** □

Étale Descent

Prop. (6.1.5.18) [Galois Descent]. Let L/K be a finite separable field extension with Galois group G, then $\operatorname{Spec} L \to \operatorname{Spec} K$ is a G-torsor in the étale topology. so Galois descent is a special case of étale descent along torsors(6.1.3.18).

Notice this is also true for arbitrary finite separable field extensions with continuity condition added, because we can take direct limits of categories over its finite normal subextensions. ⌟

Proof: Consider the locally constant group scheme $\underline{G} = \operatorname{Spec}(\prod_{g\in G} K)$, let $X = \operatorname{Spec} L, Y = \operatorname{Spec} K$, then $\{X \to Y\}$ is an étale cover, and the action $\underline{G} \times X \to X$ is given by

$$L \to \prod_{g\in G} L : x \mapsto \prod_{g\in G}(g(x)).$$

Thus $X \to Y$ is a G-equivariant map, and there is an isomorphism $G\times X \cong X\times_Y X : (g, x) \mapsto (gx, x)$ that corresponds to the isomorphism

$$L\otimes_K L \cong \prod_{g\in G} L : (a, b) \mapsto \prod_{g\in G}(g(a)b)$$

□

Cor. (6.1.5.19) [Galois Descent of Closed Immersions]. Let X be a scheme over a field k, and K/k be a Galois field extension with Galois group Γ, $X' = X \otimes_k K$. Then the category of closed subschemes of X is equivalent to the category of closed subschemes that is base change from some $X_{k'}$ where k'/k is finite, and is stable under the action of Γ. This weird finiteness condition can be removed when X is locally algebraic over k. ⌟

Proof: This is because the class of closed immersions is a stack(6.1.5.16). □

Remark (6.1.5.20). When Y is a subvariety of X and $K = k^s$, to check Y is stable under action of Γ, it suffices to check that the geometric points is closed under action of Γ. This is because the geometric points are dense in Y'(6.11.1.10). ⌟

Cor. (6.1.5.21) [Galois Descent for Ideals of Algebras]. Let $A \in \mathcal{CA}\mathrm{lg}_k$, and K/k be a Galois field extension with Galois group Γ, then the category of ideals of A is equivalent to the category of ideals of A_K that is base change from some $A_{k'}$ where k'/k is finite, and is stable under the action of Γ. This weird finiteness condition can be removed when A is f.g. over k. ⌟

Cor. (6.1.5.22) [Galois Descent of Morphisms]. Let X, Y be locally algebraic schemes over k and K/k a Galois field extension with Galois group Γ, $X' = X \otimes_k K, Y' = Y \otimes_k K$. If Y is separated, then a morphism $\varphi' : X' \to Y'$ arises from a morphism $X \to Y$ iff its graph $\Gamma_{\varphi'} \subset X' \times_{k'} Y'$ is stable under action of Γ. In this case φ is unique.

And when X, Y are varieties and $K = k^s$, then it suffices to check the map

$$\varphi'(k^s) : X'(k^s) \to Y'(k^s)$$

commutes with action of Γ. ⌟

Cor. (6.1.5.23) [Galois Descent for Qco Sheaves]. Let K/k be a Galois extension with Galois group Γ and X be a scheme over k with $X' = X \otimes_k K$, then $\mathfrak{QCoh}/X \to (\mathfrak{QCoh}/X')^\Gamma$ is an equivalence of categories. ⌟

Proof: This is because $\mathfrak{QCoh}/\mathfrak{Sch}$ is a fpqc stack(6.1.5.12). □

Cor. (6.1.5.24) [Galois Descent for Vector Spaces]. Let L/K be a Galois extension, then the functor $V \mapsto L \otimes_K V$ induces an equivalence $\mathcal{V}\mathrm{ect}_K \cong \mathrm{Rep}_L(\mathrm{Gal}(L/K))$. ⌟

Prop. (6.1.5.25) [Failure of Étale Descent for proper smooth morphisms]. Cf.[Vis08]P107. ⌟

Descending Properties

Prop. (6.1.5.26) [Properties of Morphisms Local in Fpqc Topology]. The following properties of morphisms are local on the target w.r.t. the fpqc topology.

1. quai-compact.
2. (quasi-)separated.
3. Universally closed.
4. universally open.
5. universally submersive.
6. surjective.
7. universally injective.
8. universally homeomorphism.
9. (locally)of f.t.
10. (locally)of f.p.
11. properness.
12. flatness.
13. (closed/open)immersion.
14. isomorphism/monomorphism.
15. (quasi-)affineness.
16. quasi-compact immersion.
17. integral
18. (locally)(quasi-)finite.
19. syntomic.
20. smooth, unramified, étale.
21. finite locally free.

⌟

Proof: Cf.[Sta]Chap34.20.

1.
2.
3.
4.

5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19. Cf.[Sta]00SM.
20.
21.

□

Prop. (6.1.5.27) [Properties of Schemes Local in the Fppf Topology].

-

⌟

Proof: Cf.[Sta]Chap34.13. □

Prop. (6.1.5.28) [Descending Properties that is not Fpqc Local].

- If $X \to Y$ is a faithfully flat morphism of schemes and X is (geo.)reduced, then Y is also (geo.)reduced.
- If $X \to Y$ is a faithfully flat morphism of f.p. between schemes and X is (geo.)regular, then Y is also (geo.)regular.

⌟

Proof: Looking stalkwise, these follows from(5.4.2.1). □

Prop. (6.1.5.29) [Torsors]. Let G be a group object in $(\mathcal{S}\mathrm{ch}_S)_\tau$ and $X \to S$ a G-torsor. Then if τ is a subcanonical site and $\mathscr{P}$ is a property that is local on $(\mathcal{S}\mathrm{ch}_S)_\tau$ and $G \to S$ has $\mathscr{P}$, then $X \to S$ has P. ⌟

Proof: By(6.1.1.17), there is a covering $\{Y_i \to S\}$ s.t. each $X \times_S Y_i \to Y_i \cong G \times_S Y_i$ is trivial, thus each $X \times_S Y_i \to Y_i$ has P, and then $X \to S$ has P. □

Weil Restrictions

Def. (6.1.5.30) [Weil Restrictions]. For $S' \to S \in \mathcal{S}\mathrm{ch}$, and $X \in \mathcal{S}\mathrm{ch}/S$, then the **Weil restriction** is the scheme $\mathrm{res}_{S'/S}(X) \in \mathcal{S}\mathrm{ch}/S$ representing the functor

$$\underline{\mathrm{Hom}}_S(S', X) : \mathcal{S}\mathrm{ch}/S \to \mathcal{S}\mathrm{et} : T \mapsto X(T \times_S S'),$$

if it exists. ⌟

Thm. (6.1.5.31). Let $S' \to S \in \mathcal{S}\mathrm{ch}$ be finite locally-free, and $X \in \mathcal{S}\mathrm{ch}/S'$ satisfying that: for any $s \in S$ and every finite subset of $X_{\kappa(s)}$ is contained in some affine open subset of $X_{\kappa(s)}$, then $\mathrm{res}_{S'/S}(X)$ exists. In particular, this applies to the case that X is quasi-projective. ⌟

Proof: Cf.[BLR90, Chap7.6. Thm4]. □

Thm. (6.1.5.32) [Quasi-Projectiveness]. Let $S' \to S \in \mathrm{N}\,\mathcal{S}\mathrm{ch}$ be finite locally-free, and $X \in \mathcal{S}\mathrm{ch}/S'$ is quasi-projective, then $\mathrm{res}_{S'/S}(X) \in \mathcal{S}\mathrm{ch}/S$ is also quasi-projective. ⌟

Proof: Cf.[Weil Restriction for Schemes]P5. □

Example (6.1.5.33) [Deligne Torus]. The **Deligne torus** is defined to be

$$\mathbb{S} = \mathrm{res}_{\mathbb{C}/\mathbb{R}}\, \mathbb{G}_m.$$

Then

- There are isomorphisms
$$\mathbb{S}(\mathbb{R}) \cong \mathbb{C}^\times, \quad \mathbb{S}_\mathbb{C} \cong \mathbb{G}_m \times \mathbb{G}_m,$$
where for any $T \in \mathcal{CR}\mathrm{ing}/\mathbb{C}$, the second isomorphism is given by
$$(T \otimes \mathbb{C})^\times \mapsto T^\times \times T^\times : t \otimes a \mapsto (t \otimes a, t \otimes \overline{a}).$$
- Under the isomorphism $\mathbb{S}_\mathbb{C}(\mathbb{C}) \cong \mathbb{C}^\times \times \mathbb{C}^\times$, the complex conjugation acts by $\overline{(z_1, z_2)} = (\overline{z}_2, \overline{z}_1)$.
- There is a **weight homomorphism** $w : \mathbb{G}_m \to \mathbb{S}$ s.t. for any $T \in \mathcal{CR}\mathrm{ing}/\mathbb{R}$, the map is given by
$$T^\times \to (T \otimes \mathbb{C})^\times : t \mapsto t^{-1}.$$

⌟

6 Étale Torsors

Prop. (6.1.6.1). For $X \in \mathcal{S}\mathrm{ch}$, $\check{H}^1(X, \mathrm{GL}(n)) \cong \mathcal{V}\mathrm{ect}^n(X)$ as pointed sets, by(6.1.5.2). ⌟

6.2 Ringed Topoi, Ringed Sites, Ringed G-Spaces and Schemes

1 Ringed Topoi, Ringed Sites

Def. (6.2.1.1)[Ringed Topoi]. A **ringed topos** is a pair $(\mathcal{Sh}(\mathcal{C}), \mathcal{O})$ where $\mathcal{C}$ is a site and $\mathcal{O}$ is a unital object in $\mathcal{Sh}(\mathcal{C})$, called the **structure sheaf**. A morphism of of ringed topoi $(f, f^\sharp) : (\mathcal{C}, \mathcal{O}) \to (\mathcal{C}', \mathcal{O}')$ consists of a morphism of topoi(6.1.2.18) $f : \mathcal{Sh}(\mathcal{C}) \to \mathcal{Sh}(\mathcal{C}')$ and a map of sheaves of rings $f^\sharp : f^{-1}\mathcal{O}' \to \mathcal{O}$. A composition of morphism of topoi is defined to be $(g, g^\sharp)\circ(f, f^\sharp) = (g\circ f, f^\sharp \circ f^{-1}(g^\sharp))$. ⌟

Def. (6.2.1.2)[Ringed Sites]. A **ringed site** is pair $(\mathcal{C}, \mathcal{O})$ where $\mathcal{C}$ is a site and $\mathcal{O}$ is a sheaf of rings on $\mathcal{C}$, called the **structure sheaf**. A ringed site induces a ringed topos. A morphism of ringed sites is a morphism of sites that the induced morphism of topoi(6.1.2.20) is a morphism of ringed topoi(6.2.1.1).

A site is naturally a ringed site where $\mathcal{O} = \underline{\mathbb{Z}}$ the constant sheaf(6.1.2.8). So we only consider ringed sites afterwards, then a morphism of ringed sites is naturally a morphism of ringed sites. So whenever we say $\mathcal{C}$ is a site, it is understood as a ringed site $(\mathcal{C}, \underline{\mathbb{Z}})$. ⌟

Prop. (6.2.1.3) [Ringed Topoi and Ringed Sites]. Let $(f, f^\sharp) : (\mathcal{Sh}(\mathcal{C}), \mathcal{O}_C) \to \mathcal{Sh}(\mathcal{D}, \mathcal{O}_D)$ be a morphism of ringed topoi, then we can find ringed sites $(\mathcal{C}', \mathcal{O}_{\mathcal{C}'})$ and $(\mathcal{D}', \mathcal{O}_{\mathcal{D}'})$ and a diagram

$$\begin{array}{ccc}(\mathcal{Sh}(\mathcal{C}), \mathcal{O}_{\mathcal{C}}) & \xrightarrow{(f,f^\sharp)} & (\mathcal{Sh}(\mathcal{D}), \mathcal{O}_{\mathcal{D}}) \\ \downarrow{\scriptstyle (g,g^\sharp)} & & \downarrow{\scriptstyle (e,e^\sharp)} \\ (\mathcal{Sh}(\mathcal{C}'), \mathcal{O}_{\mathcal{C}'}) & \xrightarrow{(h,h^\sharp)} & (\mathcal{Sh}(\mathcal{D}'), \mathcal{O}_{\mathcal{D}'})\end{array}$$

where

- $(g, g^\sharp)$ and $(e, e^\sharp)$ are equivalence of ringed topoi.
- $\mathcal{C}', \mathcal{D}'$ have final objects and finite products.
- $(h, h^\sharp)$ is induced by a continuous functor $\mathcal{D}' \to \mathcal{C}'$ that the preserves the final object and finite products,(thus induces a morphism of sites by(6.1.2.14)).

Moreover, given a set of sheaves $\mathcal{F}_i$ on $\mathcal{C}$ and a set of sheaves $\mathcal{G}_i$ on $\mathcal{D}$, we may choose C' and $\mathcal{D}'$ that these sheaves are representable by objects in $\mathcal{C}'$ or $\mathcal{D}'$. ⌟

Proof: [Sta]03CR. □

Prop. (6.2.1.4) [Multiplicative Structure Sheaf]. Given a ringed topoi $(\mathcal{Sh}(\mathcal{C}), \mathcal{O})$, the presheaf $U \mapsto \mathcal{O}^*(U)$ is a sheaf of groups, called the **multiplicative structure sheaf** $\mathcal{O}^*$. ⌟

Proof: This comes from the sheaf property of $\mathcal{O}$ and the fact the inverse of an element is unique. □

Def. (6.2.1.5)[Local Ringed Site]. A ringed site $(\mathcal{C}, \mathcal{O})$ is called a **local ringed site** if

$$\varnothing^\sharp \to \mathrm{Equalizer}(0, 1 : \mathrm{pt} \to \mathcal{O})$$

is an isomorphism of sheaves, and for any $U \in \mathcal{C}$ and $f \in \mathcal{O}(U)$, there exists a covering $\{U_i \to U\}$ s.t. for any j, either $f|_{U_i}$ is invertible or $(1 - f)|_{U_i}$ is invertible. ⌟

Prop. (6.2.1.6)[Characterizing Local Ringed Sites]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site, the following are equivalent:

- $(\mathcal{C}, \mathcal{O})$ is a local ringed site.
- (Partition of Unity) For any $U \in \mathcal{C}$, $f_1, \ldots, f_n \in \mathcal{O}(U)$ that $(f_1, \ldots, f_n) = (1)$, there is a covering $\{U_i \to U\}$ that for each j, there exists an i that f_i is invertible on U_j.
- The map of sheaves of sets:
$$(\mathcal{O} \otimes \mathcal{O}) \coprod (\mathcal{O} \times \mathcal{O}) \to \mathcal{O} \times \mathcal{O}$$
which maps (f, a) in the first component to (f, af) and (f, b) in the second component to $(f, b(1-f))$ is surjective.

⌟

Proof: Cf.[Sta]04ES. □

Def. (6.2.1.7) [Local Ringed Topoi]. If $f : \mathcal{S}h(\mathcal{C}') \to \mathcal{S}h(\mathcal{C})$ is a morphism of topoi and $(\mathcal{C}, \mathcal{O})$ is a local ringed site, then $(\mathcal{S}h(\mathcal{C}'), f^{-1}\mathcal{O})$ is also a local ringed site. In particular, being a local ringed site is an intrinsic property, so we can define **local ringed topoi** to be ringed topoi that the underlying ringed sites are local ringed. ⌟

Proof: Because f^{-1} is exact(6.1.2.18) and commutes with products and equalizers, it maps the isomorphism
$$\varnothing^\sharp \to \text{Equalizer}(0, 1 : \text{pt} \to \mathcal{O})$$
to the corresponding isomorphism of $\mathcal{C}'$, and also the sejection of
$$(\mathcal{O} \otimes \mathcal{O}) \coprod (\mathcal{O} \times \mathcal{O}) \to \mathcal{O} \times \mathcal{O}$$
in(6.2.1.6) to that of $\mathcal{C}'$, thus $(\mathcal{S}h(\mathcal{C}'), f^{-1}\mathcal{O})$ is also a local ringed site. □

Def. (6.2.1.8) [Morphisms of Local Ringed Topoi]. A **morphism of local ringed topoi** is a morphism of ringed topoi $(f, f^\sharp) : (\mathcal{S}h(\mathcal{C}), \mathcal{O}_C) \to (\mathcal{S}h(\mathcal{D}), \mathcal{O}_D)$ that the diagram of sheaves

$$\begin{array}{ccc} f^{-1}(\mathcal{O}_{\mathcal{D}}^*) & \xrightarrow{f^\sharp} & \mathcal{O}_{\mathcal{C}}^* \\ \downarrow & & \downarrow \\ f^{-1}(\mathcal{O}_{\mathcal{D}}) & \xrightarrow{f^\sharp} & \mathcal{O}_{\mathcal{C}} \end{array}$$

is Cartesian, where $\mathcal{O}_C^*$ is the multiplicative structure sheaf(6.2.1.4). Morphisms of local ringed topoi are stable under compositions. ⌟

Ringed Spaces

Def. (6.2.1.9) [Ringed Spaces]. A **ringed space** is a pair $(X, \mathcal{O}_X)$ consisting of a topological space X and a sheaf of rings $\mathcal{O}_X$ on X. A morphism of ringed spaces $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ consists of a pair $(f, f^\sharp)$ where f is a continuous map $X \to Y$ and $f^\sharp$, which induces a map of sites $(f^{-1}, f_*) : X_{\text{Zar}} \to Y_{\text{Zar}}$(6.2.6.7), and $f\sharp$ is a map $f^\sharp : f^{-1}(\mathcal{O}_Y) \to \mathcal{O}_X$(6.2.6.2), such that $(f, f^\sharp)$ is a map of ringed topoi(6.2.1.1). ⌟

Def. (6.2.1.10) [Local Ringed Space]. A **local ringed space** is a topological space X with a sheaf of rings $\mathcal{O}_X$ that $(X, \mathcal{O}_X)$ forms a local ringed site(6.2.1.5). A morphism of local ringed space is a morphism of ringed spaces that the corresponding morphism of ringed topoi $(\mathcal{S}h(\mathcal{C}), \mathcal{O}_{\mathcal{C}}) \to (\mathcal{S}h(\mathcal{D}), \mathcal{O}_{\mathcal{D}})$ is a morphism of local ringed topoi(6.2.1.8). ⌟

Prop. (6.2.1.11). A ringed space $(X, \mathcal{O}_X)$ is a locally ringed space iff any stalks $\mathcal{O}_{X,x}$ is either 0 or a local rings. ⌟

Proof: Cf.[Sta]04ET. □

2 Modules on Ringed Topoi

Main References are [Sta]Chap 18.

Def. (6.2.2.1) [Modules on Ringed Topoi]. Let $(\mathcal{Sh}(\mathcal{C}), \mathcal{O})$ be a ringed topos, then a sheaf of $\mathcal{O}$-modules is a presheaf of $\mathcal{O}$-modules that the underlying presheaf of Abelian groups is a sheaf. ⌟

Def. (6.2.2.2) [Support]. Let $(X, \mathcal{O}_X)$ be a ringed space, $\mathcal{F}$ a $\mathcal{O}_X$-module, then the **support** of $\mathcal{F}$ is the set of points x that $\mathcal{F}_x \neq 0$. It is denoted by $\mathrm{Supp}(\mathcal{F})$. For a section $s \in \Gamma(X, \mathcal{F})$, $\mathrm{Supp}(s)$ is defined to be the set of points x that $s_x \neq 0 \in \mathcal{F}_x$. ⌟

Prop. (6.2.2.3). Glueing sheaves is available for ringed spaces, similar to(6.1.5.3). ⌟

Proof: □

Prop. (6.2.2.4). Glueing ringed spaces is available. ⌟

Proof: □

Def. (6.2.2.5) [Local Properties of Modules]. On a ringed site $(\mathcal{C}, \mathcal{O})$, an $\mathcal{O}$-module $\mathcal{F}$ is called locally has property P if for any object $U \in \mathcal{C}$, there is a covering $\{U_i \to U\}$ that $\mathcal{F}|_{U_i}$ has property P. ⌟

Def. (6.2.2.6) [Intrinsic Properties of Modules]. An **intrinsic property** of sheaves of modules in a ringed topos $(\mathcal{Sh}(\mathcal{C}), \mathcal{O})$ that is invariant under equivalence of topoi. ⌟

Def. (6.2.2.7) [Tensor Products Sheaf]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}$-modules, then the **tensor product** $\mathcal{F} \otimes_{\mathcal{O}} \mathcal{G}$ is defined to be the shifification of the presheaf $U \mapsto \mathcal{F}(U) \otimes_{\mathcal{O}(U)} \mathcal{G}(U)$.

The tensor product is easily seen to be an intrinsic notion(6.2.2.6), so it can be defined on any ringed topoi. ⌟

Prop. (6.2.2.8) [Base Change]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{O}_2$ be a sheaf $\mathcal{O}_1$-algebras, $\mathcal{G}$ be a sheaf of $\mathcal{O}_1$-module and $\mathcal{F}$ a sheaf of $\mathcal{O}_2$-module, then

$$\mathrm{Hom}_{\mathcal{O}_1}(\mathcal{G}, \mathcal{F}_{\mathcal{O}_1}) = \mathrm{Hom}_{\mathcal{O}_2}(\mathcal{G} \otimes_{\mathcal{O}_1} \mathcal{O}_2, \mathcal{F}).$$

⌟

Proof: This can be seen from the definition of tensor product and the fact shifification doesn't bother because $\mathcal{F}$ is a sheaf. □

Def. (6.2.2.9) [Transfer of Modules on Ringed Sites]. Let $(f, f^\sharp)$ be a morphism of ringed topoi $(\mathcal{Sh}(\mathcal{C}), \mathcal{O}) \to (\mathcal{Sh}(\mathcal{C}'), \mathcal{O}')$, then there are functor:

- the **pushforward**: $f_* : \mathcal{Mod}(\mathcal{O}) \to \mathcal{Mod}(\mathcal{O}') : f_*\mathcal{F} = f_*\mathcal{F}$ as a $\mathcal{O}'$-module via $\mathcal{O}' \to f_*\mathcal{O}$.
- the **pullback** $f^* : \mathcal{Mod}(\mathcal{O}') \to \mathcal{Mod}(\mathcal{O}) : f^*\mathcal{G} = \mathcal{O} \otimes_{f^{-1}\mathcal{O}'} f^{-1}\mathcal{G}$ via $f^\sharp : f^{-1}\mathcal{O}' \to \mathcal{O}$. f^* is left adjoint to f_*, by the adjointness of f^{-1} and f_*(6.1.2.18).

If $(f, f^\sharp)$ is a morphism of ringed sites $(\mathcal{C}, \mathcal{O}) \to (\mathcal{C}', \mathcal{O}')$, then there is an **extension by zero** functor:

- (Extension by zero): For the localization of sites $j_U : (\mathcal{C}/U, \mathcal{O}_U) \to (\mathcal{C}, \mathcal{O})$ the localization map of site, $j_U^* = j_U^{-1}$ has a left adjoint $j_{U!}$ defined by shifification of the presheaf

$$\mathcal{G} \mapsto j_{U!}(\mathcal{G}) : j_{U!}(\mathcal{G})(V) = \bigoplus_{\varphi: V \to U} \mathcal{G}(V \xrightarrow{\varphi} U \in \mathcal{C}/U).$$

⌟

Proof: To show $j_{U!}$ is left adjoint to j_U^*, Cf.[Sta]03DI. □

Remark (6.2.2.10). The f^* may not be exact. f^{-1} is exact, but we tensored with $\mathcal{O}_X$, it is exact when f is flat(6.2.2.15). ⌟

Prop. (6.2.2.11) [Extension by Zero is Exact]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $U \in \mathcal{C}$, then the extension by zero functor $j_{U!} : \mathcal{M}od(\mathcal{O}_U) \to \mathcal{M}od(\mathcal{O})$ is exact and reflects exactness. ⌟

Proof: It is right exact because is a left adjoint, and it is left exact by direct inspection. For refection of exactness, Cf.[Sta]0E8G.**?** □

Prop. (6.2.2.12) [Tensor Products and Pullbacks]. Tensor products commute with pullbacks, in particular with taking stalks. So tensoring with a locally free sheaf is exact. ⌟

Proof: By(6.2.3.3) and(6.2.3.5), for any $\mathcal{O}$-module $\mathcal{H}$,

$$\mathrm{Hom}(f^*\mathcal{F} \otimes f^*\mathcal{G}, \mathcal{H}) = \mathrm{Hom}(\mathcal{F}, f_*\mathcal{H}om(f^*\mathcal{G}, \mathcal{H})) = \mathrm{Hom}(\mathcal{F}, \mathcal{H}om(\mathcal{G}, f_*\mathcal{H})) = \mathrm{Hom}(f^*(\mathcal{F} \otimes \mathcal{G}), \mathcal{H}).$$

□

Prop. (6.2.2.13) [$j_{U!}$ Commutes with Restriction]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $U \in \mathcal{C}, \mathcal{G} \in \mathcal{M}od(\mathcal{O}_U), \mathcal{F} \in \mathcal{M}od(\mathcal{O})$, then there is a natural isomorphism $j_{U!}\mathcal{G} \otimes_{\mathcal{O}} \mathcal{F} \cong j_{U!}(\mathcal{G} \otimes_{\mathcal{O}_U} \mathcal{F}|_U)$ ⌟

Proof: By(6.2.3.3) and(6.2.3.5), for any $\mathcal{H} \in \mathcal{M}od(\mathcal{O})$,

$$\begin{aligned}\mathrm{Hom}_{\mathcal{O}}(j_{U!}(\mathcal{G} \otimes_{\mathcal{O}_U} \mathcal{F}|_U), \mathcal{H}) &= \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{G} \otimes_{\mathcal{O}_U} \mathcal{F}|_U, \mathcal{H}|_U) = \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{G}, \mathcal{H}om_{\mathcal{O}}(\mathcal{F}|_U, \mathcal{H}|_U)) \\ &= \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{G}, \mathcal{H}om_{\mathcal{O}_U}(\mathcal{F}, \mathcal{H})|_U) = \mathrm{Hom}_{\mathcal{O}}(j_{U!}\mathcal{G}, \mathcal{H}om_{\mathcal{O}}(\mathcal{F}, \mathcal{H})) \\ &= \mathrm{Hom}_{\mathcal{O}}(j_{U!}\mathcal{G} \otimes_{\mathcal{O}} \mathcal{F}, \mathcal{H})\end{aligned}$$

then use Yoneda lemma. □

Prop. (6.2.2.14) [Properties of Tensor Products]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{F}, \mathcal{G}$ be sheaves of $\mathcal{O}$-modules, then

1. If $\mathcal{F}, \mathcal{G}$ are locally free, then so does $\mathcal{F} \otimes \mathcal{G}$.
2. If $\mathcal{F}, \mathcal{G}$ are locally finite free, then so does $\mathcal{F} \otimes \mathcal{G}$.
3. If $\mathcal{F}, \mathcal{G}$ are locally generated by sections, then so does $\mathcal{F} \otimes \mathcal{G}$.
4. If $\mathcal{F}, \mathcal{G}$ are of f.t., then so does $\mathcal{F} \otimes \mathcal{G}$.
5. If $\mathcal{F}, \mathcal{G}$ are quasi-coherent., then so does $\mathcal{F} \otimes \mathcal{G}$.
6. If $\mathcal{F}, \mathcal{G}$ are of f.p., then so does $\mathcal{F} \otimes \mathcal{G}$.
7. If $\mathcal{F}$ is of f.p. and $\mathcal{G}$ is coherent, then $\mathcal{F} \otimes \mathcal{G}$ is coherent. In particular, if $\mathcal{F}, \mathcal{G}$ are coherent, then so does $\mathcal{F} \otimes \mathcal{G}$(6.2.2.27).

⌟

Proof: Cf.[Sta]03L6. □

Flat Modules

Def. (6.2.2.15) [Flat Modules and Flat Morphisms]. Let $\mathcal{C}$ be a site and $\mathcal{O}$ a presheaf of rings, then a presheaf $\mathcal{F}$ of $\mathcal{O}$-modules is called **flat** if the functor $P\mathcal{M}od(\mathcal{O}) \to P\mathcal{M}od(\mathcal{O}) : \mathcal{G} \mapsto \mathcal{G} \otimes_{\mathcal{O}} \mathcal{F}$ is exact.

Let $\mathcal{C}$ be a ringed site, and $\mathcal{F}$ is a sheaf of $\mathcal{O}$-modules, then it is called **flat** if the functor $\mathcal{M}od(\mathcal{O}) \to \mathcal{M}od(\mathcal{O}) : \mathcal{G} \mapsto \mathcal{G} \otimes_{\mathcal{O}} \mathcal{F}$ is exact.

A morphism $(f, f^\sharp)$ is called a **flat morphism** if the ring map $f^\sharp : f^{-1}\mathcal{O}' \to \mathcal{O}$ is flat, or equivalently, the pullback functor(6.2.2.9) f^* is exact.

If $(f, f^\sharp)$ is a morphism of ringed topoi $(\mathcal{S}h(\mathcal{C}), \mathcal{O}) \to (\mathcal{S}h(\mathcal{C}'), \mathcal{O}')$, and $\mathcal{F}$ is a sheaf of $\mathcal{O}$-modules, then $\mathcal{F}$ is **flat** over $(\mathcal{S}h(\mathcal{C}'), \mathcal{O}')$ if $\mathcal{F}$ is flat over $f^{-1}\mathcal{O}'$. ⌟

Prop. (6.2.2.16). Let $\mathcal{C}$ be a site and $\mathcal{O}$ a presheaf of rings with shifification $\mathcal{O}^\sharp$.

- If $\mathcal{F}$ is a presheaf of $\mathcal{O}$-modules that each $\mathcal{F}(U)$ is flat $\mathcal{O}(U)$-modules, then $\mathcal{F}$ is flat.
- If $\mathcal{F}$ is a flat presheaf of $\mathcal{O}$-modules, then $\mathcal{F}^\sharp$ is a flat $\mathcal{O}^\sharp$-modules.
- A filtered colimits of flat presheaves of modules is flat. A direct sum of flat presheaves of modules is flat.
- A filtered colimits of flat sheaves of modules is flat. A direct sum of flat sheaves of modules is flat.

⌟

Prop. (6.2.2.17) [Flatness is Stalkwise]. Let $(X, \mathcal{O}_X)$ be a ringed space, then an $\mathcal{O}_X$-module $\mathcal{F}$ is flat iff the stalks $\mathcal{F}_x$ are all flat $\mathcal{O}_{X,x}$-modules. ⌟

Proof: Cf.[Sta]05NE. □

Prop. (6.2.2.18) [Flat Morphism and Support]. Let $f : (X, \mathcal{O}_X) \to (X', \mathcal{O}_{X'})$ be a flat morphism of local ringed spaces, $\mathcal{F}$ an $\mathcal{O}_{X'}$-module, then $\mathrm{Supp}(f^*(\mathcal{F})) = f^{-1}(\mathrm{Supp}(\mathcal{F}))$. ⌟

Proof: Use the fact flat ring map of local rings is faithfully flat. □

Modules of Finite Type & Finite Presentation

Def. (6.2.2.19) [Finite Type]. An $\mathcal{O}$-module is called if **finite type** iff locally a quotient of a finite free sheaf. ⌟

Prop. (6.2.2.20) [Extension of F.T. Sheaves]. if $0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0$ is an exact sequence of $\mathcal{O}$-modules and $\mathcal{F}_1, \mathcal{F}_3$ are of f.t., then $\mathcal{F}_2$ is of f.t.. ⌟

Proof: For any $U \in \mathcal{C}$, choose a covering $\{U_i \to U\}$ that $\mathcal{F}_3(U_i)$ is generated by f.m. sections, then by passing to a covering, we may assume these sections come from $\mathcal{F}_2$. Pass to another covering that $\mathcal{F}_1$ is generated by f.m. sections, then on this covering, $\mathcal{F}_2$ is generated by f.m. sections. □

Def. (6.2.2.21) [Finite Presentation]. A sheaf of modules $\mathcal{F}$ is called **of finite presentation** iff locally it is a cokernel of two finite free modules. The pullback of a f.p. sheaf is f.p, by the left adjointness of f^*. ⌟

Prop. (6.2.2.22) [FP-FT-FT]. If $f : \mathcal{G} \to \mathcal{F}$ is a surjection of $\mathcal{O}$-modules, $\mathcal{F}$ is of f.p. and $\mathcal{G}$ is of f.t., then the kernel is of finite type. ⌟

Proof: We first show for $\mathcal{G}=\mathcal{O}^n$: By pass to covering, we can construct a diagram

$$\begin{array}{ccccccccc} & & \mathcal{O}^m_{U_{ij}} & \longrightarrow & \mathcal{O}^n_{U_{ij}} & \longrightarrow & \mathcal{F}|_{U_{ij}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \ker(f)|_{U_{ij}} & \longrightarrow & \mathcal{G}|_{U_{ij}} & \longrightarrow & \mathcal{F}|_{U_{ij}} & \longrightarrow & 0 \end{array}$$

and then use snake lemma. The image and cokernel of α are all of f.t., then $\ker(f)|_{U_{ij}}$ is of f.t. by(6.2.2.20).

For general $\mathcal{G}$, locally choose a surjection $\varphi:\mathcal{O}^n_{U_i}\to\mathcal{G}|_{U_i}$, then $\ker(f|_{U_i})=\varphi(\ker(\varphi\circ f|_{U_i}))$, which is of f.t.. □

Prop. (6.2.2.23). Pullbacks of a module of finite type is of finite type. Pullback of a module of finite presentation is of finite presentation.

Finite type and finite presentation are local on the target. ⌟

Proof: This is because pullback is a left adjoint thus right exact. They are local on the target because they are defined locally. □

Prop. (6.2.2.24) [Support is Zariski Closed]. If $(X,\mathcal{O}_X)$ is a ringed space and $f:\mathcal{G}\to\mathcal{F}$ is surjective at a point x and $\mathcal{F}$ is of f.t., then it is surjective on a Zariski nbhd of x. Thus the support of a f.t. sheaf is closed (look at $0\to\mathcal{F}$). ⌟

Proof: Choose a nbhd of x that $\mathcal{F}(U)$ is generated by $s_1,\ldots,s_n\in\mathcal{F}(U)$, because f is surjective at the stalk of x, after shrinking U, we may assume $s_i=f(t_i)$ for $t_i\in\mathcal{G}(U)$, so f is surjective on U. □

(Quasi-)Coherent Sheaves

Def. (6.2.2.25) [Quasi-Coherent Sheaf]. An $\mathcal{O}$-module $\mathcal{F}$ on a ringed site is called **quasi-coherent** iff locally it is a cokernel of two free modules. A locally f.p. sheaf of modules is Qco. ⌟

Prop. (6.2.2.26) [Associated Qco Sheaves]. And for a ringed space $(X,\mathcal{O}_X)$ and a $R=\Gamma(X,\mathcal{O}_X)$-module M, we have a coherent sheaf $\mathcal{F}_M$ on X, defined as $\pi^*(M)$, where M is seen as a qco sheaf on (pt,R). It is the sheaf associated to the presheaf $U\mapsto\mathcal{O}_X(U)\otimes M$.

This construction is a functor from the category of R-module to the category of Qco $\mathcal{O}_X$-modules, and it commutes with colimits because π^* does. And it is left adjoint to Γ by(6.2.2.9):

$$\mathrm{Hom}_A(M,\Gamma(X,\mathcal{G}))\cong\mathrm{Hom}_{\mathcal{O}_X}(\mathcal{F}_M,\mathcal{G})$$

⌟

Def. (6.2.2.27) [Coherent Sheaves]. A **coherent sheaf** is a $\mathcal{O}$-module $\mathcal{F}$ that is of f.t. and for any object U and for any set of elements of $\Gamma(U,\mathcal{F})$, the kernel of $\oplus\mathcal{O}_U\to\mathcal{F}|_U$ is of f.t..

A coherent sheaf is of f.p., by base change to a smaller covering, and it is Qco. ⌟

Prop. (6.2.2.28) [Properties of Coherent Sheaves]. Any f.t. subsheaf of a coherent sheaf is coherent, by definition. Any kernel of a morphism from a f.t. sheaf to a coherent sheaf is of f.t..

$\mathfrak{Coh}(X)$ is a weak Serre subcategory of $\mathfrak{Mod}_{\mathcal{O}_X}$. In particular, if $\mathcal{O}_X$ is coherent, then a sheaf is coherent iff it is f.p. ⌟

Proof: Let $\mathcal{G}$ be a sheaf of f.t. and $\mathcal{F}$ be a coherent sheaf. For any map $f:\mathcal{G}\to F$ and $U\in\mathcal{C}$, let $\{U_i\to U\}$ be a covering that there are surjections $\varphi_i:\mathcal{O}_{U_i}^{n_i}\to G|_{U_i}$. Then $\ker(f\circ\varphi_i)$ is a $\mathcal{O}_U$-module of f.t.. Now $\varphi_i:\ker(f\circ\varphi_i)\to\ker(f)|_{U_i}$ is a surjection, so $\ker(f)|_{U_i}$ is of f.t., and $\ker(f)$ is of f.t..

The kernel of a map between coherent sheaves is of f.t. by the result above, thus it is coherent.

Let $\varphi:\mathcal{F}_1\to\mathcal{F}$ be a map between coherent sheaves, then $\mathrm{Im}(\varphi)$ and $\mathrm{Coker}(\varphi)$ are of f.t.. For any $U\in\mathcal{C}$ and sections $\overline{s}_i$ of $\mathrm{Coker}(\varphi)(U)$ inducting a map $\overline{\Phi}:\mathcal{O}_U^n\to\mathrm{Coker}(\varphi)|_U$, we can choose a covering $\{U_i\to U\}$ that $\overline{s}_i$ comes from $s_i\in\mathcal{F}(U_i)$ for any i. Now we can choose coverings $\{U_{ij}\to U_i\}$ that there are surjections $\mathcal{O}_{U_{ij}}^{n_{ij}}\to\mathrm{Im}(\varphi)(U_{ij})$. Consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}|_{U_{ij}}^{n_{ij}} & \longrightarrow & \mathcal{O}|_{U_{ij}}^{n_{ij}}\oplus\mathcal{O}_{U_{ij}}^{n} & \longrightarrow & \mathcal{O}_{U_{ij}}^{n} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow\Phi & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Im}(\varphi)|_{U_{ij}} & \longrightarrow & \mathcal{F}|_{U_{ij}} & \longrightarrow & \mathrm{Coker}(\varphi)|_{U_{ij}} & \longrightarrow & 0 \end{array},$$

then snake lemma gives a surjection $\ker\Phi\to\ker(\overline{\Phi})\to 0$. Because $\ker\Phi$ is of f.t., so does $\ker(\overline{\Phi})$, and $\mathrm{Coker}(\varphi)$ is coherent.

Let $0\to\mathcal{F}_1\to\mathcal{F}_2\to\mathcal{F}_3\to 0$ be an exact sequence that $\mathcal{F}_1,\mathcal{F}_3$ is coherent, then by(6.2.2.20), $\mathcal{F}_2$ is of f.t.. For any object $U\in\mathcal{C}$, consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & \mathcal{O}_U^n & \longrightarrow & \mathcal{O}_U^n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow\varphi_1 & & \downarrow\varphi_2 & & \\ 0 & \longrightarrow & \mathcal{F}_1|_U & \longrightarrow & \mathcal{F}_2|_U & \longrightarrow & \mathcal{F}_3|_U & \longrightarrow & 0 \end{array},$$

the snake lemma gives an exact sequence $0\to\ker(\varphi_1)\to\ker(\varphi_2)\to\mathcal{F}_1|_U$. So $\ker(\varphi_1)$ is of f.t., so $\mathcal{F}_2$ is coherent. □

Prop. (6.2.2.29). The pullback of a (quasi-)coherent module is a (quasi-)coherent, because f^* is a left adjoint. ⌟

Prop. (6.2.2.30). (Quasi-)Coherence is local on the target. ⌟

Proof: This is because they are defined locally. □

Prop. (6.2.2.31). Let $(X,\mathcal{O}_X)$ be a ringed space and $x\in X$.

- Let $f:\mathcal{G}\to\mathcal{F}$ be a map of $\mathcal{O}_X$-modules. If $\mathcal{G}$ is of f.t. and $\mathcal{F}$ is coherent, and f is injective at the stalk of x, then there exists a nbhd U of x that $f|_U$ is injective.
- Let $f:\mathcal{G}\to\mathcal{F}$ be a map of coherent $\mathcal{O}_X$-modules that is surjective at the stalk of x, then there exists a nbhd U of x that $f|_U$ is surjective.
- Let $f:\mathcal{G}\to\mathcal{F}$ be a map of coherent $\mathcal{O}_X$-modules that is isomorphism at the stalk of x, then there exists a nbhd U of x that $f|_U$ is an isomorphism.

⌟

Proof: 1: Consider the kernel of f, then it is of f.t. by definition(6.2.2.27). Then $\ker(f)_x=0$, so there is a nbhd U of x that $\ker(f)|_U=0$, by(6.2.2.24), which means $f|_U$ is injective.

2: this is immediate from(6.2.2.24).

3 follows from 1 and 2. □

3 Construction of Sheaves

Internal Hom

Def. (6.2.3.1) [Internal Hom]. Let $\mathcal{C}$ is a category and $\mathcal{O}$ is a presheaf of rings, $\mathcal{F}, G$ be presheaves of $\mathcal{O}$-modules, then $U \mapsto \mathrm{Hom}_{\mathcal{O}|_U}(\mathcal{F}|_U, \mathcal{G}|_U)$ defines a presheaf $\mathcal{H}om(\mathcal{F}, \mathcal{G})$ of $\mathcal{O}$-modules, and there is a natural evaluation map

$$\mathcal{F} \otimes_{\mathcal{O}} \mathcal{H}om(\mathcal{F}, \mathcal{G}) \to \mathcal{G}.$$

Now if $\mathcal{C}$ is a site and $\mathcal{O}$ is a sheaf of rings, $\mathcal{F}, G$ be sheaves of $\mathcal{O}$-modules, then $\mathcal{H}om_{\mathcal{O}}(\mathcal{F}, \mathcal{G})$ is a sheaf of $\mathcal{O}$-modules by(6.1.3.17), called the **internal Hom sheaf**. Denote $\mathcal{H}om(\mathcal{F}, \mathcal{O})$ by $\mathcal{F}^\vee$. ⌟

Prop. (6.2.3.2). Internal Hom sheaf commutes with localization: $\mathcal{H}om_{\mathcal{O}_U}(\mathcal{F}|_U, \mathcal{G}|_U) = \mathcal{H}om_{\mathcal{O}}(\mathcal{F}, \mathcal{G})|_U$. This follows from thedefinition. ⌟

Prop. (6.2.3.3) [Tensoring and Inner Hom]. If $\mathcal{C}$ is a site, $\mathcal{O}$ is a sheaf of rings and $\mathcal{F}, \mathcal{G}, \mathcal{H}$ are sheaves of $\mathcal{O}$-modules, then there is a canonical isomorphism of sheaves:

$$\mathcal{H}om_{\mathcal{O}}(\mathcal{H} \otimes_{\mathcal{O}} \mathcal{F}, \mathcal{G}) \cong \mathcal{H}om_{\mathcal{O}}(\mathcal{F}, \mathcal{H}om_{\mathcal{O}}(\mathcal{H}, \mathcal{G})).$$

In particular, taking limit over $\mathcal{C}$, we see $- \otimes_{\mathcal{O}} \mathcal{H}$ is left adjoint to $\mathcal{H}om_{\mathcal{O}}(\mathcal{F}, -)$:

$$\mathrm{Hom}_{\mathcal{O}}(\mathcal{H} \otimes_{\mathcal{O}} \mathcal{F}, \mathcal{G}) \cong \mathrm{Hom}_{\mathcal{O}}(\mathcal{F}, \mathcal{H}om_{\mathcal{O}}(\mathcal{H}, \mathcal{G})).$$

In particular, the monoidal category of $\mathcal{O}_X$-modules is closed(6.2.2.15). ⌟

Proof: Omitted(Recall the definition of tensor product sheaf(6.2.2.7)). □

Prop. (6.2.3.4).

$$\mathcal{H}om(\varinjlim A_i, B) \cong \varprojlim \mathcal{H}om(A_i, B) \quad \mathcal{H}om(A, \varprojlim B_i) \cong \varprojlim \mathcal{H}om(A, B_i)$$

⌟

Proof: This is immediate from(4.1.5.10). □

Prop. (6.2.3.5). f^* is left adjoint to f_* by(6.2.2.9): $\mathrm{Hom}_{\mathcal{O}_X}(f^*\mathcal{G}, \mathcal{F}) \cong \mathrm{Hom}_{\mathcal{O}_Y}(\mathcal{G}, f_*\mathcal{F})$. In fact

$$f_*(\mathcal{H}om_{\mathcal{O}}(f^*\mathcal{G}, \mathcal{F})) \cong \mathcal{H}om_{\mathcal{O}'}(\mathcal{G}, f_*\mathcal{F}).$$

by checking on every open subset $U \subset Y$. ⌟

Prop. (6.2.3.6). Let $\mathcal{C}$ be a site and $\mathcal{O} \to O'$ is a map of sheaves of rings, then for any $\mathcal{G} \in \mathcal{M}od(\mathcal{O}')$ and $\mathcal{F} \in \mathcal{M}od(\mathcal{O})$, there is a natural isomorphism

$$\mathrm{Hom}_{\mathcal{O}}(\mathcal{G}, \mathcal{F}) = \mathrm{Hom}_{\mathcal{O}'}(\mathcal{G}, \mathcal{H}om_{\mathcal{O}}(\mathcal{O}', \mathcal{F})).$$

by checking on every open subset $U \subset Y$. ⌟

Prop. (6.2.3.7). Let $f_* : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ be a morphism of ringed spaces, and $\mathcal{F}, \mathcal{G}$ are $\mathcal{O}_Y$-modules. If $\mathcal{F}$ is f.p. and f is flat, then the canonical map

$$f^*\mathcal{H}om_{\mathcal{O}_Y}(\mathcal{F}, \mathcal{G}) \to \mathcal{H}om_{\mathcal{O}_X}(f^*\mathcal{F}, f^*\mathcal{G})$$

is an isomorphism. ⌟

Proof: ? □

Prop. (6.2.3.8). Let $(X, \mathcal{O}_X)$ be a ringed space and $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}_X$-modules. If $\mathcal{F}$ is f.p. or locally free, then the canonical map

$$\mathcal{H}om(\mathcal{F}, \mathcal{G})_x \to \mathrm{Hom}_{\mathcal{O}_{X,x}}(\mathcal{F}_x, \mathcal{G}_x)$$

is an isomorphism. ⌟

Proof: Choose a presentation of $\mathcal{F}$. This follows from the exactness of taking stalks and(6.2.3.4). □

Prop. (6.2.3.9). Let $(X, \mathcal{O}_X)$ be a ringed site and $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}_X$-modules. If $\mathcal{F}$ is f.p. and $\mathcal{G}$ is coherent, then $\mathcal{H}om(\mathcal{F}, \mathcal{G})$ is also coherent. In particular, this applies to $\mathcal{F}, \mathcal{G}$ both coherent. ⌟

Proof: This follows from(6.2.3.4) and(6.2.2.28). □

Tensor Sheaves

Def. (6.2.3.10) [Tensor Sheaves]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{F}$ an $\mathcal{O}$-module, then we define

- $T(\mathcal{F})$ to be the sheafification of the presheaf $U \mapsto T_{\mathcal{O}_X(U)}(\mathcal{F}(U))$(5.1.1.21).
- $\wedge\mathcal{F}$ to be the sheafification of the presheaf $U \mapsto \wedge_{\mathcal{O}_X(U)}(\mathcal{F}(U))$(5.1.1.21).
- $\mathrm{Sym}(\mathcal{F})$ to be the sheafification of the presheaf $U \mapsto \mathrm{Sym}_{\mathcal{O}_X(U)}(\mathcal{F}(U))$(5.1.1.21).

⌟

Cor. (6.2.3.11). Over a ringed space $(X, \mathcal{O}_X)$, the construction of $T(\mathcal{F}), \wedge(\mathcal{F})$ and $Sym(\mathcal{F})$ commutes with taking stalks, because the construction of tensor algebras and shifification are both left adjoints(5.1.1.22). Also they commutes with pullbacks, because they satisfy the same universal properties. ⌟

Prop. (6.2.3.12). let $\mathcal{F}$ be an $(\mathcal{C}, \mathcal{O})$-module, then the following properties are preserved under the construction of $T(\mathcal{F}), \wedge(\mathcal{F})$ and $\mathrm{Sym}(\mathcal{F})$:

- Locally generated by sections.
- Finite Type.
- Finite Presented.
- Coherent.
- Quasi-coherent.
- Locally free.

⌟

Proof: Cf.[Sta]01CL. □

4 Sheaf of Differentials

Prop. (6.2.4.1). If $\mathcal{C}$ is a site and $\mathcal{O}_1 \to \mathcal{O}_2$ is a homomorphism of sheaves of rings and $\mathcal{F}$ is a sheaf of $\mathcal{O}_2$-modules, then an $\mathcal{O}_1$**-derivation** from $\mathcal{O}_2$ to $\mathcal{F}$ is a map that for any $U \in \mathcal{C}$, the map $\mathcal{O}_2(U) \to \mathcal{F}(U)$ is a $\mathcal{O}_1(U)$-derivation(5.4.3.1). ⌟

Prop. (6.2.4.2) [Sheaf of Differentials]. Let $\mathcal{C}$ be a site and $\mathcal{O}_1 \to \mathcal{O}_2$ is a homomorphism of sheaves of rings and $\mathcal{F}$ is a sheaf of $\mathcal{O}_2$-modules, then the functor $\mathcal{M}od(\mathcal{O}_2) \to \mathcal{A}b : \mathcal{F} \to \mathrm{Der}_{\mathcal{O}_1}(\mathcal{O}_2, \mathcal{F})$ is representable by a sheaf of modules $\Omega_{\mathcal{O}_2/\mathcal{O}_1}$, called the **sheaf of differentials**. and the map $d : \mathcal{O}_2 \to \Omega_{\mathcal{O}_2/\mathcal{O}_1}$ is called the universal derivation. ⌟

Proof: The construction is similar to that of(5.4.3.4): if for any sheaf $\mathcal{F}$ we denote $\mathcal{O}_2[\mathcal{F}]$ generated by shifification of the presheaf $U \mapsto \mathcal{O}_2(U)[\mathcal{F}(U)]$, then $\Omega_{\mathcal{O}_2/\mathcal{O}_1}$ is the cokernel of

$$\mathcal{O}_2[\mathcal{O}_2 \times \mathcal{O}_2] \oplus \mathcal{O}_2[\mathcal{O}_2 \times \mathcal{O}_2] \oplus \mathcal{O}_2[\mathcal{O}_1] \to \mathcal{O}_2[\mathcal{O}_2]$$

□

Prop. (6.2.4.3) [Localness of Sheaf of Differentials]. If $\mathcal{O}_1 \to \mathcal{O}_2$ is a homomorphism of presheaves of rings, then $\Omega_{\mathcal{O}_2^\sharp/\mathcal{O}_1^\sharp}$ is the sheafification of the presheaf $U \mapsto \Omega_{\mathcal{O}_2(U)/\mathcal{O}_1(U)}$. ⌟

Proof: This is because the construction of $\Omega_{\mathcal{O}_2^\sharp/\mathcal{O}_1^\sharp}$(5.4.3.4) for all U gives an exact sequence of presheaves, and the shifification of which is just the construction in(6.2.4.2), so we are done because shifification is exact(6.1.2.7). □

Prop. (6.2.4.4) [Change of Sites]. Let $f : \mathcal{S}h(\mathcal{D}) \to \mathcal{S}h(\mathcal{C})$ be a morphism of topoi and $\varphi : \mathcal{O}_1 \to \mathcal{O}_2$ a homomorphism of rings on $\mathcal{C}$, then there is a canonical isomorphism $f^{-1}\Omega_{\mathcal{O}_2/\mathcal{O}_1} \cong \Omega_{f^{-1}\mathcal{O}_2/f^{-1}\mathcal{O}_1}$ compatible with the universal derivations. ⌟

Proof: This follows from the construction(6.2.4.2) and the fact f^{-1} is exact(6.2.4.2). □

Prop. (6.2.4.5) [Functoriality of Ω]. Let $\varphi : (\mathcal{O}_1 \to \mathcal{O}_2) \to (\mathcal{O}_1' \to \mathcal{O}_2')$ be a commutative diagram of sheaves of rings over a site $\mathcal{C}$, then the map $\mathcal{O}_1' \to \mathcal{O}_2'$ composed with the derivative $\mathcal{O}_2' \to \Omega_{\mathcal{O}_2'/\mathcal{O}_1'}$ is a $\mathcal{O}_1'$-derivative, thus we obtain a map of $\mathcal{O}_2$-modules $\Omega_{\mathcal{O}_2/\mathcal{O}_1} \to \Omega_{\mathcal{O}_2'/\mathcal{O}_1'}$, or equivalently a map of $\mathcal{O}_2'$-modules $\Omega_{\mathcal{O}_2/\mathcal{O}_1} \otimes_{\mathcal{O}_2} \mathcal{O}_2' \to \Omega_{\mathcal{O}_2'/\mathcal{O}_1'}$. Thus $\Omega_{-/-}$ is a functor of arrows.

Moreover, if $\mathcal{O}_2' = \mathcal{O}_2 \otimes_{\mathcal{O}_1} \mathcal{O}_1'$, then this map is an isomorphism, by(6.2.4.3) and(5.4.3.6). ⌟

Prop. (6.2.4.6). Let $\mathcal{O}_1 \to \mathcal{O}_2 \to \mathcal{O}_2'$ be a map of sheaves of rings that $\mathcal{O}_2 \to \mathcal{O}_2'$ is surjective with kernel $\mathcal{I} \subset \mathcal{O}_2$, then there is a canonical exact sequence of $\mathcal{O}_2'$-modules

$$\mathcal{I}/\mathcal{I}^2 \to \Omega_{\mathcal{O}_2/\mathcal{O}_1} \otimes_{\mathcal{O}_2} \mathcal{O}_2' \to \Omega_{\mathcal{O}_2'/\mathcal{O}_1} \to 0,$$

where the first map is characterized by mapping local sections f of $\mathcal{I}$ to $df \otimes 1$. ⌟

Proof: The first map is well-defined if $d(\mathcal{I}^2) = 0$. To show the exactness, let $\mathcal{O}_2'' \subset \mathcal{O}_2'$ to be the presheaf of $\mathcal{O}_1$-algebras that $\mathcal{O}_2''(U)$ the image of $\mathcal{O}_2(U) \to \mathcal{O}_2'(U)$. Then there is an exact sequence

$$\mathcal{I}(U)/\mathcal{I}(U)^2 \to \Omega_{\mathcal{O}_2(U)/\mathcal{O}_1(U)} \otimes_{\mathcal{O}_2(U)} \mathcal{O}_2''(U) \to \Omega_{\mathcal{O}_2''(U)/\mathcal{O}_1(U)} \to 0$$

by(5.4.3.8). Now shifification of these presheaves gives use the desired result by(6.2.4.3). □

Def. (6.2.4.7) [Sheaf of Differentials]. Let $(X, \mathcal{O}_X) \to (S, \mathcal{O}_S)$ be a morphism of ringed sites,

- Let $\mathcal{F}$ be an $\mathcal{O}_X$-module, an S-derivation from $\mathcal{O}_X$ to $\mathcal{F}$ is a derivation over $f^{-1}\mathcal{O}_S$. The set of S-derivations is denoted by $\mathrm{Der}_S(\mathcal{O}_X, \mathcal{F})$.
- the **sheaf of differentials** $\Omega_{X/S}$ is defined to be a sheaf of modules $\Omega_{\mathcal{O}_X/f^{-1}\mathcal{O}_S}$(6.2.4.2), with a universal derivation $d_{X/S} : \mathcal{O}_X \to \Omega_{X/S}$.

⌟

5 Locally Free sheaves

Prop. (6.2.5.1). Pullbacks of (finite)locally free sheaves are (finite)locally free. Sub-$\mathcal{O}_X$-modules of a (finite)locally free sheaf is (finite)locally free, by(3.2.4.21). ⌟

Prop. (6.2.5.2) [Finite Locally Free Sheaves and $\mathcal{H}om$]. For any finite locally free sheaf $\mathcal{E}$ on a ringed site $(\mathcal{C}, \mathcal{O})$:

- $\mathcal{E}^{\vee\vee} \cong \mathcal{E}$.
- $\mathcal{H}om_{\mathcal{O}}(\mathcal{E}, \mathcal{F}) \cong \mathcal{E}^\vee \otimes_{\mathcal{O}} \mathcal{F}$.
- $\mathcal{H}om_{\mathcal{O}}(\mathcal{F}, \mathcal{G}) \otimes \mathcal{H} \cong \mathcal{H}om_{\mathcal{O}}(\mathcal{F}, \mathcal{G} \otimes_{\mathcal{O}} \mathcal{H})$ if $\mathcal{F}$ or $\mathcal{H}$ is finite locally free.
- $\mathcal{H}om_{\mathcal{O}}(\mathcal{E} \otimes \mathcal{F}, \mathcal{G}) \cong \mathcal{H}om_{\mathcal{O}}(\mathcal{F}, \mathcal{E}^\vee \otimes \mathcal{G})$, by the first and(6.2.3.3).

⌟

Proof: We define the map, and verify locally, which is by1. □

Prop. (6.2.5.3). $\mathcal{H}om(\mathcal{H}, -)$ is exact for any locally free sheaf $\mathcal{H}$. ⌟

Invertible Sheaves

Def. (6.2.5.4)[Invertible Sheaf]. An **invertible sheaf** $\mathcal{L}$ on a ringed topoi $(\mathcal{S}h(\mathcal{C}), \mathcal{O})$ is an invertible object in the symmetric monoidal category $\mathcal{M}od_{\mathcal{O}}$(4.1.5.21). ⌟

Prop. (6.2.5.5). Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{L}$ an $\mathcal{O}$-module, the following are equivalent:

- $\mathcal{L}$ is an invertible sheaf.
- there exists some $\mathcal{O}$-module $\mathcal{N}$ that $\mathcal{L} \otimes_{\mathcal{O}} \mathcal{N} \cong \mathcal{O}$.

And in this case, $\mathcal{L}$ is flat and of finite presentation, and $\mathcal{N} \cong \mathcal{H}om_{\mathcal{O}}(\mathcal{L}, \mathcal{O})$. ⌟

Proof: $\mathcal{L}$ is flat because tensoring $\mathcal{L}$ is an equivalence thus exact. Let $\psi : \mathcal{L} \otimes_{\mathcal{O}} \mathcal{N} \cong \mathcal{O}$ the isomorphism, U an element of $\mathcal{C}$, then by construction of $\otimes$, after localization, we may assume there exists sections $x_i \in \mathcal{L}(U), y_i \in \mathcal{N}(U)$ that $\psi(x_i \otimes y_i) = 1$. Then there is an automorphism of $\mathcal{L}|_U : x \mapsto \sum \psi(x \otimes y_i) x_i$. This automorphism factors through

$$\mathcal{L}|_U \to \mathcal{O}_U^{\oplus n} \to \mathcal{L}|_U,$$

thus $\mathcal{L}|_U$ is a direct summand of a finite free $\mathcal{O}_U$-module, thus $\mathcal{L}$ is of finite presentation.

Assume $\mathcal{L}$ is invertible, consider the evaluation map

$$\mathcal{L} \otimes_{\mathcal{O}} \mathcal{H}om(\mathcal{L}, \mathcal{O}) \to \mathcal{O},$$

and by(6.2.3.3),

$$\mathrm{Hom}(\mathcal{O}, \mathcal{O}) = \mathrm{Hom}_{\mathcal{O}}(\mathcal{L} \otimes \mathcal{N}, \mathcal{O}) \to \mathrm{Hom}_{\mathcal{O}}(\mathcal{N}, \mathcal{H}om_{\mathcal{O}}(\mathcal{L}, \mathcal{O})).$$

The image of 1 gives a morphism $\mathcal{N} \to \mathcal{H}om_{\mathcal{O}}(\mathcal{L}, \mathcal{O})$. Tensoring $\mathcal{L}$ gives the inverse of the evaluation map. □

Cor. (6.2.5.6). The pullback of an invertible sheaf is an invertible sheaf, because tensoring commutes with pullbacks(6.2.2.12). ⌟

Def. (6.2.5.7) [Picard Groups]. For any ringed site $(\mathcal{C}, \mathcal{O})$, there is a set of invertible modules over $\mathcal{C}$ that any invertible module is isomorphic to exactly one of them. Then this set forms an Abelian group, called the **Picard group** $\mathrm{Pic}(\mathcal{O})$. ⌟

Prop. (6.2.5.8) [Invertible Sheaves and Locally Free Sheaves of Rank 1]. If $(X, \mathcal{O}_X)$ is a ringed space, then any locally free $\mathcal{O}_X$-module of rank 1 is invertible. And when $(X, \mathcal{O}_X)$ is a local ringed space, the converse holds as well. ⌟

Proof: Assume $\mathcal{L}$ is locally free of rank 1 and consider the evaluation map(6.2.3.1)

$$\mathcal{L} \otimes_{\mathcal{O}} \mathcal{H}om(\mathcal{L}, \mathcal{O}) \to \mathcal{O}.$$

This map is an isomorphism when restricting to any trivializing covering of $\mathcal{L}$, so it is an isomorphism. Thus $\mathcal{L}$ is invertible by(6.2.5.5).

Assume $(\mathcal{S}\mathrm{h}(\mathcal{C}), \mathcal{O})$ is a local ringed topoi and $\mathcal{L}$ is invertible, the proof of(6.2.5.5) shows there exists a covering $\{U_i \to U\}$ that $\mathcal{L}|_{U_i}$ is a direct summand of a finite free $\mathcal{O}_{U_i}$-module. Replacing U_i by U, let π be the projection of $\mathcal{O}_U^r$ onto $\mathcal{L}|_U$ which corresponds to a matrix with entries in $\mathcal{O}(U)$. The image of π acting on $\mathcal{O}(U)^r$ is a finite free $\mathcal{O}(U)$-module M, thus there are $f_1, \ldots, f_t$ generating unit ideal of $\mathcal{O}(U)$ such that M_{f_i} is finite free. Now by definition of local ringed topoi(6.2.1.6), after replacing U by a covering, we may assume M is finite free, which means $\mathcal{L}|_U$ is free summand of $\mathcal{O}_U^r$. But $\mathcal{L}$ is invertible, thus rank of $\mathcal{L}$ is 1. □

Prop. (6.2.5.9). Let X be a locally ringed space and $\mathcal{L} \in \mathrm{Pic}(X)$ that is generated by global sections $s_0, \ldots, s_n$. If $\mathcal{F}$ is the kernel of the map $\mathcal{O}_X^{\oplus n+1} \to \mathcal{L}$, then $\mathcal{F} \otimes \mathcal{L}$ is globally generated. ⌟

Proof: $\mathcal{F}$ is finite locally free of rank n by(6.2.5.1). The elements

$$s_{ij} = (0, \ldots, 0, s_j, 0, \ldots, 0, s_i, , \ldots, 0) \in \Gamma(X, \mathcal{L}^{\oplus n+1})$$

is in $\Gamma(X, \mathcal{F} \otimes \mathcal{L})$, and it can be verified locally s.t. they generate $\mathcal{F} \otimes \mathcal{L}$. □

6 Sheaves on Spaces

Sheaves on Topological Spaces

Remark (6.2.6.1). A topological space can be regarded as a ringed space by assigning the locally constant sheaf $\underline{\mathbb{Z}}$ as the structure sheaf. ⌟

Def. (6.2.6.2) [Grothendieck's Six Operators]. Let $f : X \to Y$ be a continuous map of topological spaces, then the inverse image defines a continuous map between sites $Y_{Zar} \to X_{Zar}$, so by(6.1.2.9) and(6.1.2.11) we can define

- the **pushforward** $f^p F$, $f^p F(U) = F(f^{-1}(U))$ sends presheaf to presheaf.
- the **direct image** $f_* \mathcal{F}$, $f_* \mathcal{F}(U) = \mathcal{F}(f^{-1}(U))$ sends sheaf to sheaf.
- the **inverse image** $f_p \mathcal{G}$, $f_p \mathcal{G}(U) = \varinjlim_{f(U) \subset V} \mathcal{G}(V)$ that sends presheaf to presheaf.
- the **inverse image** $f^{-1} \mathcal{G} = f_s(\mathcal{G})$ that sends sheaf to sheaf.
- For a morphism of locally compact spaces, we can define a **proper direct image**:

$$f_!(\mathcal{F})(U) = \{s \in \Gamma(f^{-1}(U), \mathcal{F}) |\, \mathrm{Supp}(s) \to U \text{ proper}\}$$

This is a subsheaf of $f_* \mathcal{F}$ and it is left exact. we denote $\Gamma_c(X, \mathcal{F})$ as the group $f_!(\mathcal{F})$ where $f : X \to \mathrm{pt}$. And the stalk $f_!(\mathcal{F})_y = \Gamma_c(f^{-1}(y), \mathcal{F}|_{f^{-1}(y)})$ Cf.[Gelfand P224 P225].

- the **proper inverse image** (special case) $i^!$ for a closed immersion $Z \subset X$ defined by

$$i^!(\mathcal{F})(U = V \cap Z) = \{s \in \Gamma(V, \mathcal{F}) | \operatorname{Supp}(s) \in Z\}.$$

  sends Abelian sheaves to Abelian sheaves.
- the internal tensor product.
- the internal Hom.

⌟

Proof: Check that $f_!$ is a sheaf: it is separated clearly, it suffices to show that for a covering $\cup U_i = W$ and $\xi_i \in F(f^{-1}(U_i))$, the section $\xi \in F(f^{-1}(W))$ they generated by sheaf property of F is in $f_! F(W)$. For a compact subset K, there is a finite cover $\cup_i U_i$ of it, thus $K - \cup_{i\neq j} U_j$ is compact in U_j, thus its inverse image is compact in $\operatorname{Supp}(\xi)$. there are f.m. U_j, thus the inverse image of K is compact in $\operatorname{Supp}(\xi)$. □

Def. (6.2.6.3) [Stalks]. The convenience of rings spaces compared to the case of sites is the it has stalk functors: For any presheaf $\mathcal{F}$ on X and a point $i : x \to X$, define the **stalk** $\mathcal{F}_x = i_p(\mathcal{F})$(6.2.6.2). ⌟

Prop. (6.2.6.4) [Stalks Commutes with Shifification]. Taking stalks commutes with shifification. ⌟

Proof: Cf.[Sta]007Z. □

Prop. (6.2.6.5). If a sheaf on a ringed space has only one non-vanishing stalk, then it is a skyscraper sheaf. (Because the restriction map to that point for every open set is an isomorphism). ⌟

Prop. (6.2.6.6)[Stalks]. Taking stalks is a left adjoint to the skyscraper sheaf from Presheaves to Sets, thus it preserves cokernel. Moreover, for a map of sheaves $\mathcal{F} \to \mathcal{G}$ on X,

- φ is a monomorphism iff φ_x is injective for all $x \in X$.
- φ is an epimorphism iff φ_x is surjective for all $x \in X$.
- φ is an isomorphism iff φ_x is surjective for all $x \in X$.

⌟

Proof: 1: If φ is a monomorphism, then φ_x is clearly. Conversely, if φ_x are all injective, if $s \in \mathcal{F}(U)$ mapsto $0 \in (U)$, then s_x mapsto $0 \in \mathcal{G}_x$ for all x, thus $s_x = 0$ for all x, thus $s = 0$.

2: If φ is an epimorphism, then φ_x is surjective by definition. The converse is also true.

3: If φ_x is isomorphism for all x, then φ is monomorphism by 1, and for any $t \in \mathcal{G}(U)$, t is locally coming from some section of s, and these sections are compatible on their intersections because of monomorphism, so they glue together to a section $s \in \mathcal{F}(U)$ that $\varphi(U)(s) = t$. □

Prop. (6.2.6.7) [Topological Spaces and Sites]. Let $f : X \to Y$ be a continuous map of topological spaces, then f induces a map of sites $X \to Y$ because f^{-1} is exact(6.1.2.14), thus induces a map of topoi $f : \mathcal{S}\mathrm{h}(X) \to \mathcal{S}\mathrm{h}(Y)$(6.1.2.20). ⌟

Cor. (6.2.6.8). Let $f : X \to Y$ be a continuous map of topological spaces,

- Let $\mathcal{G}$ be a presheaf on Y, then there is a canonical bijection of stalks $(f_p(\mathcal{G}))_x = \mathcal{G}_{f(x)}$. If $\mathcal{G}$ is a sheaf on Y, then there is a canonical bijection of stalks $(f^{-1}(\mathcal{G}))_x = \mathcal{G}_{f(x)}$.
- f^{-1} is left adjoint to f_*.

- $f_!$ is left exact when X,Y are locally compact. And $j_!$ is left adjoint to the functor j^{-1} for an inclusion of open subset $j: U\subset X$.
- $i^!$ is right adjoint to i_* for a closed immersion $i: Z\to X$, in particular i_* is exact when i is a closed immersion.

⌟

Proof: 1: This is because $(-)_p$ commutes with composition(6.2.6.3), and also shifification commutes with $(-)_p$(6.2.6.4).

2: This is immediate.

3:

4: The adjointness follows form the fact that any section under a homomorphism $i_*\mathcal{G}\to\mathcal{F}$ has support contained in Z. □

Prop. (6.2.6.9). Let $i: Z\to X$ be a closed immersion, then the functor $i_*: \mathcal{A}\mathrm{b}(Z)\to\mathcal{A}\mathrm{b}(X)$ is exact, fully faithful, with the essential image those sheaves with support in Z. ⌟

Prop. (6.2.6.10) [Canonical Exact Sequences]. We have a canonical exact sequences of sheaves of modules:

$$0\to j_!(\mathcal{F}|_U)\to\mathcal{F}\to i_*(\mathcal{F}|_Z)\to 0$$

$$0\to i_*i_Y^!\mathcal{F}\to\mathcal{F}\to j_*(\mathcal{F}|_U)\to 0$$

(check on stalks), which is important to use reduction to calculate sheaf cohomology. The latter induces long exact sequences:

$$0\to H^0_Y(X,\mathcal{F})\to H^0(X,\mathcal{F})\to H^0(U,\mathcal{F}|_U)\to H^1_Y(X,\mathcal{F})\to\cdots$$

⌟

Proof: Cf.[Sta]02UT. □

Prop. (6.2.6.11). On a topological space X, for a qc open subset U, $(\oplus\mathcal{F}_i)(U)=\oplus\mathcal{F}_i(U)$. This uses the compactness of U. ⌟

Morphisms of Local Ringed Spaces

Def. (6.2.6.12)[Open Immersion of Ringed Spaces]. A morphism $f:(X,\mathcal{O}_X)\to(Y,\mathcal{O}_Y)$ of ringed spaces is called an **open immersion** if f is a homeomorphism of X onto an open subset of Y, and the map $f^\sharp: f^{-1}(\mathcal{O}_Y)\to\mathcal{O}_X$ is an isomorphism. ⌟

Prop. (6.2.6.13). Let $(X,\mathcal{O}_X)$ be a ringed space, $U\subset X$ an open subset, and $\mathcal{O}_U=\mathcal{O}_X|_U$ is a sheaf of rings on U, then $(U,\mathcal{O}_U)\to(X,\mathcal{O}_X)$ is an open immersion, and $(U,\mathcal{O}_U)$ is called the **open subspace** associated to U. ⌟

Prop. (6.2.6.14) [Universal Property of Open Immersions]. Let $f:(X,\mathcal{O}_X)\to(Y,\mathcal{O}_Y)$ be an open immersion of ringed spaces, then it has the universal property that any morphism of ringed spaces $(T,\mathcal{O}_T)\to(Y,\mathcal{O}_Y)$ that factors set-theoretically through $f(X)$ factors uniquely through $(X,\mathcal{O}_X)$. ⌟

Def. (6.2.6.15) [Closed Immersion]. Let $i: Z\to X$ be a morphism of local ringed spaces, then i is called a **closed immersion** if:

- i is a homeomorphism of Z onto a closed subspace of X.
- the map $\mathcal{O}_X \to i_*\mathcal{O}_Z$ corresponding to $f^\sharp$ is surjective with kernel $\mathcal{I}$.
- the $\mathcal{O}_X$-module $\mathcal{I}$ is locally generated by sections.

And for a closed immersion, $\mathcal{I}$ is called the **ideal sheaf** of i. ⌟

Def. (6.2.6.16) [Closed Immersion Defined by Ideals]. Let $(X, \mathcal{O}_X)$ be a local ringed space, and $\mathcal{I} \subset \mathcal{O}_X$ a sheaf of ideals on X locally generated by sections , Let Z be the support of the sheaf of rings $\mathcal{O}_X/\mathcal{I}$. Z is closed in X because it is the support of 1. by(6.2.6.9), there is a unique sheaf of rings $\mathcal{O}_Z$ on Z that $i_*\mathcal{O}_Z = \mathcal{O}_X/\mathcal{I}$. For any $z \in Z$, the stalk $\mathcal{O}_z = \mathcal{O}_{X,z}/\mathcal{I}_z$ is a quotient of a local ring and is non-zero, thus a local ring. Then $(Z, \mathcal{O}_Z)$ is a local ringed space and $i : (Z, \mathcal{O}_Z) \to (X, \mathcal{O}_X)$ is a closed immersion, called the **closed immersion defined** $\mathcal{I}$. ⌟

Prop. (6.2.6.17) [Closed Immersions are Equivalent to Ideals]. Let $f : X \to Y$ be a closed immersion of local ringed spaces with ideal sheaf $\mathcal{I}$. Let $i : Z \to X$ be the closed immersion defined by $\mathcal{I}$(6.2.6.16), then f is isomorphic to i. ⌟

Proof: Because $f_*\mathcal{O}_Z \cong \mathcal{O}_X/\mathcal{I}$ on X. □

Prop. (6.2.6.18). For a closed immersion of ringed spaces f, f_* on $\mathcal{O}_X$-mod is fully faithful, with image those modules annihilated by $\mathcal{I}$, where $\mathcal{I}$ is the structural kernel. ⌟

Proof: Cf.[Sta]08KS. □

7 Spec and Schemes

Def. (6.2.7.1)[Spectrum]. Given a commutative ring A, the **spectrum** of A Spec A is a locally ringed space whose underlying space is the set of primes of A, and the topology is generated by the standard open subsets $D(f) = \{\mathfrak{p} | f \notin \mathfrak{p}\}$.

To define the structure sheaf $\mathcal{O}_X$, we first define a sheaf on the site of standard open subsets, which takes value R_f on $D(f)$. This is truly a sheaf by(5.4.2.3), and then we can use(6.1.2.25) to extend this sheaf to a sheaf on Spec A, called the structure sheaf $\mathcal{O}_X$.

A locally ringed space of the form Spec A is called an **affine scheme**. The category of affine schemes is denoted by $\mathcal{A}\mathrm{ff}$. ⌟

Def. (6.2.7.2)[Schemes]. The category $\mathcal{S}\mathrm{ch}$ of **schemes** is the full subcategory of the category of local ringed spaces(6.2.1.10) consisting of local ringed spaces that are locally isomorphic to Spec A. ⌟

Lemma (6.2.7.3). If X is a local ringed space, $x \in X$, and $Y = \mathrm{Spec}\, A$ an affine scheme, $f : X \to Y$ is a morphism, consider the ring map $\Gamma(X, \mathcal{O}_X) \xrightarrow{f^\sharp} \Gamma(Y, \mathcal{O}_Y) \to \mathcal{O}_{X,x}$, and consider the inverse image $\mathfrak{p}$ of $\mathfrak{m}_x$, which corresponds to $y \in Y$, then $f(x) = y$. ⌟

Proof: There are commutative diagrams

$$\begin{array}{ccc} \Gamma(Y, \mathcal{O}_Y) & \longrightarrow & \mathcal{O}_{Y,f(x)} \\ \downarrow & & \downarrow \\ \Gamma(X, \mathcal{O}_X) & \longrightarrow & \mathcal{O}_{X,x} \end{array}$$

and the map of local rings is a local ring map. So the inverse image of $\mathfrak{m}_x$ is just $\mathfrak{m}_{f(x)}$, so $\mathfrak{m}_{f(x)} = \mathfrak{m}_y$.
□

Prop. (6.2.7.4). Let X be a local ringed spaces and $Y = \operatorname{Spec} A$ an affine scheme, then the map $\operatorname{Hom}(X, \operatorname{Spec} A) \to \operatorname{Hom}(A, \Gamma(X, \mathcal{O}_X))$ is an isomorphism. ⌟

Proof: The inverse map is constructed as follows: for any $\varphi : A \to \Gamma(X, \mathcal{O}_X)$ and $x \in X$, define $\Phi(x)$ to be the point corresponding to the inverse image of $\mathfrak{m}_x$ in $A \to \Gamma(X, \mathcal{O}_X) \to \mathcal{O}_{X,x}$. In this way, $\Phi^{-1}(D(f))$ is just $D(\varphi(f)) \subset X$ which is open, thus Φ is continuous. Now we want to construct a sheaf homomorphism $f^{-1}(\mathcal{O}_Y) \to \mathcal{O}_X$, and it suffices to construct compatible maps on the affine open basis $D(f)$, by(6.1.3.17). Now $\Gamma(D(f), \mathcal{O}_Y) = A_f$, and because f is invertible on $D(\varphi(f))$, there is by universal property a unique map $A_f \to D(\varphi(f))$ extending φ. Then by universal property these maps are compatible. Notice the construction here also shows the homomorphism is determined by the map set-theoretically.

Finally, we need to show this induces a local ring map on the stalks, and this is quite obvious from the definition.

Then we show these two maps are inverse to each other: It suffices to show any ring map $A \to \Gamma(X, \mathcal{O}_X)$ comes uniquely from a map $X \to Y$: the uniqueness is proven by(6.2.7.3), and the sheaf homomorphism is determined by the set-theoretical map by the above argument. □

Cor. (6.2.7.5) [Adjointness of Spec and Γ]. The Spec operator $\operatorname{Spec} : \mathcal{CA}\mathrm{lg}^{op} \to \mathcal{S}\mathrm{ch}$ is right adjoint to $X \to \Gamma(X, \mathcal{O}_X)$:

$$\operatorname{Hom}_{\mathcal{S}\mathrm{ch}}(X, \operatorname{Spec}(A)) \cong \operatorname{Hom}_{\mathcal{CA}\mathrm{lg}}(A, \Gamma(X, \mathcal{O}_X)).$$

Notice the category of schemes is a full subcategory of the category of locally ringed spaces. ⌟

Cor. (6.2.7.6). $\mathcal{A}\mathrm{ff}$ is equivalent to $\mathcal{CA}\mathrm{lg}^{op}$. ⌟

Prop. (6.2.7.7) [Points of Schemes]. Let X be a scheme and R a local ring, then there is a natural bijection between morphisms $\operatorname{Spec} R \to X$ and pairs (p, φ) where $p \in X$ is a point and $\varphi : \mathcal{O}_{X,x} \to R$ is a local ring map. ⌟

Proof: Consider where the closed point of $\operatorname{Spec} R$ is mapped to and choose an affine open nbhd of that point, then we reduce to the affine case, which is by(6.2.7.5). □

Cor. (6.2.7.8). if $f : Y \to X$ is a morphism of schemes that $f(y) = x$, then we have a commutative diagram

$$\begin{array}{ccc} \mathcal{O}_{Y,y} & \longrightarrow & Y \\ \downarrow & & \downarrow \\ \mathcal{O}_{X,x} & \longrightarrow & X \end{array}$$

⌟

Cor. (6.2.7.9). The points of X are in bijection with equivalent classes of morphisms from the spectra of fields to X, and each equivalent class contains a minimal element $\operatorname{Spec} k(x) \to X$. ⌟

Proof: This is because a local ring map from $\mathcal{O}_{X,x}$ to a field factors through $k(x)$. □

Prop. (6.2.7.10). The closure of a subset T of $\operatorname{Spec}(A)$ is $V(\cap p, p \in T)$. ⌟

Prop. (6.2.7.11) [Scheme is Sober]. The underlying space of a scheme is sober. ⌟

Proof: Firstly this is true for affine schemes, by(4.12.4.13). Then notice for any affine open subscheme U, the generic point for $Z \cap U$ is the generic point for Z. □

Construction of Schemes

Prop. (6.2.7.12) [Global Spec]. There is an S-scheme $f : \mathbf{Spec}_S \mathcal{A} \to S$ for every Qco sheaf of $\mathcal{O}_S$-algebras $\mathcal{A}$ on S that for any affine open subscheme $U \subset X$, $f^{-1}(U) \cong \operatorname{Spec} \mathcal{A}(U)$ over U. This construction is right adjoint to the direct image map:

$$\operatorname{Hom}_{\mathcal{C}\mathcal{A}\mathrm{lg}_{\mathcal{O}_S}}(\mathcal{A}, \pi_*\mathcal{O}_X) \cong \operatorname{Hom}_{\mathcal{S}\mathrm{ch}\,/S}(X, \mathbf{Spec}_S \mathcal{A}).$$

and defines an equivalence of affine morphisms over S and Qco $\mathcal{O}_S$-algebras. Moreover, this defines an equivalence of the category of $\mathcal{A}$-modules and the category of $\mathcal{O}_{\mathbf{Spec}\,\mathcal{A}}$-modules. ⌟

Proof: Choose an affine open covering $\{U_i \to X\}$ of X, and consider the schemes $\operatorname{Spec} \mathcal{A}(U_i) \to U_i$ over U_i, then their restrictions to U_{ij} are compatible, because this is true after further restriction to an affine open covering of U_{ij}, we can use(6.1.5.4). Then we can use(6.1.5.4) to get an S-scheme $f : \mathbf{Spec}_S \mathcal{A} \to S$ that $f^{-1}(U_i) \cong \operatorname{Spec} \mathcal{A}(U_i)$.

Now we check that for any affine open subset $U \subset X$, $f^{-1}(U) \cong \operatorname{Spec} \mathcal{A}(U)$ over U. But this is true after base change to $U_i \cap U$ for any i, so it is true, by(6.1.5.4).

To show the adjointness condition, by(6.1.5.4), it suffices to show canonical(thus compatible) isomorphism for S affine. In this case, this reduces to(6.2.7.5). □

Cor. (6.2.7.13). Let S be a scheme and $\mathcal{A}$ is a Qco sheaf of $\mathcal{O}_S$-algebras, then

- For any morphism $g : S' \to S$, $S' \times_S \mathbf{Spec}_S(\mathcal{A}) \cong \mathbf{Spec}_{S'}(g^*\mathcal{A})$.
- The natural map $\mathcal{A} \to \pi_*\mathcal{O}_{\mathbf{Spec}_S(\mathcal{A})}$ is an isomorphism of $\mathcal{O}_S$-algebras.

⌟

Proof: 1: It can be checked that $S' \times_S \mathbf{Spec}_S(\mathcal{A})$ and $\mathbf{Spec}_{S'}(g^*\mathcal{A})$ satisfy the same universal property.

2: It suffices to check on affine opens, then it is trivial. □

Lemma (6.2.7.14) [Affine Case]. Fiber product of affine schemes is also affine that corresponds to the tensor product of their corresponding rings, by(6.2.7.5). ⌟

Prop. (6.2.7.15) [Finite Limits of Schemes]. Fiber products exist in the category of schemes, and there is a final object $\operatorname{Spec} \mathbb{Z}$, so arbitrary limits exist in the category of schemes(4.1.1.47).

In fact, finite limits exists in the category of ringed spaces, and finite limits of schemes coincide with finite limits as ringed spaces. ⌟

Proof: Let $f : X \to S, g : Y \to S$, and U_i is an affine open covering of S, V_ij is an affine open covering of $f^{-1}(U_i)$ and W_{ik} is an affine open covering of $g^{-1}(U_i)$, then we can check $h_{V_{ij}} \times_{h_{U_i}} h_{W_{ik}}$ is a covering of $h_X \times_{h_S} h_Y$ by representable open subfunctors(9.7.0.1), by(6.2.7.14), thus it is representable. □

Cor. (6.2.7.16) [Open Subschemes]. Let $X \to S, Y \to S$, and $V \subset X, W \subset Y$ be open subschemes mapping into open subscheme $U \subset S$, then there is a natural open immersion $V \times_U W \to X \times_S Y$ with image $\pi_1^{-1}V \cap \pi_2^{-1}(W)$. ⌟

Proof: There is a natural map $V \times_U W \to X \times_S Y$ by Yoneda lemma, and this map has the universal property that any map $f : (T, \mathcal{O}_T) \to X \times_S Y$ that $\pi_1 \circ f$ has image in V and $\pi_2 \circ f$ has image in W factors uniquely through $V \times_U W$. But so does the open immersion $\pi_1^{-1}V \cap \pi_2^{-1}(W) \to X \times_S Y$(6.2.6.14), so they are equal. □

Cor. (6.2.7.17). Let $f : X \to S, g : Y \to S$, and U_i is an affine open covering of S, V_ij is an affine open covering of $f^{-1}(U_i)$ and W_{ik} is an affine open covering of $g^{-1}(U_i)$, then

$$X \times_S Y = \cup_i \cup_{j,k} V_{ij} \times_{U_i} W_{ik}$$

is an affine open covering of $X \times_S Y$.

Also, the structure sheaf of $X \otimes_S Y$ is given by $\mathcal{O}_{X\times_S Y} = \pi_1^{-1}\mathcal{O}_X \otimes_{\pi^{-1}\mathcal{O}_S} \pi_2^{-1}\mathcal{O}_Y$. ⌟

Cor. (6.2.7.18). The equalizer of two morphisms from X to Y exists, it is a locally closed subscheme of X, and it is a closed subscheme of X if Y is separated. ⌟

Proof: because it is the base change of $\Delta : Y \to Y \times Y$(4.1.1.47), then use(6.4.4.76). □

Remark (6.2.7.19) [Infinite Product of Schemes Doesn't Exists]. WARNING: infinite products of schemes may not exists, Cf.[Sta]0CNH. Intuitively, if you want to glue affine products together, you will notice you can identify only those products that is equal a.e.. ⌟

Remark (6.2.7.20). Let X be a scheme over S and $S' \to S$ is a morphism of schemes, then we sometimes denote $X \times_S S'$ by $X_{S'}$, if no confusion is caused. ⌟

Def. (6.2.7.21) [Generic Fibers and Special Fibers]. If X is a scheme over an integral ring A, then the **generic fiber** of X/A is the stalk X_η, where $\eta = (0) \in \operatorname{Spec} A$.

If X is a scheme over a ring R, a **special fiber** is the stalk of X over a maximal ring $\mathfrak{m}$. ⌟

8 Rational Maps

Def. (6.2.8.1) [Rational Maps]. Let $X, Y \in \mathcal{S}\mathrm{ch}/S$ and Y/S separated, a **rational map** over S $f : X \to Y$ is an equivalence class of maps $U \to Y$ over S where U is an open dense subset of X. A **rational function** on X is a rational map $X \to \mathbb{A}^1$. It has a ring structure. The ring of rational functions is denoted by $R(X)$.

Because two rational maps are equivalent iff they are compatible on the intersection of their domain as Y/S is separated, a rational map $\varphi : X \to Y$ has a maximal domain of definition, denoted by $\mathrm{dom}(\varphi)$. ⌟

Prop. (6.2.8.2). If X is a scheme with f.m. generic points η_i, then

$$R(X) = \prod \mathcal{O}_{X,\eta_i}.$$

⌟

Proof: Cf.[Sta]01RV. □

Def. (6.2.8.3) [Birational Maps]. $X, Y \in \mathcal{S}\mathrm{ch}/S$ are called **birational** over S if they are isomorphic in the category of S-schemes with dominant rational maps. ⌟

Prop. (6.2.8.4). Two schemes X, Y over S are birational over S iff there are nonempty open subschemes $U \subset X, V \subset Y$ that are isomorphic over S. ⌟

Proof: □

Def. (6.2.8.5) [S-Dense Subsets]. Let $X \in \mathcal{S}\mathrm{ch}/S$, a subscheme $U \subset X$ is called S**-dense** if U_s is dense in X_s for any $s \in S$. ⌟

Prop. (6.2.8.6). Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{pf}}/S$ and $V \subset X$ is a qc open subscheme, then the set of points $s \in S$ s.t. $V_s \subset X_s$ is not dense is locally constructible in S. And if V is S-dense in X, then it is also schematically dense in X. ⌟

Proof: Cf.[?]P56. □

Prop. (6.2.8.7). If $X \in \mathcal{S}\mathrm{ch}_{qc}/S$ and $U \subset X$ is an S-dense open subscheme, then U contains an S-dense open subscheme of S that is qc. ⌟

Proof: Cf.[?]P56. □

Def. (6.2.8.8) [S-Rational Maps]. Let $X, Y \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,loc.pf}}/S$ an **S-rational map** $f : X \to Y$ is an equivalence class of maps $U \to Y$ over S where U is an open subset of X that is S-dense.

Because two rational maps are equivalent iff they are compatible on the intersection of their domain as Y/S is separated, a rational map $X \to Y$ has a maximal domain of definition. ⌟

Def. (6.2.8.9) [S-Birational Maps]. Let $X, Y \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,loc.pf}}/S$ are called **S-birational** if they are isomorphic in the category of S-schemes with dominant S-rational maps. ⌟

Prop. (6.2.8.10). The notion of S-rational and S-birational maps are stable under base change, because a base change of fields is flat locally of f.p. thus open. ⌟

Prop. (6.2.8.11) [Faithfully Flat Descent]. Let $X', X, Y \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,loc.pf}}/S$ and $\varphi : Y \to S$ an S-rational map,

- If $f : X' \to X$ flat, then $\varphi \circ f$ is an S-rational map $X' \to Y$, and $\mathrm{dom}(\varphi \circ f) = f^{-1}(\mathrm{dom}(\varphi))$. In particular, if f is f.f. and $\varphi \circ f$ is a morphism, then φ is also a morphism.
- If $T \to S$ is flat, then the base change $\varphi_T : X_T \to Y_T$ satisfies $\mathrm{dom}(\varphi_T) = \mathrm{dom}(\varphi) \times_S T$.

⌟

Proof: Cf.[BLR90]P58. □

9 Associated Points

Main References are [Sta]Chap30.

Def. (6.2.9.1). For a scheme X and a Qco sheaf $\mathcal{F}$ on X, a point is called **associated to $\mathcal{F}$** iff $\mathfrak{m}_x$ is associated to $\mathcal{F}_x$, which is equivalent to $\mathfrak{m}_x$ are all zero-divisors in M by(5.2.5.18). When $\mathcal{F} = \mathcal{O}_X$, x is called an **associated point of X**. ⌟

Prop. (6.2.9.2). If X is locally Noetherian, then an associated prime is equivalent to it is an associated prime of $\Gamma(X, \mathcal{O}_X)$ of $\Gamma(U, \mathcal{F})$ for a nbhd U of x. ⌟

Proof: Cf.[[Sta]02OK]. □

Prop. (6.2.9.3). Same results of associated points are parallel to the discussion of associated primes:

- relations of $Ass(\mathcal{F})$ w.r.t exact sequences(5.2.5.14).
- $Ass(\mathcal{F}) \subset \mathrm{Supp}(\mathcal{F})$(5.2.5.16).
- When $X \in \mathrm{N}\mathcal{S}\mathrm{ch}$ and $\mathcal{F}$ is coherent, for a quasi-compact open set U of X, the number of associated points in U is finite(5.2.5.16).
- When $X \in \mathrm{N}\mathcal{S}\mathrm{ch}$, $\mathcal{F} = 0$ iff $\mathrm{Asso}(\mathcal{F})$ is empty(5.2.5.16).

- When $X \in \mathrm{N}\,\mathcal{S}\mathrm{ch}$, If $\mathrm{Asso}(\mathcal{F}) \subset$ an open subset U, then $\Gamma(X,\mathcal{F}) \to \Gamma(U,\mathcal{F})$ is injective(5.2.5.22).
- If $X \in \mathrm{N}\,\mathcal{S}\mathrm{ch}$, then the minimal elements(under specialization) of $\mathrm{Supp}(\mathcal{F})$ are associated points of $\mathcal{F}$. in particular, any generic point of an irreducible component of X is an associated points of X.
- If $X \in \mathrm{N}\,\mathcal{S}\mathrm{ch}$, then if a map $\varphi : \mathcal{F} \to \mathcal{G}$ that is injective at all the stalks of $Ass(\mathcal{F})$, then φ is injective.

⌟

10 Others

Frobenius

Def. (6.2.10.1) [Frobenius]. Let $k \cong \mathbb{F}_{p^r} \in$ p-`Field`, $X_0 \in \mathcal{S}\mathrm{ch}\,/k$, $X = X_0 \otimes_k \overline{k}$,

- The **absolute Frobenius** for X or X_0 is the automorphism $\varphi_{r,X} : X \to X$ that is the p^r-th power on $\mathcal{O}_X$.
- $F_X = \mathrm{id}_{X_0} \times_k \varphi_k^{-1}$, called the **arithmetic Frobenius**, which is not k-linear!
- $\mathrm{Fr}_X = \varphi_{X_0} \times_k \mathrm{id}_{\overline{k}} : X \to X$, which is $\overline{k}$-linear, called the **geometric Frobenius**.
- Let U be a X_0-scheme, then the **relative Frobenius** $F_{U/X_0,r} : U \to \varphi_{r,X_0}^*(U)$ is defined by the universal property of the base change of U by $\varphi_{X_0}^r$. $F_{U/X_0,1}$ is denoted by F_{U/X_0}.

⌟

Prop. (6.2.10.2). $\mathrm{Fr}_X = \varphi_{r,X} \circ F_X : X \to X$. ⌟

Proof: Easy. □

Prop. (6.2.10.3). F_{U/X_0} is a universal homeomorphism. In particular, if $U \to X_0$ is étale, then it is an isomorphism. ⌟

Proof: Because $U \to X, X \times_{\varphi_X,X} U \to X$ are both étale, F_U/X_0 is étale. And from the fact both both φ_{X_0} and φ_{U_0} are universally bijective, we see F_{U_0/X_0} is universally bijective. So it must be an isomorphism**?**. □

Prop. (6.2.10.4). If $k \in$ p-`Field` and $X \in \mathcal{S}\mathrm{ch}\,/k$, then $X^{(p)}$ is reduced iff X is geo.reduced. This follows from(6.4.3.2). ⌟

6.3 Cohomology on Ringed Sites

Main references are [Sta], [Har77] and [Sheaf Cohomology, Anonymous]. Should be refreshed with the language of ∞-categories**?**

Notation (6.3.0.1).

- We use notations defined in Sites, Sheaves, Topoi and Stacks.

⌟

1 Derived Cohomology

$D(\mathcal{M}\mathrm{od}(\mathcal{O}))$

Def. (6.3.1.1) [Setups]. Let $(\mathcal{C},\mathcal{O})$ be a ringed site, write $K(\mathcal{O})=K(\mathcal{M}\mathrm{od}(\mathcal{O})), D(\mathcal{O})=D(\mathcal{M}\mathrm{od}(\mathcal{O}))$. The Abelian category $\mathcal{M}\mathrm{od}(\mathcal{O})$ contains enough injectives by(4.8.3.29) and(4.8.3.23), so we can consider right derived functor for any left exact functor.

1. (Hom) Let K be a presheaf of sets on $\mathcal{C}$, then $\mathcal{F}\mapsto \mathrm{Hom}_{\mathcal{PS}\mathrm{h}(\mathcal{C})}(K,\mathcal{F})$ is a left exact functor $\mathcal{M}\mathrm{od}(\mathcal{O})$ to $\mathcal{A}\mathrm{b}$, thus we denote its derived functors as $H^i(K,\mathcal{F})$.
2. (Section) The **section functor** $\Gamma(U,\mathcal{F})$ is the left exact functor $\mathcal{M}\mathrm{od}(\mathcal{O})\to\mathcal{M}\mathrm{od}(\mathcal{O}(U))$ and call the derived functors $H^i(U,\mathcal{F})=H^i(R\Gamma(U,\mathcal{F}))$ as the **i-th cohomology** of $\mathcal{F}$ at U. In fact, this functor is just $\mathrm{Mor}_{\mathcal{PS}\mathrm{h}(\mathcal{C})}(h_U,\mathcal{F})$ defined in(6.3.1.1).
3. (Global Section) Let e be the final object in $\mathcal{PS}\mathrm{h}(\mathcal{C})$, then we define the **global section** functor $\Gamma(\mathcal{C},-)$ to be the left exact functor $\mathcal{M}\mathrm{od}(\mathcal{O})\to Ab:\mathcal{F}\to\mathrm{Mor}_{\mathcal{PS}\mathrm{h}(\mathcal{C})}(e,\mathcal{F})=\varprojlim_{X\in\mathcal{C}^{op}}\Gamma(X,\mathcal{F})$, then we define its derived functor $R(\mathcal{C},\mathcal{F})$, and call the derived functors $H^i(\mathcal{C},\mathcal{F})=H^i(R\Gamma(\mathcal{C},\mathcal{F}))$ the **i-th cohomology groupg** of $\mathcal{F}$ on $\mathcal{C}$.
4. (Pushforward) Let $(\mathcal{S}\mathrm{h}(\mathcal{C}),\mathcal{O})\to(\mathcal{S}\mathrm{h}(\mathcal{D}),\mathcal{O}')$ be a morphism of topoi, then f_* is a left exact functor from $\mathcal{M}\mathrm{od}(\mathcal{O})$ to $\mathcal{M}\mathrm{od}(\mathcal{O}')$(6.1.2.18), and we call its derived functors R^if_* the **i-th higher direct images**.
5. (Shifification) Let shifification functor $\iota:\mathcal{PS}\mathrm{h}(\mathcal{C})\to\mathcal{S}\mathrm{h}(\mathcal{C})$ is left exact, and we call the derived functors $\mathcal{H}^p(F)$ the **sheaf-cohomology presheaves** of F.

⌟

Def. (6.3.1.2) [$\mathbb{G}_a,\mathbb{G}_m$]. Let $(\mathcal{C},\mathcal{O})$ be a ringed site, denote $\mathbb{G}_{a,\mathcal{C}}=\mathcal{O},\mathbb{G}_{m,\mathcal{C}}=\mathcal{O}^*$. ⌟

Prop. (6.3.1.3) [Global Section as Pushforward]. For a ringed site $(\mathcal{C},\mathcal{O})$, if we endow $\mathcal{C}$ with the discrete topology, then there is a functor $\mathcal{C}\to\mathrm{pt}$ which is cocontinuous, thus induce a morphism of ringed topoi $\pi:(\mathcal{S}\mathrm{h}(\mathcal{C}),\mathcal{O})\to(\mathcal{S}\mathrm{h}(\mathrm{pt})\cong\mathcal{A}\mathrm{b},\Gamma(\mathcal{C},\mathcal{O}))$(6.1.2.21). Then π_* is exactly $\mathcal{F}\mapsto\Gamma(\mathcal{C},\mathcal{F})$, so $R\pi_*\mathcal{F}=H^i(\mathcal{C},\mathcal{F})$. ⌟

Prop. (6.3.1.4) [Change of Topologies]. Let $\mathcal{C},\mathcal{C}'$ be sites and $i:\mathcal{C}'$ be a fully subcategory of $\mathcal{C}$, $i:\mathcal{C}'\to\mathcal{C}$ is continuous and cocontinuous satisfying the hypothesis of(6.1.2.23), then for $\mathcal{F}\in\mathcal{S}\mathrm{h}(\mathcal{C}'),\mathcal{G}\in\mathcal{S}\mathrm{h}(\mathcal{C})$, there are functorial isomorphisms

$$H^p(\mathcal{C}',U,i^{-1}\mathcal{G})\cong H^p(\mathcal{C},U,\mathcal{G}).$$

And if i satisfies the hypothesis of(6.1.2.25), then moreover there are functorial isomorphisms

$$H^p(\mathcal{C}',U,F')\cong H^p(\mathcal{C};U,i_*F')=H^p(\mathcal{C};i(U),i_!F')$$

⌟

Proof: For the first assertion, notice g^{-1} preserves injectives because it is right adjoint to $g_! = f^{-1}$ is exact(6.1.2.23).

The second assertion follows immediate from(6.1.2.25). □

Calculations

Prop. (6.3.1.5) [Locality of Cohomologies]. Let $(\mathcal{C},\mathcal{O})$ be a ring site and $U\in\mathcal{C}$, then for $\mathcal{F}\in \mathcal{M}\mathrm{od}(\mathcal{O}_X)$, $H^n(U,\mathcal{F})=H^n(\mathcal{C}/U,\mathcal{F}|_U)$, by(6.3.4.2) and the composition of derived functors applied to the pullback $j^*:\mathcal{C}/U\to\mathcal{C}$. ⌟

Prop. (6.3.1.6) [Sheaf-Cohomological Presheaves]. The forgetful functor is right adjoint to the exact shifification functor, the composition of derived functors applied to the functor $\Gamma(U,-)\circ\iota$ from $\mathcal{PS}\mathrm{h}(\mathcal{C})$ to $\mathcal{A}\mathrm{b}$ shows its right derived functor is

$$\mathcal{H}^p(F)=R^p\iota(F):U\to H^p(U,F).$$

⌟

Prop. (6.3.1.7) [Higher Direct Image]. For $f:(\mathcal{C}',\mathcal{O}')\to(\mathcal{C},\mathcal{O})$ a morphism of ringed topoi and $\mathcal{F}\in\mathcal{S}\mathrm{h}(\mathcal{C})$, the composition of derived functors applied to the functor $(\sharp\circ(f_*)^{\mathcal{PS}\mathrm{h}})\circ\iota$(because $\sharp,(f_*)^{\mathcal{PS}\mathrm{h}}$ are exact(6.1.2.10)) shows that $R^pf_*\mathcal{F}=(f_*\mathcal{H}^p(\mathcal{F}))^\sharp$. So flask sheave thus flabby sheave are right acyclic for f_*.

In particular, $R^pf_*\mathcal{F}$ can be calculated locally on the base. ⌟

Prop. (6.3.1.8) [Relative Leray Spectral Sequence]. Let

$$(f,f^\sharp):(\mathcal{S}\mathrm{h}(\mathcal{C}),\mathcal{O})\to(\mathcal{S}\mathrm{h}(\mathcal{C}'),\mathcal{O}'),\quad (g,g^\sharp):(\mathcal{S}\mathrm{h}(\mathcal{C}'),\mathcal{O}')\to(\mathcal{S}\mathrm{h}(\mathcal{D}),\mathcal{O}_{\mathcal{D}})$$

be morphisms of ringed topoi, then the natural transformation $R(g\circ f)\to Rg_*\circ Rf_*$ is an isomorphisms, and for any $\mathcal{F}^\bullet\in K^+(\mathcal{O})$, there is a spectral sequence convergence

$$E_2^{p,q}=R^pg_*R^qf_*(\mathcal{F}^\bullet)\Longrightarrow E^n=R^n(g\circ f)_*\mathcal{F}^\bullet.$$

⌟

Proof: This is just the Grothendieck spectral sequence(4.10.7.11), where the condition is satisfied by(6.3.1.7) and(6.3.4.12). □

Cor. (6.3.1.9) [Leray Spectral Sequence]. Let $(f,f^\sharp):(\mathcal{S}\mathrm{h}(\mathcal{C}),\mathcal{O})\to(\mathcal{S}\mathrm{h}(\mathcal{C}'),\mathcal{O}')$ be a morphism of ringed topoi, then for any $\mathcal{F}^\bullet\in K^+(\mathcal{O})$, then $R\Gamma(\mathcal{C},-)\to R\Gamma(\mathcal{C}',-)\circ Rf_*$ is an isomorphism, and there is a spectral sequence convergence

$$E_2^{p,q}=H^p(\mathcal{C}',R^qf_*(\mathcal{F}^\bullet))\Rightarrow E^n=H^n(\mathcal{C},\mathcal{F}^\bullet).$$

⌟

Prop. (6.3.1.10) [Relative Mayer-Vietoris Sequence]. Let $(\mathcal{C},\mathcal{O})$ be a ringed site and $\mathcal{U}:\{U\to X,V\to X\}$ is a covering s.t. $U\to X$ is a monomorphism, then for any $\mathcal{F}\in\mathcal{S}\mathrm{h}(\mathcal{O})$ and any morphism of ringed sites $f:(\mathcal{C},\mathcal{O})\to(\mathcal{C}',\mathcal{O}')$, there is a long exact sequence of sheaves in $\mathcal{S}\mathrm{h}(\mathcal{O}')$:

$$0\to(f|_X)_*(\mathcal{F}|_X)\to(f|_U)_*(\mathcal{F}|_U)\oplus(f|_V)_*(\mathcal{F}|_V)\to(f|_{U\cap V})_*(\mathcal{F}|_{U\cap V})\to R^1(f|_X)_*(\mathcal{F}|_X)\to\dots$$

that is functorial in $\mathcal{F}$. ⌟

Proof: Choose a functorial injection resolution $\mathcal{F} \to \mathcal{I}^\bullet$(4.10.2.9), then there is an exact sequence of complexes

$$0 \to (f|_X)_*(\mathcal{I}^\bullet|_X) \to (f|_U)_*(\mathcal{I}^\bullet|_U) \oplus (f|_V)_*(\mathcal{I}^\bullet|_V) \to (f|_{U\cap V})_*(\mathcal{I}^\bullet|_{U\cap V}) \to 0$$

because injective sheaves are flabby(6.3.4.9) and $(U \times_X V) \times_X f^{-1}W \to V \times_X f^{-1}W$ is a monomorphism for any $W \in \mathcal{C}'$. Then we take the long exact sequence of cohomology. □

Cor. (6.3.1.11) [Mayer-Vietoris Sequence]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{U} : \{U \to X, V \to X\}$ is a covering s.t. $U \to X$ is a monomorphism, then for any $\mathcal{F} \in \mathcal{S}\mathrm{h}(\mathcal{O})$, there is a long exact sequence

$$0 \to H^0(X, \mathcal{F}) \to H^0(U, \mathcal{F}) \oplus H^0(V, \mathcal{F}) \to H^0(U \times_X V, \mathcal{F}) \to H^1(X, \mathcal{F}) \to \dots$$

that is functorial in $\mathcal{F}$. ⌟

Prop. (6.3.1.12) [Compatibility with Algebraic Structures]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{F} \in \mathcal{S}\mathrm{h}(\mathcal{C})$, $K \in \mathcal{PS}\mathrm{h}(\mathcal{C})$, then $H^*(K, \mathcal{F})$ is the same calculated as $\mathcal{O}$-modules or Abelian sheaves. ⌟

Proof: Denote $(C, \underline{\mathbb{Z}})$ the trivial ringed site and $ab : (C, \mathcal{O}) \to (C, \underline{\mathbb{Z}})$ the forgetful functor, then ab is exact and $\mathrm{Hom}(K, \mathcal{F}_{ab}) = \mathrm{Hom}(K, \mathcal{F})$, thus we can use the Leray spectral sequence(6.3.1.9). □

Prop. (6.3.1.13)[Direct Products]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{F}_i$ be a family of sites indexed over a set I, then for any presheaf of sets K on $\mathcal{C}$, there is a Leray spectral sequence convergence(6.3.1.8)

$$H^p(K, R^q(\prod_i)\mathcal{F}_i) \to R^n(\prod_i \mathrm{Hom}(K, \cdot))(\mathcal{F}_i) \cong \prod_i H^n(K, \mathcal{F}_i).$$

In particular, $H^1(K, \prod_i \mathcal{F}_i) \to \prod_i H^1(K, \mathcal{F}_i)$ is injective. ⌟

Prop. (6.3.1.14) [Filtered Colimits]. $H^n(U, -)$ commutes with filtered colimits if T is a Noetherian topology. ⌟

Proof: $n = 0$ case follows from the fact the colimit presheaf is already a sheaf, because for any finite cover, the Čech complex of the limit sheaf is the filtered colimit of Čech complexes, and filtered colimit is exact.

And a filtered colimits of injective sheaves is flask, because flask need only be checked for finite coverings at this case(because of the fact T and T^f have equivalent category of sheaves(6.1.1.3) and definition of flask(6.3.4.8)), and a filtered colimit of exact Čech complexes is exact. So we can choose a functorial injective resolution(4.10.2.9) and use the colimit resolution to calculate the cohomology. □

Lemma (6.3.1.15). If X is a qs ringed space, then $\mathcal{S}\mathrm{h}(X) \to \mathcal{S}\mathrm{h}(X_{fp})$ is an equivalence by i_s and i^s, where fp is the subtopology of X generated by qcqs open subsets. ⌟

Proof: The proof is the same proof as that of(6.1.4.20). □

Prop. (6.3.1.16) [Filtered Colimits]. $H^i(U, -)$ commutes with direct limits if X is a qs ringed space and $U \subset X$ is qc. ⌟

Proof: This follows from(6.3.1.15) the same way(8.4.1.8) follows from(6.1.4.20). □

Low Dimensions

Cf.[Sta]Chap21.5-7.

Prop. (6.3.1.17) [H^1 **and Picard Group].** Let $(\mathcal{C},\mathcal{O})$ be a local ringed site, then there is a canonical isomorphism of Abelian groups
$$H^1(\mathcal{C},\mathcal{O}^*)=\mathrm{Pic}(\mathcal{O}).$$
⌟

Proof: Let $\mathcal{L}$ be an invertible sheaf, them there exists a subsheaf
$$\mathcal{L}^*:U\mapsto\{s\in\mathcal{L}(U)|s\cdot:\mathcal{O}(U)\to\mathcal{L}(U)\text{ is an isomorphism}\}.$$

Notice if $f\in\mathcal{O}^*(U)$ and $s\in\mathcal{L}^*(U)$, then $fs\in\mathcal{L}^*(U)$, and any two $s,s'\in\mathcal{L}^*(U)$ differ by an element of $\mathcal{O}^*(U)$, so $\mathcal{L}^*$ is a pseudo-$\mathcal{O}^*$-torsor. Moreover, as $\mathcal{L}$ is locally free of rank 1 by(6.2.5.8), so $\mathcal{L}^*(U)$ has sections locally, so it is an $\mathcal{O}^*$-torsor.

In this way, we get a map
$$\mathrm{Pic}(\mathcal{O})\to\mathrm{Tor}(\mathcal{O}_X^*)\cong H^1(X,\mathcal{O}_X^*)(6.3.2.18).$$
This map is injective: if $\mathcal{L}$ corresponds to a trivial torsor, then $\mathcal{L}^*$ has a global section, and then $\mathcal{L}$ is also trivial. This map is also surjective, because if $\mathcal{F}$ is an $\mathcal{O}_X^*$-torsor, then we can define
$$\mathcal{L}_1:U\mapsto[\mathcal{F}(U)\otimes\mathcal{O}(U)]/\mathcal{O}(U)^*,$$
where the action is given by $f\cdot(s,g)=(fs,f^{-1}g)$, and $\mathcal{L}_1$ is an $\mathcal{O}$-module given the addition $(s,g)+(s',g')=(s,g+\frac{s'}{s}g)$, where $\frac{s'}{s}\in\mathcal{O}(U)$ satisfies $\frac{s'}{s}\cdot s=s'$. Then the shifification $\mathcal{L}$ of $\mathcal{L}$ is a locally trivial bundle that maps $\mathcal{F}$. □

Prop. (6.3.1.18) [H^2 **and Objects of Gerbes].** Let $\mathcal{C}$ be a site and $\mathcal{S}\to\mathcal{C}$ be a gerbe whose automorphism sheaves are Abelian. Let $\mathcal{G}$ be the sheaf defined in(6.1.3.24). If U is an object of $\mathcal{C}$ that

- there exists a cofinal system of coverings $\{U_i\to U\}$ that for any such covering, $H^1(U_i,\mathcal{G})=0,H^1(U_i\times_U U_j,\mathcal{G})=0$,
- $H^2(U,\mathcal{G})=0$.

Then $\mathcal{S}_U$ is non-empty. ⌟

Proof: By hypothesis, there is a covering $\{U_i\to U\}$ and x_i in $\mathcal{S}$ lying over U_i. By item1, after refining the covering, we may assume $H^1(U_i,\mathcal{G})=0$ and $H^1(U_{ij},\mathcal{G})=0$. Consider the sheaf
$$\mathcal{F}_{ij}=\mathrm{Isom}(x_i|_{U_{ij}},x_j|_{U_{ij}})$$
on $\mathcal{C}_{/U_{ij}}$, then there is an action $\mathcal{G}_{U_{ij}}\times\mathcal{F}_{ij}\to\mathcal{F}_{ij}$. Then $\mathcal{F}_{ij}$ is a pseudo $\mathcal{G}|_{U_{ij}}$-torsor and clearly a torsor because any two objects of a gerbe is locally isomorphic.

By(6.3.2.18), these torsors are trivial, thus having a global section. In other words, there are isomorphisms $\varphi_{ij}:x_i|_{U_{ij}}\to x_j|_{U_{ij}}$. To get an object x over U, it suffices to manage the choices of φ_{ij} to get a descent datum. For this, use the fact $H^2(U,\mathcal{G})=0$ and $\check{H}^2(\mathcal{U},\mathcal{G})\to H^2(U,\mathcal{G})$ is injective by Cech to Derived spectral sequence(6.3.2.13). □

Others

Prop. (6.3.1.19). Let $K' \to K$ be a map of presheaves of sets on $\mathcal{C}$ whose shifification is surjective. Set $K'_p = K' \times_K \times \ldots \times_K K'$, then for any $\mathcal{F} \in \mathcal{S}\mathrm{h}(\mathcal{C})$, there is a spectral sequence convergence

$$E_1^{p,q} = H^q(K'_p, \mathcal{F}) \Rightarrow H^{p+q}(K, \mathcal{F}).$$

⌟

Proof: Since shifification is exact, $(K'_p)^\sharp = (K')^\sharp_p$. Then we use(6.1.2.26) to change to a larger site $\mathcal{C}'$ where the topoi are equivalent and K', K are objects in $\mathcal{C}'$ and $K' \to K$ is a covering, then we use the E_1 page of the Čech to derived spectral sequence(6.3.2.13). Notice this need modification, the modification goes back to the proof of the Grothendieck spectral sequence, where we choose the natural Čech complex resolution in place of the CE resolution, because we have(6.3.2.3). □

Cor. (6.3.1.20)[Čech-Alexander Resolution]. If $\mathcal{C}$ is a site with the indiscrete topology, X a weakly final object(4.1.1.8) of $\mathcal{C}$, then for any Abelian sheaf $\mathcal{F}$ on $\mathcal{C}$, the total cohomology $R\Gamma(\mathcal{C}, \mathcal{F})$ is represented by the Čech complex

$$\mathcal{F}(X) \to \mathcal{F}(X \times X) \to \mathcal{F}(X \times X \times X) \to \ldots.$$

⌟

Proof: By(6.3.4.10), $H^q(X^p, \mathcal{F}) = 0$ for $q > 0$. The assumption says $h_X \to *$ is surjective, thus the conclusion is a special case of(6.3.1.19). □

2 Čech Cohomology

Def. (6.3.2.1)[Čech Complex and Čech Cohomology]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{U} : \{U_i \to U\}$ be a covering, we have a canonical complex of presheaves $\mathbb{Z}_{\mathcal{U},\bullet}$ defined to be

$$\cdots \to \bigoplus_{i_0,i_1,i_2} j_!\mathbb{Z}_{U_{i_0 i_1 i_2}} \to \bigoplus_{i_0,i_1} j_!\mathbb{Z}_{U_{i_0 i_1}} \to \bigoplus_{i_0} j_!\mathbb{Z}_{U_{i_0}} \to 0.$$

And for any presheaf of $\mathcal{O}_X$-module $\mathcal{F}$, the complex

$$\mathrm{Hom}^\bullet_{Psh(\mathcal{O})}(\mathbb{Z}_{\mathcal{U},\bullet} \otimes \mathcal{O}, \mathcal{F}) \cong \mathrm{Hom}^\bullet_{P\mathcal{A}\mathrm{b}}(\mathbb{Z}_{\mathcal{U},\bullet}, \mathcal{F})$$

is called the **Čech complex** $\check{\mathcal{C}}^\bullet(\mathcal{U}, \mathcal{F})$ of $\mathcal{F}$. The cohomology $\check{H}^*(\mathcal{U}, \mathcal{F})$ of $\check{\mathcal{C}}^\bullet(\mathcal{U}, \mathcal{F})$ is called the **Čech cohomology** of $\mathcal{F}$ w.r.t $\mathcal{U}$.

$\mathbb{Z}_{\mathcal{U},\bullet}$ is exact except in degree 0, where the homology is $j_!\mathbb{Z}_U$. This is because we have a homotopy: choose a fixed i_0, for a $s \in \Gamma(U_{i_1 \ldots i_n}, \mathcal{F})$, we map it to $(hs)_{i i_1 \ldots i_n} = \delta_{i,i_0} s$**?**. In particular, an injective sheaf is Čech acyclic. ⌟

Lemma (6.3.2.2). The Čech complexes $\check{\mathcal{C}}^\bullet(\mathcal{U}, -)$ induces a functor from $\mathcal{PS}\mathrm{h}(\mathcal{C})$ to $K^+(\mathcal{A}\mathrm{b})$, which is an exact functor. ⌟

Proof: Because in each degree this functor is a sum of functors of the form $\mathcal{F} \mapsto \mathcal{F}(U)$, which are exact functors on $\mathcal{PS}\mathrm{h}(\mathcal{C})$. □

Prop. (6.3.2.3) [Čech Complex as Derived Functors]. Let $\mathcal{C}$ be a site and $\mathcal{U}:\{U_i\to U\}$ be a covering, then $\check{H}^0(\mathcal{U},-)$ is left exact, and for $\mathcal{F}\in\mathcal{Sh}(\mathcal{C})$, there are functorial quasi-isomorphisms

$$\check{\mathcal{C}}^\bullet(\mathcal{U},\mathcal{F})\to R\check{H}^0(\mathcal{U},\mathcal{F})$$

which is functorial in $\mathcal{F}$. ⌟

Proof: Choose a functorial injective resolution of presheaves $\mathcal{I}^\bullet$ of $\mathcal{F}$, and consider the double complex $\check{\mathcal{C}}(\mathcal{U},\mathcal{I}^\bullet)$. There are maps of complexes

$$\check{\mathcal{C}}(\mathcal{U},\mathcal{F})\to\mathrm{Tot}(\check{\mathcal{C}}(\mathcal{U},\mathcal{I}^\bullet)),\quad \check{H}^0(\mathcal{U},\mathcal{I}^\bullet)\to\mathrm{Tot}(\check{\mathcal{C}}(\mathcal{U},\mathcal{I}^\bullet))$$

which are both quasi-isomorphism by an application of spectral sequence and the fact the columns and rows are exact in positive degrees: The columns are exact because of(6.3.2.2) and the rows are exact because $\mathbb{Z}_{\mathcal{U},\bullet}$ is exact in positive degrees(6.3.2.1) and $\mathcal{I}^p$ are injective. Then we have the desired quasi-isomorphism, and it is functorial in $\mathcal{F}$. □

Cor. (6.3.2.4) [Čech Cohomologies]. If we take filtered colimit for coverings, $\mathcal{F}\to\check{H}^0(U,\mathcal{F})=H^0(U,\mathcal{F})$ is a left exact functor from presheaves to sets, the derived complex is just $\varinjlim_{\mathcal{U}}\check{\mathcal{C}}^\bullet(\mathcal{U},\mathcal{F})$, and the derived functors are just $\varinjlim_{\mathcal{U}}\check{H}^q(\mathcal{U},\mathcal{F})$. ⌟

Proof: This is because we can take colimit of the conclusion of(6.3.2.3), because the colimit is filtered by(6.3.2.5) so exact, so the Čech complex also represents the derived complex. □

Lemma (6.3.2.5). The refinement morphism of Čech cohomologies of two coverings doesn't depends on the refinement map chosen. ⌟

Proof: For two refinement map, there is a commutative diagram

$$\begin{array}{ccc}\prod F(U_i) & \xrightarrow{d^0} & \prod F(U_i\times_U U_j)\\ \downarrow{\scriptstyle f-g} & \swarrow{\scriptstyle \Delta^1} & \\ \prod F(U_j') & & \end{array}$$

so it induce the same map on the kernel. □

Def. (6.3.2.6) [Alternating Čech Complexes]. Let $(\mathcal{C},\mathcal{O})$ be a ringed site and $\mathcal{U}:\{U_i\to U\}\in\mathrm{Cov}(\mathcal{C})$, $\mathcal{F}\in\mathcal{Sh}(\mathcal{O})$, then the **alternating Čech complex** of $\mathcal{F}$ is defined to be the subcomplex

$$\check{C}^\bullet_{\mathrm{alt}}(\mathcal{U},\mathcal{F})=\{s\in\check{C}^\bullet(\mathcal{U},\mathcal{F})|s_{i_0,\ldots,i_p}=0\text{ if }i_m=i_n,m\neq n,s_{i_{\sigma(0)},\ldots,i_{\sigma(p)}}=\mathrm{sgn}(\sigma)s_{i_0,\ldots,i_p}\}\subset\check{C}^\bullet(\mathcal{U},\mathcal{F}).$$

It is truly a subcomplex. ⌟

Prop. (6.3.2.7) [Alternating and Usual Complexes]. Let $(\mathcal{X},\mathcal{O}_X)$ be a <u>ringed space</u>, $\mathcal{U}:\{U_i\to U\}\in\mathrm{Cov}(\mathcal{C})$, $\mathcal{F}\in\mathcal{Sh}(\mathcal{O}_X)$, then the inclusion

$$\check{C}^\bullet_{\mathrm{alt}}(\mathcal{U},\mathcal{F})\to\check{C}^\bullet(\mathcal{U},\mathcal{F})$$

is a homotopy equivalence. ⌟

Proof: Cf.[Sta]01FM. The proof is rather complicated.? □

Remark (6.3.2.8). WARNING: This is not right for ringed sites, e.g. the étale sites, for example, cf.(8.4.1.23). ⌟

Comparison Theorems

Prop. (6.3.2.9). If two coverings are refinements of each other, then their Čech cohomology is isomorphic. ⌟

Proof: Because the refinement morphism doesn't depends on the refinement map(6.3.2.5). □

Prop. (6.3.2.10)[Comparison Theorem for Čech Acyclicity]. If there are two coverings $\mathfrak{U},\mathfrak{V}$ and a presheaf $\mathcal{F}$, then we can construct a double Čech complex with the (p,q)-term being $\mathcal{F}(U_{i_1,\ldots i_p}\cap V_{j_1,\ldots j_q})$. Then the vertical and horizontal arrays calculate the Čech cohomology $\prod_j H^*(\mathfrak{U}|_{V_{j_1\ldots,j_q}},\mathcal{F})$, $\prod_i H^*(\mathfrak{V}|_{U_{i_1\ldots,i_q}},\mathcal{F})$ respectively.

So by Spectral sequence(4.10.7.8), if both higher Čech cohomology group $H^k(\mathfrak{U}|_{V_{j_1\ldots,j_q}},\mathcal{F})$, $H^k(\mathfrak{V}|_{U_{i_1\ldots,i_q}},\mathcal{F})$ vanish, i.e., they are both $\mathcal{F}$-acyclic, then $H^*(\mathfrak{U},\mathcal{F})\cong H^*(\mathfrak{V},\mathcal{F})$. ⌟

Cor. (6.3.2.11). If $\mathfrak{V}$ is a refinement of $\mathfrak{U}$, and $\mathfrak{V}|_{U_{i_1,\ldots,i_p}}$ are all $\mathcal{F}$ acyclic, then $H^*(\mathfrak{U},\mathcal{F})\cong H^*(\mathfrak{V},\mathcal{F})$. ⌟

Proof: It suffices to prove $\mathfrak{U}|_{V_{i_1,\ldots,i_q}}$ is $\mathcal{F}$-acyclic. But $\mathfrak{U}|_{V_{i_1,\ldots,i_q}}$ and $\mathrm{id}_{V_{i_1,\ldots,i_q}}$ are refinements of each other, so(6.3.2.9) settles the proof. □

Cor. (6.3.2.12). If $\mathfrak{V}|_{U_{i_1,\ldots,i_p}}$ is $\mathcal{F}$-acyclic, then the covering $H^*(\mathfrak{U}\times\mathfrak{V},\mathcal{F}) = H^*(\{U_i\cap V_j\},\mathcal{F})\cong H^*(\mathfrak{U},\mathcal{F})$. ⌟

Proof: Because $\mathfrak{V}|_{U_{i_1,\ldots,i_p}}$ and $\mathfrak{U}\times\mathfrak{V}|_{U_{i_1,\ldots,i_p}}$ are refinement of each other, so $\mathfrak{U}\times\mathfrak{V}|_{U_{i_1,\ldots,i_p}}$ are $\mathcal{F}$-acyclic by(6.3.2.9), and $\mathfrak{U}\times\mathfrak{V}$ refines $\mathfrak{U}$, so(6.3.2.11) can be applied. □

Prop. (6.3.2.13)[Čech to Derived]. For any $\mathcal{F}\in\mathcal{S}\mathrm{h}(\mathcal{C})$, the Grothendieck spectral sequence applied to $\Gamma(U,-)=H^0(\{U_i\to U\},-)\circ\iota=\check{H}^0(U,-)\circ\iota$ gives us:

$$H^p(\{U_i\to U\},\mathcal{H}^q(\mathcal{F}))\Longrightarrow H^{p+q}(U,\mathcal{F}).$$

$$\check{H}^p(U,\mathcal{H}^q(F))\Longrightarrow H^{p+q}(U,\mathcal{F}).$$

⌟

Cor. (6.3.2.14)[$\check{H}^0$ of Sheaf-Cohomology Presheaves]. For any $\mathcal{F}\in\mathcal{S}\mathrm{h}(\mathcal{C})$, $\mathcal{H}^p(\mathcal{F})^{++}=\mathcal{H}^p(F)^\sharp=0$ for $p>0$, so

$$\mathcal{H}^p(\mathcal{F})^+(U)=\check{H}^0(U,\mathcal{H}^p(F))=0\quad p>0.$$

because $\mathcal{H}^p(\mathcal{F})^+$ is separated by(6.1.2.7). In particular, for any $s\in H^p(U,\mathcal{F}),p>0$, there exists a covering $\mathcal{U}$ of U s.t. $s|_{U_i}=0$ for any i.

Thus the low degree of Čech to sheaf says(4.10.7.12):

$$0\to\underline{\check{H}^1(U,\mathcal{F})\to H^1(U,\mathcal{F})}\to 0\to\check{H}^2(U,\mathcal{F})\to H^2(U,\mathcal{F})\to\check{H}^1(U,\mathcal{H}^1(\mathcal{F}))\to\check{H}^3(U,\mathcal{F})\to H^3(U,\mathcal{F}).$$

⌟

Proof: By Grothendieck spectral sequence applied to forgetful functor and exact $\sharp$ functor, where the condition are satisfied by(6.3.4.3). □

Cor. (6.3.2.15) [Acyclic Covering Calculates Derived Cohomologies]. If we have $H^q(U_{i_0i_1\ldots i_r},\mathcal{F})=0,q>0$, then $H^p(\{U_i\to U\},\mathcal{F})=H^p(U,\mathcal{F})$ as $\mathcal{O}_X(U)$-modules. ⌟

Proof: Because $H^p(\{U_i \to U\}, \mathcal{H}^q(F))$ vanish for $q > 0$. $\square$

Prop. (6.3.2.16) [Čech Acyclic Čech Comparison]. If $\mathcal{C}$ be a ringed site, $\mathfrak{G} \subset \mathcal{C}$, $\mathrm{Cov} \subset \mathrm{Cov}(\mathcal{C})$ and $\mathcal{F} \in \mathcal{S}\mathrm{h}(\mathcal{C})$ that

- For any $\{U_i \to U\} \in \mathrm{Cov}$, $U_i, U \in \mathfrak{G}$, and $U_{i_0,\ldots,i_p} \in \mathfrak{G}$.
- $\mathrm{Cov}|_U$ is cofinal in $\mathrm{Cov}(\mathcal{C}/U)$ for any $U \in \mathfrak{G}$.
- $\check{H}^q(U, \mathcal{F}) = 0$ for any $U \in \mathfrak{G}$ and $q > 0$.

Then $H^p(X, \mathcal{F}) = \check{H}^p(X, \mathcal{F}) = H^p(\{U_i \to X\}, \mathcal{F})$ for any $\{U_i \to X\} \in \mathrm{Cov}$. ⌟

Proof: By(6.3.2.15), we only have to show that $H^q(U, \mathcal{F}) = 0$ for $U \in \mathfrak{G}$ and $q > 0$. Use induction on q, use Čech to sheaf2: $\check{H}^p(U, \mathcal{H}^q(\mathcal{F})) \Rightarrow H^{p+q}(U, \mathcal{F})$. The case $q \neq 0$ is by condition2, 3, and induction hypothesis. For $p = 0$, use (6.3.2.14). $\square$

Non-Abelian Čech Cohomologies

Def. (6.3.2.17) [Non-Abelian Cohomology]. Let $\mathcal{C}$ be a site and $\mathcal{G} \in \mathcal{S}\mathrm{h}^{\mathcal{G}\mathrm{rp}}(\mathcal{C})$, for any covering $\mathcal{U} = \{U_i \to U\} \in \mathrm{Cov}(\mathcal{C})$, we can define a **non-Abelian Čech cohomology** $\check{H}^1(\mathcal{U}, \mathcal{G})$ as follows: Define $Z^1(\mathcal{U}, \mathcal{G})$=sets of families

$$\{(c_i) | c_i \in \Gamma(U_{ij}, \mathcal{G}) : c_{jk} c_{ik}^{-1} c_{ij} = 1\}.$$

If $\mathsf{c} \in Z^1(G, M)$, then for any $g \in \Gamma(U, \mathcal{G})$,

$$\mathsf{c}_g = (c'_{ij} = g|_{U_i}^{-1} c_{ij} g|_{U_j})$$

is also in $Z^1(\mathcal{U}, \mathcal{G})$. This defines an equivalence relation on $Z^1(\mathcal{U}, \mathcal{G})$, the equivalence classes are called $\check{H}^1(G, M)$. This is compatible with the commutative case.

Taking filtered colimit over all coverings of U, we can also define $\check{H}^1(U, \mathcal{G})$. ⌟

Prop. (6.3.2.18) [H^1 and Torsors]. Let $\mathcal{C}$ be a site and $\mathcal{H} \in \mathcal{S}\mathrm{h}(\mathcal{C})$, then there is a canonical isomorphism of $\mathcal{H}$-torsors(6.1.1.14) and $H^1(\mathcal{C}, \mathcal{H})$. ⌟

Proof: Cf.[Sta]03AJ. Should have a non-commutative version. $\square$

Prop. (6.3.2.19) [Long Exact Sequence of Non-Abelian Čech Cohomologies]. Let $\mathcal{C}$ be a site and $1 \to \mathcal{A} \to \mathcal{B} \to \mathcal{C} \to 1$ is an exact sequence in $\mathcal{S}\mathrm{h}^{\mathcal{G}\mathrm{rp}}(\mathcal{C})$, then for any $U \in \mathcal{C}$, there is a long exact sequence of pointed sets

$$1 \to \Gamma(U, \mathcal{A}) \to \Gamma(U, \mathcal{B}) \to \Gamma(U, \mathcal{C}) \xrightarrow{\delta} \check{H}^1(U, \mathcal{A}) \to \check{H}^1(U, \mathcal{B}) \to \check{H}^1(U, \mathcal{C}) \xrightarrow{\Delta} \check{H}^2(U, \mathcal{A})$$

the last term is defined only when $\mathcal{A}$ is in the center of $\mathcal{B}$ and U satisfies: For any covering $\mathcal{U}$ and a refinement $\mathcal{W} \to \mathcal{U} \times \mathcal{U}$, there exists a refinement $\mathcal{U}' \to \mathcal{U}$ s.t. $\mathcal{U}' \times \mathcal{U}'$ is a refinement of $\mathcal{W}$.

δ is defined as follows: for $c \in \Gamma(\mathcal{C}, \mathcal{C})$, by taking a covering $\{U_i \to U\}$, we may assume that $c|_{U_i} = b_i \in \Gamma(U_i, \mathcal{B})$, then $a_{ij} = b_i^{-1} b_j$ is a cocycle, and a different choice differ by a cocyle, so this is well-defined.

Δ is defines as: for any covering $\mathcal{U}$ of U and $\mathsf{c} = (c_{ij})$ a cocycle in $\check{H}^1(\mathcal{U}, \mathcal{C})$, by passing to a refinement, we may assume that $c_{ij} \in \Gamma(U_{ij}, \mathcal{B})$, then $\delta(\mathsf{c})$ is represented by the 2-cocycle $a_{ijk} = c_{jk} c_{ik}^{-1} c_{ij} \in \Gamma(U, \mathcal{A})$. ⌟

Proof: ??The verification of well-definedness of Δ is checked at [Serre Local Fields P124].?

For the exactness at C^G, the definition of δ shows that $\delta(c) = 1$ iff there is an inverse image b that $b^{-1}\sigma(b) = 1$ for all σ.

For the exactness at $H^1(G, A)$, $a_\sigma = b^{-1}\sigma(b)$ if a_σ is in the image of δ. Conversely, the image of b in C is in C^G, so it is in the image of δ.

For the exactness at $H^1(G, B)$, one way is clear, and for the other, if $\pi(b_\sigma) = c^{-1}\sigma(c)$, then if t is an inverse image of c, then $tb_\sigma\sigma(t)^{-1}$ is a cocycle in A cohomologous to b_σ.

For the exactness at $H^1(G, C)$, one way is clear, and if b_s is an inverse image of b_s and $a_{\sigma,\tau} = b_\sigma\sigma(b_\tau)b_{\sigma\tau}^{-1}$ is a coboundary, then it is $a_\sigma\sigma(a_\tau)a_{\sigma\tau}^{-1}$, so we change b to $a_\sigma^{-1}b_\sigma$, as A is in the center of B, this lifts c to a cocycle in B. □

Prop. (6.3.2.20)[Hilbert's Theorem 90]. For L/K a Galois extension, $H^1(\mathrm{Gal}(L/K), \mathrm{GL}_n(L)) = 1$, where L is equipped with the discrete topology. ⌟

Proof: We prove any cocycle is a coboundary, for this, notice any cocycle factor through a finite quotient, and the images of it is contained in a finite extension of K, hence it reduce to the case of L/K finite.

By definition, this is equivalent to any B-semi-linear representation of G free of finite rank is trivial, which is by(18.1.1.14). □

Cor. (6.3.2.21) [semi-linear representations]. The proposition implies that any semi-linear L-representation of $G_{L/K}$ is trivial. ⌟

Cor. (6.3.2.22). $H^1(G(L/K), SL_n(L)) = 1$. This is seen from the exact sequence $1 \to \mathrm{SL}(n, L) \to \mathrm{GL}(n, L) \to L^\times \to 1$. ⌟

3 Derived Homology

K-Flat Complexes

Def. (6.3.3.1)[K-flat Complexes]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site, a complex $\mathcal{K}^\bullet$ of $\mathcal{O}$-modules is called ***K*-flat** if for any acyclic complex $\mathcal{F}^\bullet$ of $\mathcal{O}$-modules, the total complex $\mathrm{Tot}^\oplus(\mathcal{F}^\bullet \otimes_\mathcal{O} \mathcal{K}^\bullet)$ is acyclic, or equivalently, tensoring with $\mathcal{K}^\bullet$ maps quasi-iso to quasi-iso, by the long exact sequence and the fact tensoring is an exact functor of triangulated categories(4.8.9.4). ⌟

Prop. (6.3.3.2). If K, K' are K-flat complexes of $\mathcal{O}$-modules,

- $\mathrm{Tot}^\oplus(K \otimes_\mathcal{O} K')$ is K-flat.
- If (K_1, K_2, K_3) is a distinguished triangle in $K(\mathcal{O})$, if two of them is K-flat, then the third is also K-flat.
- Any bounded above complex of flat $\mathcal{O}$-modules is K-flat.
- Any filtered colimits of K-flat complexes are K-flat.

⌟

Proof: 1: This follows from(4.8.9.2).

3: use(4.8.9.4), and the long exact sequence.

4: Cf.[Sta]06YQ.

5: because we are taking termwise-colimit, and Tot and tensor all commute with filtered colimits.

□

Prop. (6.3.3.3) [K-Flat Resolutions]. Any complex $P^\bullet$ of $\mathcal{O}$-modules has a K-flat resolution $K^\bullet \to P^\bullet$, moreover, each term of $K^\bullet$ is a flat $\mathcal{O}$-module and $K^\bullet \to P^\bullet$ is termwise surjective. ⌟

Proof: Cf.[Sta]06Y4. □

Lemma (6.3.3.4). Let $P \to Q$ be a quasi-iso of K-flat complexes of $\mathcal{O}$-modules, then for any complex L of $\mathcal{O}$-modules, $\mathrm{Tot}(L \otimes P) \to \mathrm{Tot}(L \otimes Q)$ is a quasi-isomorphism. ⌟

Proof: Choose a K-flat resolution(6.3.3.3) K of L, then notice

$$\mathrm{Tot}(L \otimes P) \cong \mathrm{Tot}(K \otimes P) \cong \mathrm{Tot}(K \otimes Q) \cong \mathrm{Tot}(L \otimes Q)$$

by definition of K-flatness(6.3.3.1). □

Prop. (6.3.3.5) [Pullback of K-Flat is K-Flat]. Let $f : (\mathcal{S}\mathrm{h}(\mathcal{C}'), \mathcal{O}_{\mathcal{C}'}) \to (\mathcal{S}\mathrm{h}(\mathcal{C}), \mathcal{O}_{\mathcal{C}})$ be a morphism of ringed topoi, then f^* maps K-flat complexes to K-flat complexes. ⌟

Proof: Cf.[Sta]0G7E. □

Derived Tensor Product and Tor

Def. (6.3.3.6) [Derived Tensor Product]. Let $\mathcal{A} \to \mathcal{B}$ be a homomorphism of sheaves of rings over a site $\mathcal{C}$, then the functor $\mathrm{Tot}^{\oplus}(- \otimes_{\mathcal{O}} -)$ is a bi-exact bifunctor of triangulated categories $K(\mathcal{A}) \times K(\mathcal{B}) \to D(\mathcal{B})$ by(4.8.9.4)(4.8.4.8), and the class of K-flat complexes in $K(\mathcal{A})$ and K-flat complexes in $K(\mathcal{B})$ satisfies the condition of (the dual of)**??** by(6.3.3.1) and(6.3.3.3), so we get a left derived functor

$$- \otimes^L_{\mathcal{A}} - : D(\mathcal{A}) \times D(\mathcal{B}) \to D(\mathcal{B}),$$

called the **derived tensor product**. And if any of $M^\bullet, N^\bullet \in K(\mathcal{A})$ is K-flat, the natural map $M^\bullet \otimes^L_{\mathcal{A}} N^\bullet \to \mathrm{Tot}^{\oplus}(M^\bullet \otimes_{\mathcal{A}} N^\bullet)$ is an isomorphism in $D(\mathcal{B})$ ⌟

Prop. (6.3.3.7). Let $\mathcal{A} \to \mathcal{B}$ be a homomorphism of sheaves of rings over a site $\mathcal{C}$. Let $N^\bullet$ be a $\mathcal{B}$-module, then for $M^\bullet \in D(\mathcal{A})$, there are a functorial isomorphisms

$$M^\bullet \otimes^L_{\mathcal{A}} N^\bullet \cong (M^\bullet \otimes^L_{\mathcal{A}} \mathcal{B}) \otimes^L_{\mathcal{B}} N^\bullet$$

⌟

Proof: Consider both sides as right derived functors of the multi-exact multifunctor. As this is true for $\mathrm{Tot}^{\oplus}$, these follow from the universal property and(4.10.3.14), the conditions are satisfied by(6.3.3.3)(6.3.3.4)(6.3.3.5). □

Cor. (6.3.3.8) [Commutative Monoidal Structure]. If $\mathcal{A} = \mathcal{B} = \mathcal{C} = \mathcal{O}$ and $K, L, M \in K(\mathcal{O})$, there are natural isomorphisms

$$K \otimes^L L \cong L \otimes^L K, \quad (K \otimes^L L) \otimes^L M \cong K \otimes^L (L \otimes^L M).$$

Thus $D^*(\mathcal{O})$ has a commutative monoidal structure. ⌟

Remark (6.3.3.9) [WARNING]. If M, N are two A-modules, then we can define $M_R \otimes^L_R N$ and $M \otimes^L_R N_R$, but there are no reason for them to be isomorphic. ⌟

Prop. (6.3.3.10). Let $\mathcal{A} \to \mathcal{B} \to \mathcal{C}$ be homomorphism of sheave of rings on a site $\mathcal{C}$, then for $M^\bullet \in K(\mathcal{A})$, $N^\bullet \in K(\mathcal{B})$ and $K^\bullet \in K(\mathcal{C})$, there are functorial isomorphisms

$$(M \otimes_A^L N) \otimes_B^L K = M \otimes_A^L (N \otimes_B^L K) = (M \otimes_A^L C) \otimes_C^L (N \otimes_B^L K)$$

and

$$(M \otimes_A^L N) \otimes_B^L K \cong (M \otimes_A^L K) \otimes_C^L (N \otimes_B^L C)$$

⌟

Proof: Consider both sides as right derived functors of the multi-exact multifunctor. As these are true for $\mathrm{Tot}^\oplus$, these follow from the universal property and(4.10.3.14), the conditions are satisfied by(6.3.3.3)(6.3.3.4)(6.3.3.5). □

Def. (6.3.3.11)[Tor Modules]. Let $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}$-modules, then the **Tor modules** $\mathrm{Tor}_p^{\mathcal{O}}(\mathcal{F}, \mathcal{G})$ is defined to be $H^{-p}(\mathcal{F} \otimes_{\mathcal{O}}^L \mathcal{G})$. ⌟

Prop. (6.3.3.12) [Flatness and Tor]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site, and $\mathcal{F}$ is an $\mathcal{O}$-module. Then $\mathcal{F}$ is a flat $\mathcal{O}$-modules iff $\mathrm{Tor}_1^{\mathcal{O}}(\mathcal{F}, \mathcal{G}) = 0$ for any $\mathcal{O}$-module $\mathcal{G}$. ⌟

Proof: If $\mathcal{F}$ is flat, then clearly $\mathrm{Tor}_1^{\mathcal{O}}(\mathcal{F}, \mathcal{G}) = 0$ for any $\mathcal{O}$-module $\mathcal{G}$. Conversely, use the long exact sequence associated to $\mathcal{F} \otimes_{\mathcal{O}}^L \cdot$(4.8.9.4). □

Def. (6.3.3.13)[Relative Cup Product]. Let $f : (\mathcal{Sh}(\mathcal{C}), \mathcal{O}_{\mathcal{C}}) \to (\mathcal{Sh}(\mathcal{D}), \mathcal{O}_{\mathcal{D}})$ be a morphism of ringed topoi, then for any $K, L \in D(\mathcal{O}_{\mathcal{C}})$, there is a canonical functorial **relative cup product**

$$Rf_*K \otimes_{\mathcal{O}_{\mathcal{D}}}^L Rf_*L \to Rf_*(K \otimes_{\mathcal{O}_{\mathcal{C}}}^L L)$$

in $D(\mathcal{O}_{\mathcal{D}})$ that is the adjunction map of the map

$$Lf^*(Rf_*K \otimes_{\mathcal{O}_{\mathcal{D}}}^L Rf_*L) \to Lf^*Rf_*K \otimes_{\mathcal{O}_{\mathcal{C}}}^L Lf^*Rf_*L \to K \otimes_{\mathcal{O}_{\mathcal{C}}}^L L$$

by(6.3.3.15). This map is symmetric and associative.

In particular, if $(\mathcal{Sh}(\mathcal{D}), \mathcal{O}_{\mathcal{D}}) = (\mathcal{Sh}(\mathrm{pt}), \Gamma(\mathcal{C}, \mathcal{O}_{\mathcal{C}}) = A)$(6.3.1.3), we get a map

$$R\Gamma(\mathcal{C}, K) \otimes_A^L R\Gamma(\mathcal{C}, L) \to \Gamma(\mathcal{C}, K \otimes_{\mathcal{O}_{\mathcal{C}}}^L L).$$

⌟

Derived Pullback

Def. (6.3.3.14) [Derived Pullback]. Let $f : (\mathcal{Sh}(\mathcal{C}'), \mathcal{O}') \to (\mathcal{Sh}(\mathcal{C}), \mathcal{O})$ be a morphism of ringed site, define the **derived pullback**

$$Lf^* : D(\mathcal{O}) \to D(\mathcal{O}') : \mathcal{F}^\bullet \mapsto f^{-1}\mathcal{F}^\bullet \otimes_{f^{-1}\mathcal{O}}^L \mathcal{O}'\text{(6.3.3.6)}.$$

In particular, if $\mathcal{F}^\bullet$ is K-flat, then there are natural isomorphisms $Lf^*\mathcal{F}^\bullet \cong f^*\mathcal{F}^\bullet$.

Moreover, Lf^* is also naturally isomorphic to the left derived functor of the pullback morphism f^*, by composition of derived functors applied to the $f^* = \mathrm{Tot}(\cdot \otimes_{f^{-1}\mathcal{O}} \mathcal{O}') \circ f^{-1}$ where f^{-1} is exact. In particular, Lf^* only depends on the underlying map f^* of ringed topoi. ⌟

Prop. (6.3.3.15). Let $f : (\mathcal{Sh}(\mathcal{C}), \mathcal{O}_{\mathcal{C}}) \to (\mathcal{Sh}(\mathcal{D}), \mathcal{O}_{\mathcal{D}})$, $g : (\mathcal{Sh}(\mathcal{D}), \mathcal{O}_{\mathcal{D}}) \to (\mathcal{Sh}(\mathcal{E}), \mathcal{O}_{\mathcal{E}})$ be a morphism of ringed topoi, then

- There is a natural isomorphism $L(g\circ f)^*\cong Lf^*\circ Lg^*$. In particular, as localizing map j^* is exact, Lf^* can be calculated locally on the base.
- For $\mathcal{F}^\bullet,\mathcal{G}^\bullet\in\mathcal{M}\mathrm{od}_{\mathcal{O}_\mathcal{D}}$, there are natural functorial isomorphisms
$$Lf^*(\mathcal{F}^\bullet\otimes^L_{\mathcal{O}_\mathcal{D}}\mathcal{G}^\bullet)\cong Lf^*\mathcal{F}^\bullet\otimes^L_{\mathcal{O}_\mathcal{C}}Lf^*\mathcal{G}^\bullet.$$
In particular, as localizing map j^* is exact, the derived tensor product can be calculated locally on the base.
- For $\mathcal{F}^\bullet\in\mathcal{M}\mathrm{od}_{\mathcal{O}_\mathcal{C}},\mathcal{G}^\bullet\in\mathcal{M}\mathrm{od}_{\mathcal{O}_\mathcal{D}}$, there are natural functorial isomorphisms
$$\mathcal{F}^\bullet\otimes^L_{\mathcal{O}_\mathcal{C}}Lf^*\mathcal{G}^\bullet\cong\mathcal{F}^\bullet\otimes^L_{f^{-1}\mathcal{O}_\mathcal{D}}f^{-1}\mathcal{G}'$$
- For $\mathcal{F}^\bullet,\mathcal{G}^\bullet\in\mathcal{M}\mathrm{od}_{\mathcal{O}_\mathcal{D}}$, the natural isomorphisms satisfy a commutative diagram
$$\begin{array}{ccc}
Lf^*(\mathcal{F}^\bullet\otimes^L_{\mathcal{O}_\mathcal{D}}\mathcal{G}^\bullet) & \longrightarrow & Lf^*\operatorname{Tot}^\oplus(\mathcal{F}^\bullet\otimes_{\mathcal{O}_\mathcal{D}}\mathcal{G}^\bullet)\\
\downarrow & & \downarrow\\
Lf^*\mathcal{F}^\bullet\otimes^L_{\mathcal{O}_\mathcal{C}}Lf^*\mathcal{G}^\bullet & & f^*\operatorname{Tot}^\oplus(\mathcal{F}^\bullet\otimes_{\mathcal{O}_\mathcal{D}}\mathcal{G}^\bullet)\\
\downarrow & & \downarrow\\
f^*\mathcal{F}^\bullet\otimes^L_{\mathcal{O}_\mathcal{C}}f^*\mathcal{G}^\bullet & \longrightarrow & \operatorname{Tot}^\oplus(f^*\mathcal{F}^\bullet\otimes_{\mathcal{O}_\mathcal{C}}f^*\mathcal{G}^\bullet)
\end{array}$$

⌟

Proof: 1, 2, 3: These follow from(6.3.3.10).

4: By a universal argument, $(\mathcal{F}^\bullet,\mathcal{G}^\bullet)\mapsto Lf^*(\mathcal{F}^\bullet\otimes^L_{\mathcal{O}_\mathcal{D}}\mathcal{G}^\bullet)$ is the derived functor of the bi-exact bifunctor
$$F:K(\mathcal{O}_\mathcal{D})\times K(\mathcal{O}_\mathcal{D})\to D(\mathcal{O}_\mathcal{C}):(\mathcal{F}^\bullet,\mathcal{G}^\bullet)\mapsto f^*\operatorname{Tot}^\oplus(\mathcal{F}^\bullet\otimes_{\mathcal{O}_\mathcal{D}}\mathcal{G}^\bullet).$$
Then by the universal property, both natural transformations corresponds to a natural transformation $\theta_i:LF\to LF$. So it suffices to show that they are isomorphic. But K-flat morphisms are essentially surjective in $D(\mathcal{O}_\mathcal{D})$, thus it suffices to prove the diagram is commutative for $\mathcal{F},\mathcal{G}$ K-flat. But in this case, there are commutative diagrams
$$\begin{array}{ccc}
LF(\mathcal{F}^\bullet,\mathcal{G}^\bullet) & \xrightarrow{\eta_{(\mathcal{F},\mathcal{G})}} & F(\mathcal{F}^\bullet,\mathcal{G}^\bullet)\\
\downarrow{\scriptstyle\theta_i\star(Q_{\mathcal{O}_\mathcal{D}}\times Q_{\mathcal{O}_\mathcal{D}})} & & \downarrow{\scriptstyle\mathrm{id}}\\
LF(\mathcal{F}^\bullet,\mathcal{G}^\bullet) & \xrightarrow{\eta_{(\mathcal{F},\mathcal{G})}} & F(\mathcal{F}^\bullet,\mathcal{G}^\bullet)
\end{array}$$
and $\eta_{(\mathcal{F},\mathcal{G})}$ is an isomorphism, so $\theta_1=\theta_2$. □

Prop. (6.3.3.16) [Adjunction]. Lf^* is left adjoint to Rf_*, by(4.10.3.15) and(6.2.2.9). ⌟

Prop. (6.3.3.17) [Base Change Map]. Let
$$\begin{array}{ccc}
(\mathcal{S}\mathrm{h}(\mathcal{C}'),\mathcal{O}_{\mathcal{C}'}) & \xrightarrow{g'} & (\mathcal{S}\mathrm{h}(\mathcal{C}),\mathcal{O}_\mathcal{C})\\
\downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f}\\
(\mathcal{S}\mathrm{h}(D'),\mathcal{O}_{D'}) & \xrightarrow{g} & (\mathcal{S}\mathrm{h}(\mathcal{D}),\mathcal{O}_\mathcal{D})
\end{array}$$

be a commutative diagram of ringed topoi, then for any $K\in D(\mathcal{O}_{\mathcal{C}})$, there is a canonical base change map
$$Lg^*Rf_*K\to R(f')_*L(g')^*K$$
functorial in K, and this map is compatible with composition of diagrams. ⌟

Proof: By adjunction(6.3.3.16), this follows from the canonical map
$$Rf_*K\to Rg_*R(f')_*L(g')^*K=Rf_*R(g')_*L(g')^*K,$$
which comes from the adjunction map $K\to R(g')_*L(g')^*K$. □

Cor. (6.3.3.18) [Flat Base Change Morphism]. Let
$$\begin{array}{ccc}(\mathcal{S}\mathrm{h}(\mathcal{C}'),\mathcal{O}_{\mathcal{C}'}) & \xrightarrow{g'} & (\mathcal{S}\mathrm{h}(\mathcal{C}),\mathcal{O}_{\mathcal{C}})\\ \downarrow f' & & \downarrow f\\ (\mathcal{S}\mathrm{h}(\mathcal{D}'),\mathcal{O}_{\mathcal{D}'}) & \xrightarrow{g} & (\mathcal{S}\mathrm{h}(\mathcal{D}),\mathcal{O}_{\mathcal{D}})\end{array}$$
be a commutative diagram of ringed sites. Assume both g,g' are flat, then for any $\mathcal{F}^\bullet\in K^+(\mathcal{O}_{\mathcal{C}})$, there is a canonical base change map
$$g^*Rf_*\mathcal{F}^\bullet\to Rf'_*(g')^*\mathcal{F}^\bullet.$$
and when $(\mathcal{S}\mathrm{h}(\mathcal{D}'),\mathcal{O}_{\mathcal{D}})=(\mathcal{S}\mathrm{h}(\mathcal{C}/U),\mathcal{O}_U)$ is the localizing site, then this map is an isomorphism
$$(Rf_*\mathcal{F}^\bullet)_U\cong Rf'_*\mathcal{F}^\bullet_U.$$
⌟

Proof: The last assertion follows from the fact the restriction of a K-injective is also a K-injective(6.3.4.2). □

Def. (6.3.3.19) [Projection Map]. Let $f:(\mathcal{S}\mathrm{h}(\mathcal{C}),\mathcal{O}_{\mathcal{C}})\to(\mathcal{S}\mathrm{h}(\mathcal{D}),\mathcal{O}_{\mathcal{D}})$ be a morphism of ringed topoi, then for any $E\in D(\mathcal{O}_{\mathcal{C}})$ and $K\in D(\mathcal{O}_{\mathcal{D}})$, there is a canonical functorial **projection map**
$$Rf_*E\otimes^L_{\mathcal{O}_{\mathcal{D}}}K\to Rf_*(E\otimes^L_{\mathcal{O}_{\mathcal{C}}}Lf^*K)$$
which is the adjunction of the map
$$Lf^*(Rf_*E\otimes^L_{\mathcal{O}_{\mathcal{D}}}K)\cong Lf^*Rf_*E\otimes^L_{\mathcal{O}_{\mathcal{C}}}Lf^*K\to E\otimes^L_{\mathcal{O}_{\mathcal{C}}}Lf^*K$$
by(6.3.3.15). ⌟

Prop. (6.3.3.20) [Projection Formula]. In situation(6.3.3.19), if K is perfect(6.3.4.17), then the projection map is an isomorphism. ⌟

Proof: To check it is an isomorphism, it suffice to find a covering $\{U_i\to V\}$ for each $V\in\mathcal{C}$ that this map is an isomorphism on U_i.(To see this, look at H^i, and notice $U\mapsto\mathcal{M}\mathrm{od}(\mathcal{O}_U)$ is a stack). Then we may assume K is a finite complex of $\mathcal{O}_U$-modules consisting of finite free $\mathcal{O}_U$-modules. And then we use truncation to reduce to the case K is discrete, in which case it is trivial. □

Inner Hom

Def. (6.3.3.21) [Sheaf Hom Complexes]. Let $(\mathcal{C},\mathcal{O})$ be a ringed site and $P^\bullet, Q^\bullet \in K(\mathcal{O})$, we define the **Sheaf Hom complex** $\mathcal{H}om^\bullet(P^\bullet, Q^\bullet)$ to be

$$\mathcal{H}om^n(P^\bullet, Q^\bullet) = \prod_i \mathcal{H}om_{\mathcal{O}}(P^i, Q^{n+i})(6.2.3.1),$$

with the differential giving by $d(\{f_k\})_i = \{df_i - (-1)^i f_{i+1} d\}$ and suitable signatures.

It is clear that

$$\Gamma(U, \mathcal{H}om^\bullet_{\mathcal{O}}(P^\bullet, Q^\bullet)) = \mathrm{Hom}^\bullet_{\mathcal{O}_U}(P^\bullet|_U, Q^\bullet|_U), \quad \Gamma(\mathcal{C}, \mathcal{H}om^\bullet_{\mathcal{O}}(P^\bullet, Q^\bullet)) = \mathrm{Hom}^\bullet_{\mathcal{O}}(P^\bullet|_U, Q^\bullet|_U)$$

and

$$H^n(\Gamma(U, \mathcal{H}om^\bullet(P^\bullet, Q^\bullet))) = \mathrm{Hom}_{K(\mathcal{O}_U)}(P^\bullet|_U, Q^\bullet|_U[n]), \quad H^n(\Gamma(\mathcal{C}, \mathcal{H}om^\bullet(P^\bullet, Q^\bullet))) = \mathrm{Hom}_{K(\mathcal{O})}(P^\bullet, Q^\bullet[n]).$$

⌟

Prop. (6.3.3.22) [Adjunction]. For $\mathcal{K}^\bullet, \mathcal{M}^\bullet, \mathcal{L}^\bullet \in K(\mathcal{O})$, there is a canonical functorial isomorphism:

$$\mathcal{H}om^\bullet(K, \mathcal{H}om^\bullet(L, M)) = \mathcal{H}om^\bullet(\mathrm{Tot}(K \otimes_R L), M).$$

⌟

Proof: Cf.[Sta]0A5Y. □

Prop. (6.3.3.23). For $\mathcal{K}^\bullet, \mathcal{M}^\bullet, \mathcal{L}^\bullet \in K(\mathcal{O})$, there are canonical functorial morphisms:

- $\mathrm{Tot}(\mathcal{H}om(\mathcal{K}^\bullet, \mathcal{L}^\bullet) \otimes_{\mathcal{O}} \mathcal{K}^\bullet) \to \mathcal{L}^\bullet$,
- $\mathrm{Tot}(\mathcal{H}om^\bullet(L, M) \otimes_{\mathcal{O}} \mathcal{H}om^\bullet(K, L)) \to \mathcal{H}om^\bullet(K, M)$,
- $\mathrm{Tot}(\mathcal{H}om^\bullet(L, M) \otimes_{\mathcal{O}} K) \to \mathcal{H}om^\bullet(\mathcal{H}om^\bullet(K, L), M)$,
- $\mathrm{Tot}(K \otimes_{\mathcal{O}} \mathcal{H}om^\bullet(M, L)) \to \mathcal{H}om^\bullet(M, \mathrm{Tot}(K \otimes_{\mathcal{O}} L))$,
- $K \to \mathcal{H}om^\bullet(L, \mathrm{Tot}(K \otimes_{\mathcal{O}} L))$.

⌟

Proof: All these are consequences of(6.3.3.22). □

Lemma (6.3.3.24). Let $(\mathcal{C},\mathcal{O})$ be a site and $(\mathcal{I}^\bullet)' \to \mathcal{I}^\bullet$ be a quasi-isomorphism of K-injective $\mathcal{O}$-modules and $(\mathcal{L}^\bullet)' \to \mathcal{L}^\bullet$ be a quasi-isomorphism of $\mathcal{O}$-modules, then the natural map

$$\mathcal{H}om^\bullet(\mathcal{L}^\bullet, (\mathcal{I}^\bullet)') \to \mathcal{H}om^\bullet((\mathcal{L}^\bullet)', \mathcal{I}^\bullet)$$

is a quasi-isomorphism. ⌟

Proof: $H^n(\mathcal{H}om^\bullet(\mathcal{L}^\bullet, (\mathcal{I}^\bullet)'))$ is the the sheaf $U \mapsto \mathrm{Hom}_{K(\mathcal{O}_U)}(\mathcal{L}^\bullet_U, (\mathcal{I}^\bullet)'_U[n])$, and $(\mathcal{I}^\bullet)'_U[n]$ is K-injective by(6.3.4.2). □

Def. (6.3.3.25) [Internal Hom]. Let $(\mathcal{C},\mathcal{O})$ be a ringed site, $K(\mathcal{O})$ has enough K-injectives, thus by(4.10.3.13), we can define the **internal Hom**

$$R\mathcal{H}om : D(\mathcal{O})^{op} \times D(\mathcal{O}) \to D(\mathcal{O})$$

as the right derived functor of the bi-exact bifunctor $\mathcal{H}om^\bullet : K(\mathcal{O})^{op} \times K(\mathcal{O}) \to D(\mathcal{O})$, where the conditions are satisfied by(6.3.3.24). ⌟

Prop. (6.3.3.26)[Internal Hom and Localization]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site, for any $\mathcal{G}, \mathcal{F} \in K(\mathcal{O})$ and $U \in \mathcal{C}$, the natural transformation

$$R\mathcal{H}om(\mathcal{F}, \mathcal{G})|_U \to R\mathcal{H}om(\mathcal{F}|_U, \mathcal{G}|_U)$$

is an isomorphism. In particular, we can calculate $\mathcal{E}xt$ locally. ⌟

Proof: This follows from(6.3.3.21)(6.3.4.2) and trivial Grothendieck duality applied to restrictions. □

Prop. (6.3.3.27) [Derived Hom and Internal Hom]. For a ringed site $(\mathcal{C}, \mathcal{O})$ and $\mathcal{F}, \mathcal{G} \in D(\mathcal{O})$, $U \in \mathcal{C}$,

$$R\Gamma(\mathcal{C}, R\mathcal{H}om(\mathcal{F}, \mathcal{G})) = R\operatorname{Hom}(\mathcal{F}, \mathcal{G}), \quad R\Gamma(U, R\mathcal{H}om(\mathcal{F}, \mathcal{G})) = R\operatorname{Hom}_{\mathcal{O}_U}(\mathcal{F}|_U, \mathcal{G}|_U).$$

In particular,

$$\Gamma(U, R\mathcal{H}om(\mathcal{F}, \mathcal{G})) = \operatorname{Hom}_{D(\mathcal{O}_U)}(\mathcal{F}|_U, \mathcal{G}|_U),$$

and

$$H^0(\mathcal{C}, R\mathcal{H}om(\mathcal{F}, \mathcal{G})) = \operatorname{Hom}_{D(\mathcal{O})}(\mathcal{F}, \mathcal{G}), \quad H^p(\mathcal{C}, R\mathcal{H}om(\mathcal{F}, \mathcal{G})) = \operatorname{Ext}^p_{\mathcal{O}}(\mathcal{F}, \mathcal{G})$$

by(6.3.3.21)(6.3.4.2)(6.3.4.13) and the composition of derived functors. ⌟

Prop. (6.3.3.28). If $\mathcal{K}, \mathcal{L}, \mathcal{M} \in D(\mathcal{O})$, then there is a natural isomorphism

$$R\mathcal{H}om_{\mathcal{O}}(\mathcal{K}, R\mathcal{H}om(\mathcal{L}, \mathcal{M})) \cong R\mathcal{H}om_{\mathcal{O}}(\mathcal{K} \otimes^{\mathrm{L}}_{\mathcal{O}} \mathcal{L}, \mathcal{M}).$$

⌟

Proof: Consider both sides as the derived functor of the triple-exact triple-functor

$$K(\mathcal{O})^{op} \times K(\mathcal{O})^{op} \times K(\mathcal{O}) \to D(\mathcal{O}) : (\mathcal{K}^\bullet, \mathcal{L}^\bullet, \mathcal{M}^\bullet) \mapsto \operatorname{Tot}^{\oplus}(\mathcal{K}^\bullet \otimes_{\mathcal{O}} \operatorname{Tot}^{\oplus}(\mathcal{L}^\bullet \otimes_{\mathcal{O}} \mathcal{M}^\bullet)),$$

the conditions are satisfied by(6.3.4.13)(6.3.3.3). As this is true for Tot by(6.3.3.22), this follows from the universal properties and(4.10.3.14). □

Cor. (6.3.3.29) [Adjunction]. By(6.3.3.28), taking $H^0(R\Gamma(\mathcal{C}, -))$, we get:

$$\operatorname{Hom}_{D(\mathcal{O})}(\mathcal{K}, R\mathcal{H}om(\mathcal{L}, \mathcal{M})) = \operatorname{Hom}_{D(\mathcal{O})}(\mathcal{K} \otimes^L \mathcal{L}, \mathcal{M}).$$

that is, derived tensor is left adjoint to internal hom. ⌟

Prop. (6.3.3.30). Given complexes $\mathcal{K}, \mathcal{L}, \mathcal{M} \in D(\mathcal{O})$, there are canonical functorial morphisms:

- $\mathcal{H}om(K, L) \otimes^L_{\mathcal{O}} K \to L$,
- $R\mathcal{H}om(L, M) \otimes^L_{\mathcal{O}} R\mathcal{H}om(K, L) \to R\mathcal{H}om(K, M)$,
- $R\mathcal{H}om(L, M) \otimes^L_{\mathcal{O}} K \to R\mathcal{H}om(R\mathcal{H}om(K, L), M)$,
- $K \otimes^L_{\mathcal{O}} R\mathcal{H}om(M, L) \to R\mathcal{H}om(M, K \otimes^L_{\mathcal{O}} L)$,
- $K \to R\mathcal{H}om(L, K \otimes^L_{\mathcal{O}} L)$.

⌟

Proof: These are direct consequences of(6.3.3.29). □

Prop. (6.3.3.31). Let $(\mathcal{S}\mathrm{h}(\mathcal{C}),\mathcal{O})\to(\mathcal{S}\mathrm{h}(\mathcal{C}'),\mathcal{O}')$ be a morphism of ringed site and $\mathcal{K},\mathcal{L}\in D(\mathcal{O})$, there is a natural morphism

$$Rf_*R\mathcal{H}om_{\mathcal{O}}(L,K)\to R\mathcal{H}om_{\mathcal{O}'}(Rf_*L,Rf_*K).$$

⌟

Proof: This follows from the adjunction(6.3.3.28)(6.3.3.30) and the relative cup product(6.3.3.13). □

Def. (6.3.3.32) [Internal Ext Groups]. For any $\mathcal{G},\mathcal{F}\in K(\mathcal{O})$, we define the **internal Ext groups**

$$\mathcal{E}xt^n_{\mathcal{O}}(\mathcal{G},\mathcal{F})=H^i(R\mathcal{H}om(\mathcal{G},\mathcal{F}))\in\mathcal{M}\mathrm{od}(\mathcal{O}).$$

⌟

Prop. (6.3.3.33). For $\mathcal{E},\mathcal{F},\mathcal{L}\in\mathcal{M}\mathrm{od}(\mathcal{O}_X)$ and $\mathcal{L}$ finite locally free,

$$\mathcal{E}xt^i(\mathcal{F}\otimes\mathcal{L},\mathcal{G})\cong\mathcal{E}xt^i(\mathcal{F},\mathcal{L}^\vee\otimes\mathcal{G})\cong\mathcal{E}xt^i(\mathcal{F},\mathcal{G})\otimes\mathcal{L}^\vee$$

because there are maps between them(6.2.5.2), and $\mathcal{E}xt$ is local, so check locally. In particular,

$$\mathrm{Ext}^i(\mathcal{F}\otimes\mathcal{L},\mathcal{G})=\mathrm{Ext}^i(\mathcal{F},\mathcal{L}^\vee\otimes\mathcal{G}).$$

⌟

Prop. (6.3.3.34) [Spectral Sequences for Internal Ext]. Let $(\mathcal{C},\mathcal{O})$ be a ringed site and $\mathcal{K}^\bullet\in K^-(\mathcal{O}),\mathcal{F}^\bullet\in K^+(\mathcal{O})$, then there are spectral sequence convergence

$$E_2^{i,j}=\mathcal{E}xt^i_{\mathcal{O}}(H^{-j}(\mathcal{K}^\bullet),\mathcal{F}^\bullet)\Longrightarrow\mathcal{E}xt^{i+j}_{\mathcal{O}}(\mathcal{K}^\bullet,\mathcal{F}^\bullet).$$
$$E_1^{i,j}=\mathcal{E}xt^j_{\mathcal{O}}(\mathcal{K}^{-i},\mathcal{F}^\bullet)\Longrightarrow\mathcal{E}xt^{i+j}_{\mathcal{O}}(\mathcal{K}^\bullet,\mathcal{F}^\bullet)$$
$$E_2^{i,j}=H^i(\mathcal{C},\mathcal{E}xt^j_{\mathcal{O}}(\mathcal{K}^\bullet,\mathcal{F}^\bullet))\Longrightarrow\mathrm{Ext}^{i+j}_{\mathcal{O}}(\mathcal{K}^\bullet,\mathcal{F}^\bullet)$$

⌟

Proof: 1, 2: Choose a (bounded below) injective resolution $\mathcal{I}^\bullet$ of $\mathcal{F}^\bullet$, and these are the two spectral sequences associated to the double complex $\mathcal{H}om^\bullet_{\mathcal{O}}(\mathcal{K}^\bullet,\mathcal{I}^\bullet)$.

3: Use Grothendieck spectral sequence on(6.3.3.27). □

4 Acyclic Sheaves

Prop. (6.3.4.1) [Pushforward of Injectives]. Let $f:(\mathcal{S}\mathrm{h}(\mathcal{C}),\mathcal{O}_C)\to(\mathcal{S}\mathrm{h}(\mathcal{D}),\mathcal{O}_D)$ be a flat map of ringed topoi, then f preserves injectives, as f^* is exact. ⌟

Prop. (6.3.4.2) [Restriction of (K-)Injectives]. Let $(\mathcal{C},\mathcal{O})$ be a ringed site, $U\in\mathcal{C}$, then

- If $\mathcal{K}^\bullet$ be a K-injective complex $\mathcal{O}$-modules, then $(\mathcal{K}^\bullet)|_U$ is a K-injective complex of $\mathcal{O}_U$-modules.
- If $\mathcal{I}$ is an injective $\mathcal{O}$-module, then $\mathcal{I}|_U$ is an injective $\mathcal{O}$-module.

⌟

Proof: Use(4.10.2.6) and the fact j_U^* is right adjoint to the exact functor $j_{U!}$(6.2.2.9)(6.2.2.9). □

Prop. (6.3.4.3). If $\mathcal{I}\in\mathcal{S}\mathrm{h}(\mathcal{C})$ is injective, then $\mathcal{I}$ is also injective in $\mathcal{PS}\mathrm{h}(\mathcal{C})$. ⌟

Proof: Because restriction is right adjoint to the exact shifification functor. □

Prop. (6.3.4.4). For an injective sheaf $\mathcal{F}$ on a site $(\mathcal{C},\mathcal{O})$, $F(U)$ is injective Abelian group for every $U\in\mathcal{C}$. ⌟

Proof: This is because for the morphism $i:\mathrm{pt}\to\mathcal{C}:\mathrm{pt}\mapsto U$, i_p is exact($i_pA(V)=\oplus_{\mathrm{Hom}(V,U)}A$), hence i^p preserves injectives. □

Flask Sheaves

Def. (6.3.4.5) [Totally Acyclic Sheaves]. A **totally acyclic sheaf** on a ringed site $(\mathcal{C},\mathcal{O})$ is an object in $\mathcal{S}h(\mathcal{C})$ that is acyclic for any functor $\mathrm{Hom}_{\mathcal{PS}h(\mathcal{C})}(K,-)$. ⌟

Prop. (6.3.4.6) [Characterization of Totally Acyclic Sheaves]. Let $\mathcal{C}$ be a site and $\mathcal{F}\in\mathcal{S}h(\mathcal{C})$, then $\mathcal{F}$ is totally acyclic iff

- $\mathcal{F}$ is acyclic for $\Gamma(U,-)$ for any $U\in\mathcal{C}$.
- For every surjection $K'\to K$ of sheaves of sets the extended Čech complex
$$0\to H^0(K,\mathcal{F})\to H^0(K',\mathcal{F})\to H^0(K'\times_K K',\mathcal{F})\to\dots$$
is exact.

⌟

Proof: Cf.[Sta]07A1. □

Prop. (6.3.4.7). A totally acyclic sheaf is acyclic for any map of ringed topoi $f:(\mathcal{S}h(\mathcal{C}),\mathcal{O}_C)\to(\mathcal{S}h(\mathcal{D}),\mathcal{O}_D)$. ⌟

Proof: This follows from the description of R^if_* in(6.3.1.7). □

Def. (6.3.4.8)[Flask Sheaves]. A **flask sheaf** on a ringed site $(\mathcal{C},\mathcal{O})$ is an object of $\mathcal{S}h(\mathcal{C})$ that satisfies the following equivalent conditions:

- it is acyclic for ι.
- It is acyclic for any $\check{H}^0(\{U_i\to U\},-)$
- It is acyclic for all $\Gamma(U,-)$.

In particular a totally acyclic sheaf is flask.

A **flabby sheaf** is an object of $\mathcal{S}h(\mathcal{C})$ that for any monomorphism $U\to V$, $\mathcal{F}(V)\to\mathcal{F}(U)$ is surjective; ⌟

Proof: $1\iff 3$ is by(6.3.1.6),

$3\to 2$: use Čech to sheaf1(6.3.2.13), notice the $q>0$ terms vanish, thus $\check{H}^p(\{U_i\to U\},\mathcal{F})=H^p(U,\mathcal{F})=0$.

$2\to 3$ follows from(6.3.2.16). □

Prop. (6.3.4.9). Injective sheaves are flabby, Flabby sheaves on a ringed space are flask. ⌟

Proof: For the first assertion, use(6.2.2.9) and the fact $j_!\mathcal{O}_U\to j_!\mathcal{O}_V$ is a monomorphism for $V\to U$ a monomorphism by definition(6.2.2.9).

For the last assertion, use(4.10.3.29): Injectives are flabby, so it is sufficiently large. For an exact sequence $0\to\mathcal{F}\to\mathcal{G}\to\mathcal{H}\to 0$ of sheaves, if $\mathcal{F}$ is flabby, then H is just the presheaf cokernel. (It reduces to $\check{H}^1(\{U_i\to U\},F)=0$, and this is done by Zorn's lemma). Thus if $\mathcal{F}$ is flabby, $\mathcal{G}$ is flabby iff $\mathcal{H}$ is flabby(by five lemma). □

Prop. (6.3.4.10). On a discrete site, all sheaves is flask, because ι is the identity functor. ⌟

Prop. (6.3.4.11). Filtered colimits of flabby sheaves is flabby. (This is because filtered colimits are exact).

Filtered colimits of injective sheaves over a Noetherian topological space is injective. (Use Baer criterion, then notice every sub-object of $\mathbb{Z}_U$ is finitely generated because it has only f.m. connected component(4.12.3.4) so it maps to some F_α). ⌟

Prop. (6.3.4.12) [Pushforward of Totally Acyclic/Flask Sheaves]. Let $f : (\mathcal{Sh}(\mathcal{C}), \mathcal{O}_C) \to (\mathcal{Sh}(\mathcal{D}), \mathcal{O}_D)$ be a map of ringed topoi(reps. ringed site), then f_* maps totally acyclic(resp. flask) sheaves to totally acyclic(resp. flask) sheaves(6.3.4.5)(6.3.4.8). in particular, it maps injectives to totally acyclic sheaves. ⌟

Proof: By(6.2.1.3) we may assume f is a map of ringed sites, and $K = h_U$ for some $U \in \mathcal{C}$. Then we notice $H^*(\{U_i \to U\}, f_*\mathcal{F}) = H^*(\{f^{-1}(U_i) \to f^{-1}(U)\}, \mathcal{F})$, then we can use(6.3.2.16) to show $f_*\mathcal{F}$ is totally acyclic. □

Prop. (6.3.4.13) [Technical Lemma]. If $\mathcal{K}^\bullet$ is K-flat $\mathcal{O}$-modules and $\mathcal{I}^\bullet$ is K-injective $\mathcal{O}$-modules, then $\mathcal{H}om^\bullet(\mathcal{K}^\bullet, \mathcal{I}^\bullet)$ is K-injective. ⌟

Proof: Use definitions(6.3.3.1)(4.10.2.1) and(6.3.3.22). □

Prop. (6.3.4.14). If $\mathcal{I}$ is an injective $\mathcal{O}_X$-module, then for a coherent locally free sheaf $\mathcal{L}$, $\mathcal{L} \otimes \mathcal{I}$ is also injective, because tensoring with $\mathcal{L}$ is adjoint to tensoring with $\mathcal{L}^\vee$(6.2.5.2), which is exact. ⌟

Pseudo-Coherent Sheaves

Def. (6.3.4.15) [Strictly Perfect Complexes of Modules]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site, a **strictly perfect complex of $\mathcal{O}$-modules** of $\mathcal{O}$-modules is a finite complex of $\mathcal{O}$-modules that each term is a direct summand of a finite free $\mathcal{O}$-module. ⌟

Def. (6.3.4.16) [Pseudo-Coherent Complexes of Modules]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site, then $\mathcal{K} \in D(\mathcal{O}_X)$ is called an **m-pseudo-coherent $\mathcal{O}_X$-module** if for any $U \in \mathcal{C}$, there exists a covering $\{U_i \to U\}$ s.t. for any i, there are strictly perfect object $E_i \in D(\mathcal{O}_{U_i})$ and a morphism $E_i \to K|_{U_i}$ that induces isomorphisms on H^i for $i > m$ and surjection on H^m.

$K \in D(R)$ is called a **pseudo-coherent $\mathcal{O}_X$-module** if it is m-pseudo-coherent for any m. ⌟

Perfect Sheaves

Def. (6.3.4.17) [Perfect Complexes of Modules]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site, a **perfect complex of $\mathcal{O}$-modules** of $\mathcal{O}$-modules is an object E in $\mathcal{D}(\mathcal{O})$ that for any $U \in \mathcal{C}$ there is a covering $\{U_i \to U\}$ that $E|_{U_i}$ is can be represented by a strictly perfect complexes(6.3.4.15). ⌟

Prop. (6.3.4.18). Every mapping from a strictly perfect complex to an acyclic complex has a cover of open sets that on each open set the map is nullhomotopic. ⌟

Proof: This is true for a single direct summand of a finite free sheaf, and we can use induction to prove, Cf.[Sta]08C7. □

Cor. (6.3.4.19). The strictly perfect complexes are fake "K-projective" objects in $K(\mathcal{O}_X)$. Note it is note technically K-projective, but it has all the properties of K-projective when proven, noticing the fact it is irrelevant when taken shifification. ⌟

Def. (6.3.4.20) [Perfect Sheaves]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site, an object $K^\bullet$ in $K(\mathcal{O})$ **perfect** if there is a covering $\mathcal{U}$ that on each U_i there is a quasi-iso $K_i^\bullet \to K^\bullet|_{U_i}$ with $K_i^\bullet$ strictly perfect.

This is equivalent to $K^\bullet$ is locally represented by perfect objects in $D(\mathcal{O})$ by the fact that perfect object is fake K-projective. ⌟

Prop. (6.3.4.21). When X is local ringed space, perfectness is equivalent to the fact that it is locally a finite free $\mathcal{O}_{U_i}$-module. ⌟

Proof: This is because direct summand of a finite free module is free, Cf.[Sta]0BCI. □

Prop. (6.3.4.22) [Strictly Perfect Modules are "Acyclic" for $\mathrm{Hom}^\bullet$**].** If $(\mathcal{C}, \mathcal{O})$ is a ringed site and $\mathcal{E}^\bullet, \mathcal{F}^\bullet \in K(\mathcal{O})$, then $R\mathcal{H}om(\mathcal{E}^\bullet, \mathcal{F}^\bullet)$ can be calculated directly by $\mathcal{H}om^\bullet(\mathcal{E}, \mathcal{F})$ in the following cases:

- $\mathcal{E}^\bullet$ is strictly perfect.
- $\mathcal{E}^\bullet \in D^-(\mathcal{O}_X), \mathcal{F}^\bullet \in D^+(\mathcal{O}_X)$, and each term $\mathcal{E}^n$ is a direct summand of a finite free $\mathcal{O}_X$-module.

⌟

Proof: Cf.[Sta]08I5, 08DM. □

Prop. (6.3.4.23) [Duals]. Let K be a perfect object in $D(\mathcal{O})$, then

- $K^\vee = R\mathcal{H}om(K, \mathcal{O})$ is also a perfect object, and $(K^\vee)^\vee \cong K$.
- For any $M \in D(\mathcal{O})$, there are functorial isomorphisms

$$M \otimes^{\mathrm{L}} K^\vee \cong R\mathcal{H}om(K, M), \quad H^0(\mathcal{C}, M \otimes^{\mathrm{L}} K^\vee) \cong \mathrm{Hom}_{D(\mathcal{O})}(K, M).$$

⌟

Proof: Cf.[Sta]08JJ. □

Def. (6.3.4.24) [Relative Perfect Modules]. Let $(X, \mathcal{O}_X) \to (S, \mathcal{O}_S)$ be a morphism of ringed sites that is flat and locally of f.p., then $E \in D(\mathcal{O}_X)$ is called a **perfect object relative to** S if E is pseudo-coherent and E locally has finite tor dimension as an object in $D(f^{-1}\mathcal{O}_S)$. Cf.[Sta]08CG. ⌟

5 Topological Sheaves

References are [Sheaf Cohomology, Anonymous].

A topological space can be seen as a ringed site, so the theory of ringed sites applies to topological spaces.

Acyclic sheaves

Def. (6.3.5.1). An Abelian sheaf on a paracompact Hausdorff topological space X is called

soft iff is and $\forall$ closed $V, \mathcal{F}(X) \to \mathcal{F}(V)$ is surjective. A flabby sheaf is soft.

fine iff the sheaf of rings $\mathrm{Hom}(\mathcal{F}, \mathcal{F})$ is soft.

Fine and soft are local properties (Use Zorn's lemma to construct one-by-one).

⌟

Prop. (6.3.5.2). For a sheaf of **unital rings** over a paracompact Hausdorff space X, the following are equivalent,

1. it is a soft sheaf.
2. for any disjoint closed sets V, W, there is a section of X that is 0 on V, and 1 on W.
3. it possesses a partition of unity.
4. it is a fine sheaf.

Note any soft sheaf possesses a partition of unity. ⌟

Proof: 1 $\iff$ 2 is easy and $1 \to 3$ is the to choose a closed locally finite subcover and use Zorn's lemma to construct one-by-one. For $3 \to 1$, notice a closed section can extend to a slightly larger nbhd.

Because for a sheaf of rings $\mathcal{F}$, a partition of unity is equivalent to a partition of unity $\mathrm{Hom}(\mathcal{F},\mathcal{F})$, so 34 are equivalent because 13 are equivalent. □

Cor. (6.3.5.3).

- Note that a fine sheaf possesses a decomposition of section because the previous proposition applies to $\mathrm{Hom}(\mathcal{F},\mathcal{F})$, and a partition of unity in $\mathrm{Hom}(\mathcal{F},\mathcal{F})$ yields a decomposition of section in $\mathcal{F}$. Thus a fine sheaf is soft. (extend to a small nbhd and use partition of unity).
- The sheaf of modules over a soft sheaf of rings is soft, by partition of unity.
- The continuous function sheaf on a paracompact Hausdorff space or the smooth function sheaf on a smooth manifold is fine, thus any smooth module is fine (Use bump function).

⌟

Prop. (6.3.5.4). Soft sheaf, e.g. fine sheaf is adapted to $\Gamma(X,-)$. (Similar as in(6.3.4.9), notice flabby is soft and the others are the same as before). ⌟

Prop. (6.3.5.5). Let X be a locally compact space of finite compact dimension, when S is a soft sheaf, and one of S and $\mathcal{F}$ is flat, then $S \otimes_k \mathcal{F}$ is soft. Cf.[Cohomology of Sheaves Iversen P319]. ⌟

Prop. (6.3.5.6). Over a locally compact space of finite dimension, any flat sheaf $\mathcal{F}$ on X has a resolution of soft flat sheaves. ⌟

Proof: Cf.[Gelfand P232]. □

Lemma (6.3.5.7). A constant sheaf on an irreducible topological space is flabby, thus flask. ⌟

Basics

Prop. (6.3.5.8). If $i : Z \to X \in \mathcal{T}\mathrm{op}$ is a closed immersion, then for any $\mathcal{F} \in \mathcal{S}\mathrm{h}(Z)$, $H^*(Z,\mathcal{F}) = H^*(Z, i_*\mathcal{F})$. ⌟

Proof: This is because i_* is exact(6.2.6.7), so we can apply the Leray spectral sequence(6.3.1.9). □

Comparison Theorems

Prop. (6.3.5.9) [Singular]. For any locally contractible topological space X and $G \in \mathcal{A}\mathrm{b}$, there are canonical isomorphisms

$$H^*_{\mathrm{sing}}(X, G) \cong H^*(X, \underline{G}).$$

⌟

Proof: Shifification of the singular cochain complex is a flabby presheaf resolution of $\underline{G}$ because it is locally contractible, check on stalks. Then we only have to prove $C^\bullet(X) \to (C/V)^\bullet(X)$ is quasi-isomorphism, where V is the presheaf of locally vanishing cochain. It suffice to prove $V^\bullet(X)$ is exact.

For any i-cocycle φ, for any $i-1$-complex σ, use barycentric subdivision, we can construct a c_σ whose boundary is σ and other simplexes on which ϕ vanishes, so we have the coboundary of $\eta : \sigma \to \varphi(c_\sigma)$ is φ. □

Lemma (6.3.5.10) [Poincaré]. For a smooth manifold X of dimension n, there is an exact sequence

$$0 \to \underline{\mathbb{R}}_X \xrightarrow{\mathrm{d}} \Omega - X^0 \xrightarrow{\mathrm{d}} \Omega - X^1 \xrightarrow{\mathrm{d}} \ldots \xrightarrow{\mathrm{d}} \Omega_X^n \to 0$$

⌟

Proof: □

Prop. (6.3.5.11) [DeRham]. For any smooth manifold X,

$$H^*_{\mathrm{dR}}(X, \underline{\mathbb{R}}_X) \cong H^*(X, \underline{\mathbb{R}})$$

Where the right is constant sheaf cohomology. ⌟

Proof: Use the fact that smooth sheaf is fine so adapted to sheaf cohomology(6.3.5.4), and Poincaré lemma(6.3.5.10). □

Prop. (6.3.5.12) [Period Maps]. For a smooth manifold X, by a similar method as(6.3.5.9), we can define a **differentiable singular cohomology** $H^*_{\mathrm{sing},\infty}(X)$, and prove a canonical isomorphism

$$H^*_{\mathrm{sing},\infty}(X, \mathbb{R}) \cong H^*(X, \overline{\mathbb{R}}).$$

Then combining with(6.3.5.11), we get a canonical isomorphism

$$H^*_{\mathrm{dR}}(X, \underline{\mathbb{R}}_X) \cong H^*_{\mathrm{sing},\infty}(X, \mathbb{R})$$

which can be described as follows: there is a map of sheaves

$$\Omega^k \to C^\bullet_{\mathrm{sing},\infty}(X)$$

that is locally defined to be $\omega \mapsto \sigma \mapsto \int_\sigma \omega$, then this map gives a map of complexes

$$\Omega^\bullet \to C^\bullet_{\mathrm{sing},\infty}(X)$$

that induces the isomorphism. ⌟

Proof: **?** Cf.[Warner, P206]. □

Prop. (6.3.5.13) [Čech and Sheaf Cohomology]. For a paracompact Hausdorff space X, there are isomorphisms

$$\check{H}^i(X, \mathbb{Z}) \cong H^i(X, \mathbb{Z}).$$

⌟

Proof: Cf.[Godement, Prop5.10.1].**?** □

Cohomology with Proper Support

References are [Cohomology of Sheaves Iversen].

Prop. (6.3.5.14). Soft sheaf is adapted to $f_!$ when X, Y are locally compact. Cf.[Gelfand P226]. So we can use soft resolution to define $R^i f_!$, in particular, when $Y = \mathrm{pt}$, we denote it by $H^i_c(X, \mathcal{F})$. Using(6.2.6.2), we get the stalk of $R^i f_!(\mathcal{F})$ at y is just $H^i_c(f^{-1}(y), \mathcal{F}|_{f^{-1}(y)})$. ⌟

Def. (6.3.5.15). The **compact dimension** of a locally compact topological space is the smallest n that $H^i_c(X, \mathcal{F}) = 0$ for $i > n$. It is also the maximal length of minimal soft resolution.

$\dim_c \mathbb{R}^n = n$, and when Y is an open or closed subset of X, $\dim_c Y \le \dim_c X$. $\dim_c$ is local in the sense if every point has a nbhd of dimension$\le n$, then $\dim_c X \le n$. Cf.[Iversen]. ⌟

Prop. (6.3.5.16) [Proper Pushforward Commutes with Pullback]. For a pullback diagram

$$\begin{array}{ccc} X \times_Y Z & \xrightarrow{\tau'} & X \\ \downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} \\ Z & \xrightarrow{\tau} & Y \end{array}$$

we have $\tau^{-1}(\pi_! \mathcal{F}) = \pi'_!(\tau')^{-1}\mathcal{F}$. ⌟

Proof: □

Cohomology on Noetherian Spaces

There are three basic objects, the derived functor for f_* as an Abelian sheaf, f_* as a $\mathcal{O}_X$-module, $\Gamma(U, -)$ as an Abelian sheaf. Notice that an Abelian group is just a $\mathbb{Z}$-module.

Prop. (6.3.5.17) [Grothendieck Vanishing]. The sheaf cohomology of an Abelian sheaf over a Noetherian topological space of dimension n vanish for $k > n$. ⌟

Proof: Use(6.2.6.10) and(6.3.5.8) and long exact sequence, we can reduce to the case of X irreducible. Then we induct on dimension. Notice first any sheaf is a filtered colimits of sheaf generated by f.m sections, thus we can use(6.3.1.14) to reduce to f.m sections case. And notice $\mathcal{F}_{\alpha'} \to \mathcal{F}_\alpha \to \mathcal{G}$, then G Is generated by at most $|\alpha| - |\alpha'|$ elements, so reduce to the one section case.

Now it is a quotient sheaf of $\mathbb{Z}$, look at the kernel R. If the kernel is $d\mathbb{Z}$ at the generic pt, then $R|_V \cong \mathbb{Z}$ on some nbhd, and $R|_V/\mathbb{Z}$ supports on a lower dimension set, then we only need to consider the pushout of constant sheaf $\mathbb{Z}_U$.

Now there is an exact sequence $0 \to \mathbb{Z}_U \to \mathbb{Z} \to \mathbb{Z}_Y \to 0$(6.2.6.10), $\mathbb{Z}$ is flabby(6.3.5.7) so flask, and the conclusion follows by induction.

Cf.[Sta]02UU.? □

Prop. (6.3.5.18). For $f : X \to Y$, if $\mathcal{I}$ is an injective module on X, then $\check{H}^p(\{U_i \to U\}, f_*\mathcal{I}) = 0$ for every open cover for an open subset U(6.3.4.8). This is because Čech cohomology is a derived functor. (Notice $f_*\mathcal{I}$ may not be injective when f is not flat). ⌟

Cor. (6.3.5.19) [Mayer-Vietoris]. For $X = U \cup V$, there is a long exact sequence

$$0 \to H^0(X, \mathcal{F}) \to H^0(U, \mathcal{F}) \otimes H^0(V, \mathcal{F}) \to H^0(U \cap V, \mathcal{F}) \to H^1(X, \mathcal{F}) \to \cdots$$

derived from the Čech to sheaf1 because it has only two column, just wrap out the definition. ⌟

6.4 Properties of Schemes

Main References are [Har77], [Sta] and [Tin20].

1 Basic Scheme Properties

Affine Local Properties of Schemes

Lemma (6.4.1.1) [Nike's Trick]. In a scheme X and $x \subset \operatorname{Spec} A \cap \operatorname{Spec} B$, x has an open nbhd in $\operatorname{Spec} A \cap \operatorname{Spec} B$ that are distinguished in both $\operatorname{Spec} A$ and $\operatorname{Spec} B$. ⌟

Proof: Choose a nbhd of x that is distinguished in $\operatorname{Spec} A$ that is contained in $\operatorname{Spec} \cap \operatorname{Spec} B$, then because distinguished of distinguished is distinguished, we may assume $i : \operatorname{Spec} A \subset \operatorname{Spec} B$. Now let $f \in B$ be an element that $D(f) \subset \operatorname{Spec} A$, then I claim $D(i^\sharp(f)) = D(f)$, this will finish the proof, but this is equivalent to $i^{-1}(\operatorname{Spec} B_f) = \operatorname{Spec} A_{i^\sharp(f)}$, which is true for ideal-theoretical reason. □

Prop. (6.4.1.2) [Affine Communication Theorem]. A property P of affine open subsets is called **affine local** if: $\operatorname{Spec}(A)$ has $P \Rightarrow$ all $\operatorname{Spec}(A_f)$ has P, and any cover of $\operatorname{Spec}(A_{f_i})$ has $P \Rightarrow \operatorname{Spec}(A)$ has P. Notice a stalk-wise property is obviously affine-local.

Now if we call X has $\widetilde{P}$ if $X = \bigcup_i \operatorname{Spec} A_i$ that A_i has P. Then the following is equivalent:

- any open affine subscheme of X has P.
- any open subscheme of X has $\widetilde{P}$.
- X has a cover of open subschemes that has $\widetilde{P}$.
- X has $\widetilde{P}$.

⌟

Proof: $1 \to 2 \to 3 \to 4$ is obvious. It suffices to prove $4 \to 1$: if $X = \cup \operatorname{Spec} A$, for any open affine subscheme of X, by(6.4.1.1), it can be covered by distinguished opens that are also distinguished in some $\operatorname{Spec} A_i$, so by hypothesis it has P. □

Remark (6.4.1.3). When proving locality of morphism properties using affine communication theorem, one usually resort to Local Properties. ⌟

Prop. (6.4.1.4) [List of Stalkwise Properties]. All properties defined by a stalkwise ring-theoretic property that is stalkwise.(5.1.4.2) ⌟

Prop. (6.4.1.5) [List of properties affine local on the target]. (All the property besides the H-projectiveness is local on the target).

1. Because affineness is local on the target(6.1.5.26), all properties defined by a ring-theoretic property local on the target is local on the target(5.1.4.4).
2. All properties that is stalkwise.
3. All properties that satisfies faithfully flat descent.(6.1.5.26)
4. Locally projective morphism.

⌟

Prop. (6.4.1.6) [List of properties affine local on the source]. (not complete)

1. All properties defined to be local ring map property local on the source.(5.1.4.4)

2. Openness.

⌟

Proof:

1. Trivial.
2. Trivial.

□

Irreducible

Def. (6.4.1.7) [Irreducible Schemes]. A scheme is called **irreducible** iff its underlying topological space is irreducible. ⌟

Prop. (6.4.1.8) [Nearly Affine Local]. For a scheme, the following are equivalent:

1. It is irreducible.
2. There is an affine cover U_i of X that U_i are all irreducible and $U_i \cap U_j \neq \varnothing$.
3. Every affine open subset of X is irreducible.

⌟

Proof: A scheme is sober(6.2.7.11), if X is irreducible, then X has a unique generic pt η that $\overline{\{\eta\}} = X$, then $2, 3$ all holds. If 2 holds, then for a decomposition $X = Z_1 \cup Z_2$, any U_i belongs to Z_1 or Z_2, so it is easy to see $Z_1 = X$ or $Z_2 = X$. If 3 holds, then choose an affine cover U_i of X, then $U_i \cap U_j \neq 0$, otherwise $U_i \coprod U_j$ is affine and not irreducible, contradiction, so 2 holds. □

Cor. (6.4.1.9). The fiber product of irreducible schemes is irreducible, because . ⌟

Reducedness

Def. (6.4.1.10) [Reduced Schemes]. A scheme is called **reduced** if $\mathcal{O}_X(U)$ is reduced for every open set U. Reduced is a stalk-wise property(6.4.1.5), it suffices to check reducedness at closed pts. ⌟

Prop. (6.4.1.11). For a reduced scheme X, $\Gamma(X, \mathcal{O}_X) \to \prod_{x\in X} k(x)$ is injective. ⌟

Prop. (6.4.1.12). If X is locally Noetherian, the set of points with reduced stalk is open in X. ⌟

Proof: This set is just the set of points x that $\mathcal{N}_x = 0$, where $\mathcal{N}$ is the sheaf of nilradicals, which is coherent, so it has closed supports(6.5.1.38). □

Prop. (6.4.1.13) [Reduction]. There is a $X_{\text{red}} \to X$ associated tot every scheme, it is $\mathbf{Spec}(\mathcal{O}_X/\mathcal{N})$ where $\mathcal{N}$ is the sheaf of nilpotent elements. This construction is right adjoint to the forgetful functor by the adjoint property of **Spec**(6.2.7.12). $X_{\text{red}} \to X$ is an closed immersion.

It's useful to change to X_{red} when the proposition only involve topology because X_{red} has the same topology as X. A map can induce a map on their reduced structure. ⌟

Prop. (6.4.1.14) [Induced Reduced Scheme Structure]. Let Z be a locally closed subset of a scheme X, There is a unique reduced subscheme Z_{red} of X with underlying topological space Z, called the **induced reduced scheme structure** of Z. It has the universal property that any morphism from a reduced scheme Y to X that has image in Z factors through this subscheme(By virtue of reducedness).

In particular, there is a closed subscheme structure X_{red} of X, called the **underlying reduced subscheme** of X. ⌟

Proof: The uniqueness is clear by the universal property. The existence is clear when X is affine and Z is closed in X. Then we can use the uniqueness to glue them to a global subscheme structure. □

Integral

Def. (6.4.1.15) [Integral Schemes]. A scheme X is called **integral** if $\mathcal{O}_X(U)$ are all integral. This is equivalent to reduced and irreducible. So a scheme is integral iff there is an integral open affine cover that are pairwise-intersect(6.4.1.7).

The category of integral schemes is denoted by $\mathcal{S}\mathrm{ch}^{\mathrm{int}}$. ⌟

Proof: If X is irreducible and reduced, then so does any affine subscheme $\operatorname{Spec} R$, so R is integral as (0) is the generic prime, because it has only one minimal prime consisting of nilpotent elements. Conversely, if X is reduced, then any affine subscheme $\operatorname{Spec} R$ is integral so reduced, and is irreducible by the presence of prime (0). □

Cor. (6.4.1.16). The projective space over an integral scheme is integral. (Check the affine covers are dense). The projective space $P^n_{\mathbb{Z}}$ is integral. ⌟

Prop. (6.4.1.17)[Integral is Almost Stalkwise]. Let X be a non-empty and connected scheme, then X is integral iff all the ⌟

Def. (6.4.1.18)[Function Field]. Let X be an integral scheme with generic point η, then $R(X) \cong \mathcal{O}_{X,\eta}$ is a field(6.2.8.2), called the **function field of** X, denoted by $K(A)$. Then any rational function on X is defined on an open dense subset of X. ⌟

Prop. (6.4.1.19). If X is an integral scheme and Z_1, Z_2 are closed subschemes of X with generic points η_1, η_2, then $\mathcal{O}_{X,\eta_1} \not\subseteq \mathcal{O}_{X,\eta_2}$. In particular, if $Z = \{x\}$ consists of a closed point, then there is a rational function defined near x that is not in $\mathcal{O}_{X,\eta_2}$. ⌟

Proof: [Sta]02NF. □

Noetherian

Def. (6.4.1.20) [Noetherian Scheme]. A scheme is called **locally Noetherian** if it can be covered by open affine schemes of noetherian rings. It is called **Noetherian** if moreover it is quasi-compact.

(Locally)Noetherian is affine local(6.4.1.5). ⌟

Prop. (6.4.1.21)[Noetherian Scheme is Noetherian]. The underlying space of a Noetherian scheme is a Noetherian space. ⌟

Proof: By(4.12.3.3), we are reduced to the affine case. Now it is clear from the definition. □

Prop. (6.4.1.22). Any locally closed subscheme of a (locally)Noetherian scheme is (locally)Noetherian. In particular, an subset of a Noetherian scheme is quasi-compact. ⌟

Proof: This is because any localization and quotients of a Noetherian ring is Noetherian(5.1.1.41), and any subset of a Noetherian space is quasi-compact(4.12.3.2)(6.4.1.21). □

Prop. (6.4.1.23) [Finitely Many Irreducible Components]. For a closed subscheme in a locally Noetherian space, the collection of its irreducible components is locally finite in X, because a Noetherian space has f.m. irreducible components(4.12.3.4).

In particular, a locally Noetherian space is locally connected. ⌟

Prop. (6.4.1.24). Let k'/k be a f.g. field extension, then a scheme X over k is locally Noetherian iff $X_{k'}$ is locally Noetherian. ⌟

Proof: Locally Noetherian is affine local, so the problem is totally ring-theoretic. If $X_{k'}$ is Noetherian, then so does X by ff descent(5.4.2.1). If X is Noetherian, then so does $X_{k'}$ by(5.1.1.45). □

Jacobson

Def. (6.4.1.25). An scheme is called **Jacobson** iff its underlying topological space is Jacobson(4.12.3.21). In particular, an affine scheme $\operatorname{Spec} R$ is Jacobson iff R is Jacobson(5.2.6.5).

So by(4.12.3.22), being Jacobson is a local property. ⌟

Prop. (6.4.1.26) [Locally Algebraic Scheme is Jacobson]. For a scheme locally algebraic over a field k, the set of closed points X_0 is dense in every closed subset of X, Because it is a Jacobson space by(4.12.3.22) and(5.2.6.10). Equivalently, every locally closed subset of X contains a closed point.

Moreover, the residue field of a closed point is finite over k by(5.2.6.10), and the converse is also true. In particular, by(6.2.7.9), the closed points of X are just the geometric points. ⌟

Proof: For the converse, because $k \subset A/\mathfrak{p}_x \subset k(x)$ are finite hence integral extensions, by(5.2.1.3) $A/\mathfrak{p}_x$ is a field, thus x is a closed point. □

Cor. (6.4.1.27) [Algebraic Scheme Preserves Closed Points]. A morphism between algebraic schemes over a field k maps closed points to closed points. ⌟

Remark (6.4.1.28). When X is geo.reduced, a stronger statement shows the set of separable closed points of X is dense in X, Cf.(6.4.3.3). ⌟

Cor. (6.4.1.29) [Check Surjectiveness on Closed Points]. If a morphism of locally algebraic schemes over a field k is surjective on closed points, then it is surjective. ⌟

Proof: By Chevalley theorem(6.6.1.5), the image is a locally constructible set, thus the supplement set is also locally constructible. Now if it is not surjective, then there is an open closed subset $U \cap Z$ not in the image. But this set contains a closed point by(6.4.1.26), which is a contradiction . □

Cohen-Macaulay

Def. (6.4.1.30) [Cohen-Macaulay Schemes]. A **Cohen-Macaulay scheme** of a C.M. scheme is a scheme $X \in \mathcal{S}ch$ s.t. all its stalks is C.M. local. Thus being C.M. is a stalkwise property. ⌟

Catenary Schemes

Def. (6.4.1.31) [Catenary Schemes]. A **catenary scheme** is a scheme that its underlying space is catenary. A scheme S is called **universally catenary** iff S is locally Noetherian and every scheme locally of f.t. over S is catenary.

(Universally) catenary is a stalkwise property, by(5.1.4.2). ⌟

Prop. (6.4.1.32) [Catenary and Dimension Functions]. Let $X \in \mathcal{S}ch$ be locally Noetherian, then X is catenary iff locally around every point there is a dimension function, by(4.12.3.39). ⌟

Example (6.4.1.33) [Universally Catenary Schemes]. The following are some examples of universally catenary schemes, by(5.2.4.7).

- A scheme locally of f.t. over a universally catenary scheme.
- A C.M. scheme.
- Spectrum of a 1-dimensional Noetherian domains,
- Spectrum of a fields.

⌟

Japanese & Nagata Schemes

Def. (6.4.1.34) [Japanese & Nagata Schemes]. A (universally)**Japanese scheme** is a scheme that can be covered by open affine spectrum of (universally)Japanese rings(5.3.8.1). A **Nagata scheme** is a scheme that can be covered by open affine spectrum of Nagata rings(5.3.8.1). ⌟

Prop. (6.4.1.35). Being (universally)Japanese or Nagata is a local property, and are stable under taking open subschemes, by(5.3.8.1). ⌟

Prop. (6.4.1.36). Let X be a locally Noetherian scheme, then X is Nagata iff every integral closed subscheme Z of X is Japanese. ⌟

Proof: One direction is clear. If every integral closed subscheme Z of X is Japanese, let $U = \operatorname{Spec} A \subset X$ be an affine open subscheme and $Z = V(\mathfrak{p}) \subset U$, we need to show $A/\mathfrak{p}$ is Japanese. Consider $\overline{Z}$ with the reduced induced structure is an integral closed subscheme of X and Z is an open subscheme of $\overline{Z}$, thus $\overline{Z}$ is Japanese and so is Z by(6.4.1.34). □

2 Normal & Regular

Def. (6.4.2.1) [Normal & Regular Schemes]. A scheme is called **normal** if all its stalks are normal domains(5.3.5.1), or equivalently all its affine sections are normal rings. In particular, a normal scheme is reduced.

A locally Noetherian scheme is called **regular** iff all its stalk are regular local rings(5.3.5.17), i.e. all affine opens are regular rings. Regular only have to be checked at close pt by(5.3.5.17). ⌟

Def. (6.4.2.2). Let X be a locally Noetherian scheme, the points x that $\mathcal{O}_{X,x}$ is a regular local ring is called the **regular locus** of X, and the complement of the regular locus is called the **singular locus** of X. ⌟

Prop. (6.4.2.3) [Noetherian and Integral]. Let X be a locally Noetherian scheme, then X is normal iff it is a disjoint union of integral normal schemes. ⌟

Proof: It suffices to show that a connected locally Noetherian scheme is integral. Thus it suffices to show it is irreducible. Suppose there are several irreducible components, and let p be a intersection point, then we may assume X is affine, then this follows from(5.3.5.4). □

Cor. (6.4.2.4). A normal scheme is integral iff it is connected. ⌟

Prop. (6.4.2.5). If X is an integral normal scheme, then $\Gamma(X, \mathcal{O}_X)$ is a normal ring. ⌟

Proof: If X is integral, then $R = \Gamma(X, \mathcal{O}_X)$ is integral. If $f = a/b \in K(R)$ that is integral over R, then for any affine open $U \subset X$, $b|_U$ is non-zero as X is integral, thus $f|_U$ is integral over $\mathcal{O}_X(U)$ thus $f|_U \in \mathcal{O}_X(U)$, thus $f \in R$. □

Prop. (6.4.2.6) [Normalization]. For an integral scheme X, there is a $X_{nom} \to X$ which is $\mathbf{Spec}(\mathcal{O}_{X,nom})$, any dominant morphism f from a normal integral scheme to X will factor through X_{nom}. (Use the adjointness for **Spec** and notice f maps generic to generic). ⌟

Proof: □

Prop. (6.4.2.7) [Normalizations are Birational]. The normalization of an integral scheme X is a finite birational map. ⌟

Proof: ? □

Prop. (6.4.2.8) [Normalization is not flat]. Non-trivial normalization is never flat. ⌟

Proof: Use(6.6.2.6).? □

Prop. (6.4.2.9) [Regular and Normal]. Regular scheme is C.M and locally factorial, hence normal, by(5.3.5.21) and(5.3.5.19). A Normal scheme is regular in codimension 1, by(5.3.5.32). ⌟

Cor. (6.4.2.10). A regular connected scheme X is irreducible, by(6.4.2.4). ⌟

Prop. (6.4.2.11). For a locally Noetherian scheme of dimension≤ 1, normal is equivalent to regular, by(11.2.3.4). ⌟

Factorial Schemes

Def. (6.4.2.12) [Factorial Schemes]. A **factorial scheme** is a scheme that all the local rings are UFD. ⌟

Prop. (6.4.2.13). If A is a UFD, then $\operatorname{Spec} A$ is factorial. ⌟

Dedekind Scheme

Def. (6.4.2.14) [Dedekind Scheme]. A **Dedekind scheme** is an integral Noetherian normal scheme of dimension 1. ⌟

Prop. (6.4.2.15). Let X be a Dedekind scheme and $x \in X$ is a closed pt, let $\widehat{X} = \operatorname{Spec}(\widehat{\mathcal{O}}_{X,x}) \to X$ be the completion of X at x, then there is a pullback of categories:

$$\begin{array}{ccc} \mathrm{Bun}_X & \longrightarrow & \mathrm{Bun}_{X\setminus\{x\}} \\ \downarrow & & \downarrow \\ \mathrm{Bun}_{\widehat{X}} & \longrightarrow & \mathrm{Bun}_{\widehat{X}\setminus\{x\}} \end{array}$$

⌟

Proof: We may study locally near x, then we can assume that X is affine. Now shrink X even more, we can assume that x is defined by a single $f \in A$(localized at the maximal ideal defined by x), then we finish by(5.4.2.12). □

3 Geometrical properties

Def. (6.4.3.1) [Geometric Properties over Fields].

- A scheme X is called **geometrically integral/reduced/separated/irreducible**... over a field k iff for any field extension k'/k, $X_{k'}$ is integral/reduced/separated/....
- A locally Noetherian scheme is called **geometrically regular** iff for any f.g. field extension K/k, X_K is regular. It is stalkwise by(6.4.3.18).

⌟

Geo.reducedness

Prop. (6.4.3.2) [Geo.Reduced]. For a scheme X over a field k, the following are equivalent:

1. X is geometrically reduced.
2. For every reduced k-scheme Y, the product $X \otimes_k Y$ is reduced.
3. All stalks are geometrically reduced ring.
4. X is reduced and for every maximal point η of X, the residue field $k(\eta)$ is separable over k.
5. $X_{k^{per}}$ is reduced.
6. X_K is reduced for every finite purely inseparable field extension K/k.
7. $X_{k^{1/p}}$ is reduced.

In particular, if k has characteristic 0, then geo.reduced $\iff$ reduced. ⌟

Proof: As reduced is local, these all follows from(5.3.6.2). □

Prop. (6.4.3.3) [Geo.Reduced and Arithmetic Points]. Let X be a locally algebraic geo.reduced scheme over a field k, then the set of closed points with finite separable field extensions $k(x)/k$ is dense in X. ⌟

Proof: Combine(6.6.4.19) and(6.6.4.21). □

Def. (6.4.3.4) [Density of Points]. Let X be an algebraic scheme over a field k and k'/k be a field extension, then a subset $S \subset X(k')$ is said to be **schematically dense** in X if the only closed subscheme $Z \subset X$ over k that $S \subset Z(k')$ is X itself.

? Should merge with the definition of scheme-theoretical image. ⌟

Prop. (6.4.3.5) [Schematically Dense Subset]. Let X be an algebraic scheme over a field k, $S \subset X(k)$ be a subset. Then the following are equivalent:

1. S is schematically dense in X.
2. X is reduced and S is dense in $|X|$.
3. The family of homomorphisms $\mathcal{O}_X \to k : f \mapsto f(s)$ is jointly injective.

⌟

Proof: $1 \to 2$: Let $\overline{S}$ be the induced reduced structure of the closure S in X(6.4.1.14), then $\overline{S} = X$, so X is reduced with $X = \overline{S}$.

$2 \to 3$: ? Cf.[Milne Algebraic Groups, P10]. □

Cor. (6.4.3.6). A schematically dense subset remains schematically dense after field base changes. ⌟

Cor. (6.4.3.7). The schematic closure of a subset commutes with base change. ⌟

Proof: Use the third definition in(6.4.3.5), notice that the valuation maps are also jointly injective because k'/k is flat. □

Cor. (6.4.3.8). If X admits a schematically dense subset S, then X is geo.reduced. ⌟

Prop. (6.4.3.9). If $X(k')$ is dense in X, then X is reduced. Conversely, if $X(k')$ is dense in $|X_{k'}|$ and X is geo.reduced, then $X(k')$ is dense in X. ⌟

Proof: X is reduced because $X_{\text{red}}(k') = X(k')$. Conversely if $Z \subset X$ is a closed subscheme that $Z(k') = X(k')$, then $|Z_{k'}| = |X_{k'}|$ by condition, and then $Z_{k'} = X_{k'}$ as $X_{k'}$ is reduced. Thus $Z = X$ by flatness. □

Cor. (6.4.3.10)[Geometric Points Schematically Dense]. If X is locally algebraic and geo.reduced, then $X(k')$ is schematically dense in X for any separably closed field k' containing k. ⌟

Proof: $X(k')$ is dense in $|X_{k'}|$ by(6.4.3.3), thus it is schematically dense in X by the proposition. □

Cor. (6.4.3.11). If Z, Z' are closed subvarieties of a locally algebraic algebraic scheme X over k that $Z(k') = Z'(k') \subset X(k')$ for some separably closed field k' containing k, then $Z = Z'$. In other words, a closed subvariety of X is determined by the subset $Z(k^s) \subset X(k^s)$. ⌟

Proof: The closed subscheme $Z \cap Z'$ satisfies $Z \cap Z'(k') = Z(k')$, so $Z \cap Z' = Z$ by(6.4.3.10). Similarly $Z \cap Z' = Z'$. □

Geo.Connected and Geo.Irreducible

Prop. (6.4.3.12) [Geo.Connectedness]. For a scheme X over a field k, the following are equivalent:

- For every connected k-scheme Y, the product $X \otimes_k Y$ is connected.
- X is geometrically connected.
- X_{K^s} is connected.
- X_K is connected for any finite separable extension K/k.

⌟

Proof: Cf. [Sta]0385, 0389.**?** □

Prop. (6.4.3.13) [Invariance of Base Change]. Let X be a scheme over a field k and k'/k a field extension, then X is geo.connected iff $X_{k'}$ is geo.connected. ⌟

Proof: Cf.[Sta]054N. □

Prop. (6.4.3.14). Let $T \to X$ be a map of schemes over a field k, if T is geo.connected and X is connected, then X is geo.connected. ⌟

Proof: Cf.[Sta]056R. □

Cor. (6.4.3.15) [Connected with a Rational Point]. Let X be a scheme over a field k. Assume X is connected and has a point x that k is alg.closed in $k(x)$, then X is geo.connected. In particular, if X is connected and has a rational point, then X is geo.connected. ⌟

Proof: Cf.[Sta]04KV. □

Prop. (6.4.3.16) [Geometrically Irreducible]. For a scheme X over a field k, the following are equivalent:

- For every irreducible k-scheme Y, the product $X \otimes_k Y$ is irreducible.
- X is geometrically irreducible.
- X_{k^s} is irreducible.
- X is irreducible and if η is the generic pt of X, then k is separably closed in $k(\eta)$.
- X_K is irreducible for any finite separable extension K/k.

⌟

Proof: Cf.[Gortz P136].? □

Geo.Integral

Cor. (6.4.3.17)[geometrically Integral]. For a scheme X over a field k, the following are equivalent:

- For every integral k-scheme Y, the product $X \otimes_k Y$ is integral.
- X is geometrically integral.
- X_K is irreducible for any finite extension K/k.
- $X_{\overline{k}}$ is integral.
- X is integral and if η is the generic pt of X, then k is alg.closed in $k(\eta)$ and $k(\eta)/k$ is separable.

⌟

Proof: $1 \to 2 \to 3 \to 4$ is easy, Cf.[Gortz P136].? □

Geometrically Regular

Prop. (6.4.3.18). Let X be a locally Noetherian scheme over a field k, then X is geometrically regular iff the local ring $\mathcal{O}_{X,x}$ is geometrically regular over k. Thus it suffice to check for finite purely inseparable field extensions k'/k, by(5.3.6.6). ⌟

Proof: For a finite purely inseparable field extension, $\mathcal{O}_{X,x} \otimes_k k'$ is also a local ring because their spectra are the same(5.1.7.26), so $\mathcal{O}_{X,x}$ is geometrically regular by(5.3.6.6).

Conversely, if $\mathcal{O}_{X,x}$ is geo.regular, then for any field extension k'/k, stalks of $X_{k'}$ are localization of $\mathcal{O}_{X,x} \otimes_k k'$, so it is regular by(5.3.5.17). □

Cor. (6.4.3.19). A geometrically regular ring is geometrically reduced, by(5.3.5.19) and(6.4.3.2). ⌟

Prop. (6.4.3.20)[Partially Invariance Under Base Change]. If k'/k is a f.g. field extension, then $X_{k'}$ is geo.regular over k' iff X_k is geo.regular over k.

In fact, this is true for any field extension k'/k if X is locally algebraic over k, because in this case geo.regular is equivalent to smoothness. ⌟

Proof: One direction is trivial, for the other, Cf.[Sta]038W?. □

4 Basic Morphism Properties

Main references are [Sta]02WE.

Base Change Trick

Prop. (6.4.4.1) [Base Change Trick]. If a property P of morphisms satisfy:

- Closed immersion has P.
- Stable under base change and composition.

Then

- it is stable under product.
- $g \circ f : X \to Y \to Z$ has P and g separated implies f has P.
- it is stable under f_{red}. (Notice $X_{\text{red}} \to X$ is closed immersion).

⌟

Proof: For the product, we may assume one of them is identity and use composition, but then the product is just base change, so it has P.

For the second, factorize $f : X \to X \times_Z Y \to Y$, the first is base change of $\Delta : Y \to Y \times_Z Y$, so it satisfies P because g is separable, and the second map is a base change of $X \to Z$, so it satisfies P, so f satisfies P.

$X_{\text{red}} \to X \to Y = X_{\text{red}} \to Y_{\text{red}} \to Y$ has P because $X_{\text{red}} \to X$ is closed immersion, and $Y_{\text{red}} \to Y$ is separable because closed immersion is separable(checked directly), so by what has been proved, $X_{\text{red}} \to Y_{\text{red}}$ has P. □

Prop. (6.4.4.2). Lists of properties satisfying the base change trick(6.4.4.1)(not complete):

1. Universal closed/universal injective morphisms.
2. Affineness.
3. Morphisms (locally)of finite type.
4. Finite Morphisms.
5. Integral Morphisms.
6. Morphisms (locally)of finite presentation.
7. Quasi-affine morphisms.
8. Closed Immersions.
9. Quasi-compactness.
10. (Quasi-)Separatedness.
11. Proper.
12. Unramified.
13. Monomorphisms.
14. (Locally) Quasi-finiteness.
15. H-projectiveness.

⌟

Proof:

1. Trivial.
2. Because affineness is local on the target(6.4.1.5), this follows from(6.2.7.17) and(6.2.7.14).

3. Trivial.
4. Trivial.
5.
6. By(5.3.7.9).
7. Affine morphism is quasi-compact: because quasi-compactness is local on the target, we can reduced to the affine case, thus it is quasi-compact, by(6.4.4.26). To show a base change of quasi-compact morphism is quasi-compact, because quasi-compactness is local on the target(6.4.1.5), then we can choose a cover by affine opens that the image is contained in an affine open, thus it reduces to show a map between affine schemes is quasi-compact, which is(6.4.4.26).
8. For closed immersions, use(6.2.7.16) and check locally, for open immersions, use(6.2.7.16).
9. It suffices to show an affine map is quasi-compact.
10. Closed immersion is separated is checked directly. Composition: For $X \to Y \to Z$, the diagonal map decomposes as $X \to X \times_Y X \to X \times_Z X$, the second one is closed immersion(or quasi-compact) by(6.4.4.78), so this follows from that of closed immersion and qc. Base change: The diagonal commutes with base change(4.1.1.48), so this follows from that of closed immersion and qc.
11. Because universally closed, f.t. and separatedness both do(6.4.4.2).
12.
13.
14.

□

Injectivity and Monomorphisms

Def. (6.4.4.3) [Injectivity and Monomorphisms]. A morphism of schemes is called **injective** if it is injective topologically. A morphism of schemes is called a monomorphism if it is a monomorphism in the category of schemes. ⌟

Prop. (6.4.4.4) [Universally Injective]. For a morphism of schemes $X \to S$, the following are equivalent:

- It is universally injective.
- It is injective and the residue field extension are all purely inseparable.
- The diagonal map is surjective.
- For any field K, $\mathrm{Hom}(\mathrm{Spec}\, K, X) \to \mathrm{Hom}(\mathrm{Spec}\, K, S)$ is injective.

In particular, any monomorphism is universally injective. ⌟

Proof: $1 \to 4$: For $s \in \mathrm{Hom}(\mathrm{Spec}\, K, S)$, a $x \in \mathrm{Hom}(\mathrm{Spec}\, K, X)$ mapping to s is a section of the injective map $X \times_S \mathrm{Spec}\, K \to \mathrm{Spec}\, K$, which is unique if it exists.

$4 \to 1$: If $S' \to S$ is a morphism, $X' = X \times_S S'$, and $x, x' \in X'$ map to the same point $s' \in S'$, then we can choose a common field extension $K/k(s')$ of $k(x)/k(s)$ and $k(x')/k(s)$. Then we get two elements in $\mathrm{Hom}(\mathrm{Spec}\, K, X')$, and the hypothesis says they map to the same element in $\mathrm{Hom}(\mathrm{Spec}\, K, X)$. Thus they are the same, as X' is the fiber product.

$1 \to 2$: It the residue field extension is not purely inseparable, then tensoring with this field extension, we get two points mapping to the same, contradiction.

$2 \to 4$: It the residue field extension is purely inseparable, then $k(x) \to K$ is determined by the composition, $k(s) \to k(x) \to K$, which means 4 is true.

$1 \to 3$: If $X \to S$ is universally injective, then $X \times_S X \to X$ is injective, and $\Delta_{X/S}$ is a section of this map, thus it must be surjective.

$3 \to 1$: If $\Delta_{X/S}$ is surjective, then for any base change $S' \to S$, $\Delta_{X'/S'}$ is surjective, thus $X' \to S'$ is injective, thus 1 holds. □

Prop. (6.4.4.5)[Monomorphism and Injectivity]. A morphism of schemes $j : X \to Y$ is a monomorphism if j is an injective map and for any $x \in X$, $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is surjective. ⌟

Proof: First check topologically, then check the local ring map. □

Cor. (6.4.4.6). For any scheme X and a point x, $\operatorname{Spec} \mathcal{O}_{X,x} \to X$ is a monomorphism. ⌟

Closed Map

Prop. (6.4.4.7) [Universal Closed]. Universal closedness is local on the basis and satisfies the base change trick(6.4.4.2). ⌟

Prop. (6.4.4.8). If g is surjective, then $f \circ g$ is universally closed iff f is universally closed (because surjective is S.u.B). ⌟

Prop. (6.4.4.9)[Closed Map and Specialization]. The image of a quasi-compact morphism is closed iff it is stable under specialization. And it is a closed map iff specializations lift along f. ⌟

Proof: For the first, the question is local, so reduce to Y affine, and then X is qc$= \cup U_i$, then we can replace X by an affine $\coprod U_i$, then reduce to the affine case(5.1.7.14).

For the second, for any closed subset of X with its induced reduced structure, the restriction to it is still qc and specialization lifts, so we prove the image is closed. Now the image is stable under specialization, so the result follows from the first assertion. □

Affine Map

Prop. (6.4.4.10). X is affine if there is a finite set of elements $f_i \in \Gamma(X, \mathcal{O}_X)$ that generate the unit ideal and X_{f_i} is affine. ⌟

Proof: First prove that $X_{f_i} \cap X_{f_j} = X_{f_i f_j}$ is affine because affine intersect X_{f_i} is affine. Second, prove $\Gamma(X_f, \mathcal{O}_X) = \Gamma(X, \mathcal{O}_X)_f$, finally glue them to get a map $X \to \operatorname{Spec}(A)$ and use the fact isomorphism is local on the target(6.4.1.5). X is affine scheme if $X \to \operatorname{Spec}(\Gamma(X))$ is affine. □

Cor. (6.4.4.11). Affineness is affine local on the target, and it satisfies the base change trick(6.4.4.2).
⌟

Lemma (6.4.4.12) [Serre Criterion of Affineness].

- A qc scheme X is isomorphic to an affine scheme iff $H^1(X, \mathcal{I}) = 0$ for every Qco sheaf of ideals $\mathcal{I}$.
- If X is qcqs, then it suffices to show $H^1(X, \mathcal{I}) = 0$ for every Qco sheaf of ideals $\mathcal{I}$ of f.t..
- If $f : X \to Y$ is a quasi-compact morphism between quasi-separated schemes, then f is affine iff for any Qco sheaf of ideals $\mathcal{I}$ on X, $R^1 f_* \mathcal{I} = 0$.

⌟

Proof: ? Cf.[Sta]01XF.

The case of affine scheme is proven by(6.7.1.1) and(6.7.1.2). The converse: For every point p, choose an open affine nbhd U, let $Y = X - U$, by the exact sequence

$$0 \to \mathcal{I}_{Y\cup\{p\}} \to \mathcal{I}_Y \to k(P) \to 0,$$

we have a surjective map $\Gamma(X, \mathcal{I}_Y) \to \Gamma(X, k(P))$ thus there is a $f \in A = \Gamma(X, \mathcal{O}_X)$ that $P \in X_f \subset U$ is affine. So using(6.4.4.10), we only have to show that for f.m f_i, they generate $\Gamma(X, \mathcal{O}_X)$. This is by considering the kernel F of $\mathcal{O}_X^r \to \mathcal{O}_X : (a_1, \ldots, a_r) \to \sum f_i a_i$, and there is a filtration on F, the quotient of which are all coherent sheaves because kernel and cokernel are Qco, and there by induction and hypothesis, $H^1(X, F) = 0$, thus the result.

2: In the qcqs case, by(6.7.1.6), we can use filtered colimit to show that $H^1(X, \mathcal{I}) = 0$ for any Qco sheaf of ideals.

3: For any affine open U of Y, the inclusion $U \to Y$ is qc, thus $f^{-1}(U) \to X$ is also qc. Now any Qco sheaf of ideals $\mathcal{I}$ on U extends to a Qco sheaf of ideals on X by(6.5.1.8), then we can use Leray spectral sequence to conclude that $H^1(f^{-1}(U), \mathcal{I}) = 0$, so $f^{-1}(U)$ is affine. □

Cor. (6.4.4.13). For a Noetherian scheme X, X is affine iff X_{red} is affine. ⌟

Proof: The canonical exact sequence(6.2.6.10) reads: $0 \to \mathcal{N}\mathcal{F} \to \mathcal{F} \to i_* i^* \mathcal{F} \to 0$, so iff X_{red} is affine, then we have $H^i(\mathcal{F}) \cong H^i(\mathcal{N}\mathcal{F})$, and notice $\mathcal{N}^k = 0$ for some k. □

Cor. (6.4.4.14). For a Noetherian reduced scheme X, X is affine iff each irreducible component is affine. (The same as the above, notice that $\prod p_i = 0$, for the minimal primes of A). (The reducedness can be dropped by the last proposition). ⌟

Lemma (6.4.4.15). If a morphism $X \to Y$ is a homeomorphism onto a closed subset of Y, then f is affine. ⌟

Proof: Cf.[[Sta]04DE]. □

Quasi-affine

Def. (6.4.4.16) [Quasi-Affine Morphism]. A scheme is called **quasi-affine** iff it is isomorphic to a qc open subscheme of an affine scheme. A morphism is called **quasi-affine** iff the inverse of any affine scheme is quasi-affine. ⌟

Prop. (6.4.4.17). Quasi-affine is local on the target and satisfies the base change trick. ⌟

Proof: Cf.[Sta]01SN. □

Prop. (6.4.4.18). Any qc immersion i of a quasi-affine scheme is quasi-affine. ⌟

Proof: As i is qc, i factors through a map $Z \to U \to X$, where U is a quasi-compact open subset of X. Thus it suffices to consider the closed immersion case, which is clear. □

Prop. (6.4.4.19). A morphism $f : X \to S$ is quasi-affine iff $\mathcal{O}_X$ is f-ample. In particular, A scheme is quasi-affine iff $\mathcal{O}_X$ is ample. ⌟

Proof: Cf.[Sta]01QE. □

Cor. (6.4.4.20). Let X be a quasi-affine scheme and $H^p(X, \mathcal{O}_X) = 0$ for $p > 0$, then X is affine. ⌟

Proof: By(6.4.4.19) $\mathcal{O}_X$ is ample, then by(6.5.4.20), X is affine. □

Prop. (6.4.4.21) [Descent]. Let X be a scheme over a field k and K/k be a field extension, then X is quasi-affine iff X_K is quasi-affine. ⌟

Proof: Cf.[Sta]0BDD. □

Dominant

Prop. (6.4.4.22). Let $f : X \to S$ be a map of schemes.

- If every generic point of irreducible components of S is in the image of f, then f is dominant.
- If f is quasi-compact, then the converse is also true. More precisely, if a generic point η is not in the image, then it is not in the closure of the image.
- If X has only f.m. irreducible component, then the converse is also true.

⌟

Proof: Cf.[Sta]Chap28.8. □

Prop. (6.4.4.23) [Dominant Map between Integral Schemes]. If $f : X \to S$ is a map between integral schemes, then the following are equivalent:

- f is dominant.
- $f(\eta_X) = \eta_Y$.
- for some(all) affine open subset $U \subset X, V \subset Y$ with $f(U) \subset V$, the ring map $\mathcal{O}_Y(V) \to \mathcal{O}_X(U)$ is injective.
- for some(all) $x \in X$, the local ring map $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is injective.

⌟

Proof: Cf.[Sta]0CC1. □

Def. (6.4.4.24) [Dominant Rational Maps]. A rational map between irreducible schemes is called a **dominant map** if it maps the generic point to the generic point. ⌟

Quasi-Compact

Prop. (6.4.4.25) [Quasi-Compact Morphism]. A morphism $f : X \to S$ of schemes is quasi-compact iff the inverse image of any quasi-compact open subsets is quasi-compact, because affine opens form a basis of X.

Quasi-compactness is local on the target and satisfies the base change trick(6.4.4.2). ⌟

Prop. (6.4.4.26). A map between affine schemes is quasi-compact. ⌟

Proof: Because quasi-compactness is local on the target(6.4.1.5), it suffices to show the inverse image of a distinguished open subset is quasi-compact, and this is true. □

Prop. (6.4.4.27). Let $f : X \to Y$, $g : Y \to Z$. If $g \circ f$ is quasi-compact and g is qs, then f is qc. ⌟

Proof: Factor it through $X \to X \times_Z Y \to Y$. The second map is a base change of $X \to Z$ hence qc, the first map is a section of $X \times_Z Y \to X$, which is a base change of $Y \to Z$, hence qs, so by(17.5.3.19), the first map is also qc. □

Prop. (6.4.4.28). Any map between Noetherian schemes is quasi-compact, by(6.4.1.22). ⌟

Finite Type

Def. (6.4.4.29) [Morphisms of Finite Type]. A morphism $f : X \to S$ is called of **locally of finite type** if for there exists an affine open cover $\{\mathrm{Spec}(B_i)\}$ of S that $f^{-1}(U_i)$ has an affine open cover of spec of finite generated B_i-algebras. It is called **finite type** if moreover it is quasi-compact.

Let $k \in \mathtt{Field}$, then $S \in \mathcal{S}\mathrm{ch}/k$ is called **(locally)algebraic** iff S is (locally)of finite type over $\mathrm{Spec}\, k$.

For $S \in \mathcal{S}\mathrm{ch}$, denote $\mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S(\mathcal{S}\mathrm{ch}^{\mathrm{ft}}/S)$ the full subcategory of $\mathcal{S}\mathrm{ch}/S$ consisting of (locally) of finite type schemes over S.

(Locally)Finite type is affine local on the target and on the source, and satisfies the base change trick(6.4.4.2). ⌟

Prop. (6.4.4.30) [Closed Subschemes Descending Chain Stablizes]. The closed subschemes of an algebraic scheme X over a field k satisfy the descending chain condition. ⌟

Proof: As X is Noetherian, the topological chain $|Z_1| \supset |Z_2| \supset \ldots$ stablizes, so we may assume $|X| = |Z_1| = |Z_2| = \ldots$. Now choose a finite affine cover $\mathrm{Spec}\, A_i$ of X, then Z_i corresponds to ideals I_i of A_i, so they stablizes, as A_i are Noetherian. □

Cor. (6.4.4.31). Arbitrary intersection of closed subschemes of an algebraic scheme X is well-defined. ⌟

Prop. (6.4.4.32) [Algebraic Schemes of Dimension 0]. Let X be a locally algebraic variety over a field k of dimension 0, then X is a disjoint union of f.d. local Artinian k-algebras. ⌟

Proof: Cf.[Sta]06LH.**?** □

Prop. (6.4.4.33) [Dimensions for Locally Algebraic k-Schemes]. Let k be a field and X is a locally algebraic k-scheme.

if X is irreducible, then $\dim X = \dim U$ for any nonempty open $U \subset X$. ⌟

Proof: It suffices to show any two affine open subsets U, U' of X have the same dimension, then use(4.12.3.26). Now $U \cap U' \neq \varnothing$ as X is irreducible, and then it contains a maximal pt x by Hilbert's Nullstellensatz, and then $\dim U = \dim(\mathcal{O}_{X,x}) = \dim U'$ because f.g. algebras over a field is catenary. □

Integral & Finite Map

Def. (6.4.4.34) [Finite and Integral Map]. A morphism $f : X \to S$ is called **integral** if it is affine and there is a affine open covering $U_i = \mathrm{Spec}\, A_i$ of S that $f^{-1}(U_i) = \mathrm{Spec}\, B_i$ and $A_i \to B_i$ is integral.

Integral is affine local on the target and satisfies the base change trick(6.4.4.2).

A morphism $f : X \to S$ is called **finite** if it is affine and there is a affine open covering $U_i = \mathrm{Spec}\, A_i$ of S that $f^{-1}(U_i) = \mathrm{Spec}\, B_i$ and B_i are finite modules over A_i.

Finiteness is affine local on the target and satisfies the base change trick(6.4.4.2).

A morphism $f : X \to S$ is called **(locally) quasi-finite** if it is (locally)of f.t. and the inverse of a point is a discrete set. ⌟

Prop. (6.4.4.35) [Integral Morphism is Closed]. Specialization lifts along an integral morphism. In particular, an integral morphism is closed, by(6.4.4.9). ⌟

Proof: If $f(x) = y, y \to y'$, then we can choose an open affine U containing y', which also contains y. So we can choose an open affine containing x mapping into U, then it reduces to the affine case(5.1.7.13). □

Prop. (6.4.4.36) [Chevalley]. If $f : Y \to X$ is integral surjective, Y is affine, then X is affine. ⌟

Proof: Cf.[Sta]05YU. □

Lemma (6.4.4.37). If $f : Y \to X$ is finite surjective, Y is affine, then X is affine. ⌟

Proof:

□

Prop. (6.4.4.38) [Finite and Integral]. A morphism is finite iff it is integral of f.t.. ⌟

Prop. (6.4.4.39) [Integral and Affine u.c.]. Integral map is equivalent to u.c. and affine. ⌟

Proof: Integral is stable under base change. And if it is integral, then it is closed by(5.2.1.5).

Conversely, we need to prove if $\operatorname{Spec} B \to \operatorname{Spec} A$ is u.c., then $A \to B$ is integral. For any $a \in B$, let J be the kernel of $A[X] \to B[X]/(aX - 1)$, then if $f \in J$, then $f(X) = (aX - 1)q(X)$, and $X^{deg(f)} f(\frac{1}{X}) = (a - X)X^{\deg(q)} q(\frac{1}{X})$ vanishes at a, so it suffices to find a $f \in J$ with constant term 1. It suffices to show that $\operatorname{Spec}(A[X]/J + (x))$ is empty:

As f is universally closed, $\operatorname{Spec} B[X] \to \operatorname{Spec} A[X]$ is closed, thus the image of $\operatorname{Spec}(B[X]/(aX - 1))$ is closed in $\operatorname{Spec} A$, which is the underlying set of $\operatorname{Spec} A/J$, by(6.4.4.64). Now notice $T = \operatorname{Spec}(A[X]/J + (x)) \times_{\operatorname{Spec}(A[X]/J)} \operatorname{Spec}(B[X]/(aX - 1))$ is empty, because $(A[X]/J + (x)) \otimes_{A[X]/J} (B[X]/(aX - 1)) = \operatorname{Spec} A \otimes_{\operatorname{Spec} A[X]} \operatorname{Spec}(B[X]/(aX - 1)) = 0$, as X is invertible in $B[X]/(aX - 1)$ but vanish in A. But $T \to \operatorname{Spec}(A[X]/J + (x))$ is surjective, as a base change of $\operatorname{Spec}(B[X]/(aX - 1)) \to \operatorname{Spec} A/J$, thus we are done. □

Def. (6.4.4.40)[Degree of Finite Morphisms at a Point]. Suppose $\pi : X \to Y$ is a finite morphism, then $\pi_* \mathcal{O}_X$ is a $\mathcal{O}_Y$-module of f.t.. Let $p \in Y$, then the **degree of** π **at** p is the rank of this sheaf on Y(6.5.1.11), which is an upper-semicontinuous function(6.5.1.41). ⌟

Prop. (6.4.4.41). The degree of a finite morphism $\pi : X \to Y$ at p is the dimension over $k(p)$ of the fiber of π at p. In particular, the degree is zero iff $\pi^{-1}(p) = 0$. ⌟

Proof: Look affine locally. □

Lemma (6.4.4.42). For $f : Y \to X$ finite surjective and X locally Noetherian, for every integral subscheme Z of X with generic point ξ, there is a coherent sheaf $\mathcal{F}$ on Y that the support of $f_* \mathcal{F}$ is Z and $(f_* Z)_\xi$ is annihilated by $\mathfrak{m}_\xi$. ⌟

Proof: W consider an inverse image of $\xi = \xi'$, and let $Z' = \overline{\{\xi'\}}$ with the induced reduced structure, then let $\mathcal{F} = i_* \mathcal{O}_{Z'}$ on Y, $\mathcal{F}$ is coherent, then we need to show that $(f_* \mathcal{F})_\xi$ is annihilated by m_ξ. This is because it factors through Z.**?** Cf.[Sta]01YO. □

Quasi-Finiteness

Def. (6.4.4.43) [Quasi-Finite Morphisms]. **?**

(Locally)Quasi-finite morphisms are local on the target and satisfies base change trick. ⌟

Prop. (6.4.4.44) [Characterization of Quasi-Finiteness]. Let $f : X \to S$ be a morphism, then the following are equivalent:

- f is quasi-finite.
- f is locally quasi-finite and quasi-compact.
- f is locally of f.t., quasi-finite and has finite fibres.

⌟

Proof: Cf.[Sta]01TJ, 02NH. □

Prop. (6.4.4.45). Immersions are locally quasi-finite. ⌟

Prop. (6.4.4.46). Let $f : X \to S$ be a morphism of schemes and $s \in S$. Assume that f is locally of f.t. and $f^{-1}(s)$ is a finite set, then X_s is a finite discrete topological space, and f is quasi-finite at every point of $f^{-1}(s)$. ⌟

Proof: Cf.[Sta]02NG. □

Prop. (6.4.4.47) [Zariski's Main Theorem]. Let $f : Y \to X$ be an affine morphism of f.t.. Let $Y \xrightarrow{f'} X' \xrightarrow{\nu} X$ where X' is the normalization of X in Y, then there exists an open subscheme $U' \subset X'$ that $(f')^{-1}(U) \to U$ is an isomorphism and $(f')^{-1}(U)$ is the set of points at which f is quasi-finite. ⌟

Proof: Cf.[Sta]03GT. □

Prop. (6.4.4.48) [Quasi-Finite Locus is Open]. Let $f : X \to S$ be a morphism of schemes, then the set of points of X that f is quasi-finite is an open subset $U \subset X$, and $U \to S$ is locally quasi-finite. ⌟

Proof: Cf.[Sta]01T1. □

Prop. (6.4.4.49) [Zariski's Main Theorem]. For a morphism $X \to S$ that is quasi-finite and separated, if S is qcqs, Then there is a factorization $X \to T \to S$ that $X \to T$ is a qc open immersion and $T \to S$ is finite. ⌟

Proof: Cf.[Sta]05K0. □

Prop. (6.4.4.50). If $f : Y \to X$ is a quasi-finite morphism of schemes, and $T \subset Y$ is nowhere dense, then $f(T) \subset X$ is also nowhere dense. ⌟

Proof: Cf.[Sta]03J2. □

Generically Finiteness

Def. (6.4.4.51) [Generically Finite Morphisms]. A **generically finite morphism** is a morphism $f : X \to Y$ locally of f.t. and there exists a dense open subset $U \subset X$ s.t. $U \to Y$ is locally quasi-finite. ⌟

Lemma (6.4.4.52). Let $R \to S$ be a ring map of f.t., if $\mathfrak{p} \subset R$ is a minimal prime that there are f.m. primes in S lying over $\mathfrak{p}$, then there is a $g \in R$, $g \notin \mathfrak{p}$ that $R_g \to S_g$ is finite. ⌟

Proof: The condition means $S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}$ has only f.m. primes and $\mathfrak{p}S_\mathfrak{p}$ is locally nilpotent. Then $\kappa(\mathfrak{p}) \to S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}$ if finite. Let x_i generate S over R, then there are polynomials $P_i \in R[X]$ that $P_i(x_i) = 0 \in S_\mathfrak{p}/\mathfrak{p}S_\mathfrak{p}$, and thus $P_i^{e_i}(x_i) = 0 \in S_\mathfrak{p}$. Now choose $g \notin \mathfrak{p}$ that g divides the common divisors of the coefficients of P_i and $P_i(x_i) = 0 \in S_g$, then $R_g \to S_g$ is finite. □

Prop. (6.4.4.53) [Generically Finiteness]. Let $f : X \to Y$ be a morphism of finite type. If $\eta \in Y$ is a generic point, then:

- $f^{-1}(\eta)$ is a finite set iff there are affine opens $U_i \subset X, i = 1, \ldots, n$ and $V \subset Y$ that $f(U_i) \subset V, \eta \in V$ and $f^{-1}(\eta) \subset \cup U_i$ and $U_i \to V$ are finite.
- If f is qs, then we can further restrict to $n = 1$.
- If f is qcqs, then we can further restrict to $U_1 = f^{-1}(V)$.

⌟

Proof: These are local on Y, so we can change Y to an affine open subscheme containing η.

1: If these affine opens exist, then $\#f^{-1}(\eta) < \infty$ because finite maps are quasi-finite(6.4.5.5).

If $f^{-1}(\eta) = \{\xi_1, \ldots, \xi_n\}$, choose affine opens U_i around each ξ_i, then we reduce to the affine case(6.4.4.52).

2: Cf.[Sta]02NW.

3: □

Prop. (6.4.4.54) [Extension of Fraction Fields]. Let $f : X \to Y$ be a dominant morphism locally of f.t. between integral schemes, then the following are equivalent:

- tr.deg $K(X)/K(Y) = 0$.
- $K(X)/K(Y)$ is finite.
- there exists non-empty affine opens $U \subset X, V \subset Y$ s.t. $f(U) \subset V$ and $U \to V$ is finite.
- the generic point of X is the only point mapping to the generic point of Y.
- If f is qc or qs, we can assume $U = f^{-1}(V)$.

⌟

Proof: Cf.[Sta]02NX. □

Def. (6.4.4.55) [Degree Generically Finite Morphisms]. Let $f : X \to Y$ be a dominant morphism of f.t. between integral schemes, then by(6.4.4.23), f induces an injective map of function fields $K(Y) \to K(X)$, the degree of $[K(X) : K(Y)]$ is called the **degree of** f, denoted by $\deg(f)$. It is a positive integer or ∞.

When $\deg(f)$ is finite(i.e. the conditions of(6.4.4.54) hold), it is called a **separable/purely inseparable morphism** if the field extension $K(X)/K(Y)$ is separable/purely inseparable. And also we can define the separable, inseparable degree of f. ⌟

Immersions

Def. (6.4.4.56) [Immersions]. A **closed immersion** of schemes is a closed immersion of local ringed spaces(6.2.6.15). A **closed subscheme** of a scheme X is a closed sub-ringed space(6.2.6.15) that is also a scheme.

An **open immersion** of schemes is an open immersion of local ringed spaces(6.2.6.15). An **open subscheme** of a scheme X is an open subspace(6.2.6.15) that is also a scheme.

Open and closed immersions are affine local on the target(6.4.1.5).

An **immersion** is a morphism that is a closed immersion of an open immersion. ⌟

Lemma (6.4.4.57) [Closed Immersion for Schemes]. Let $f : Y \to X$ be a morphism of schemes that induces a homeomorphism of Y onto a closed subset of X, and $f^\sharp : \mathcal{O}_X \to f_*\mathcal{O}_Y$ is surjective, then it is a closed immersion(6.2.6.15). ⌟

Proof: It suffices to show that the kernel of $f^\sharp$ is Qco. For this, notice that f is quasi-compact, and it is a monomorphism by(6.4.4.5), in particular separated by(6.4.4.86). Then(6.5.1.6) shows $f_*\mathcal{O}_Y$ is Qco. Then the kernel is Qco by(6.5.1.3). □

Prop. (6.4.4.58) [Closed Subschemes of Affine Schemes]. The closed sub-ringed spaces of $X = \operatorname{Spec} A$ are all closed subschemes, and they corresponds to ideals $I \subset A$:

- If $I \subset A$ is an ideal, then the morphism $Z = \operatorname{Spec} A/I \to \operatorname{Spec} A$ is a homeomorphism of Z onto a closed subspace $V(I)$ of X, and also the stalk map at a point $\mathfrak{p} \subset Z$ is $R_\mathfrak{p} \to (R/I)_{\mathfrak{p}/I} = R_\mathfrak{p}/IR_\mathfrak{p}$, which is surjective. So this is a closed immersion by(6.4.4.57).
- By(6.2.6.17), for any closed subscheme Z of X with sheaf of ideals $\mathcal{I}$, Z is isomorphic to the closed subscheme of X defined by $\mathcal{I}$. Now $\mathcal{I}$ is locally generated by sections, so the quotient sheaf $\mathcal{O}_X/\mathcal{I}$ is a Qco sheaf, so it is of the form $\widetilde{S}$ for some A-module S, by(6.5.1.2). Then $\mathcal{I}$, as the kernel of $\mathcal{O}_X \to \widetilde{S}$, is also Qco(6.5.1.3), so it equals $\widetilde{I}$ for some ideal $I \subset A$. Thus $S = R/I$, and we are done.

⌟

Prop. (6.4.4.59) [Closed Subscheme of Schemes]. The closed sub-ringed spaces of a scheme X are all closed subschemes, and they corresponds to Qco $\mathcal{O}_X$-sheaves of ideals via the ideal sheaf(6.2.6.15): ⌟

Proof: Let $i : Y \to X$ be a closed immersion, for any $x \in X$, choose an open affine nbhd U of $x \in X$, then $i : i^{-1}(U) \to U$ is also a closed immersion, so it corresponds to $\operatorname{Spec} A/I \to \operatorname{Spec} A$ for some ideal I by(6.4.4.58). So Z is a scheme, and the ideal sheaf $\mathcal{I}$ is Qco. □

Prop. (6.4.4.60). Closed immersion satisfies the base change trick(6.4.4.2). Open immersion are stable under base change and composition. Immersions are stable under base change and composition. ⌟

Proof: For immersion, shrink the open subset. □

Remark (6.4.4.61). A open immersion followed by a closed immersion can be written as a closed immersion followed by an open immersion, but not reversely. The reverse happens if the immersion is quasi-compact or the source is reduced (use the reduced induced structure). ⌟

Def. (6.4.4.62) [Scheme-Theoretical Image]. For a morphism $f : X \to Y$, there is a closed scheme called **scheme-theoretic image** that is the smallest closed subscheme of Y that f factors through Z.

For an immersion of schemes, the scheme-theoretic image of the immersion is called the **scheme-theoretic closure**. ⌟

Proof: Consider the kernel of the structural map, and the kernel contains a maximal Qco sheaf of ideals $\mathcal{I}$ by(6.5.1.12). □

Prop. (6.4.4.63). If $\begin{array}{ccc} X_1 & \xrightarrow{f_1} & Y_1 \\ \downarrow & & \downarrow \\ X_2 & \xrightarrow{f_2} & Y_2 \end{array}$ be a commutative diagram of schemes and $Z_i \subset Y_i$ be the scheme-theoretic image of f_i, then it induces a commutative diagram $\begin{array}{ccccc} X_1 & \longrightarrow & Z_1 & \longrightarrow & Y_1 \\ \downarrow & & \downarrow & & \downarrow \\ X_2 & \longrightarrow & Z_2 & \longrightarrow & Y_2 \end{array}$. ⌟

Proof: It suffices to show Z_1 factors through the closed subscheme $Z_2 \times_{Y_2} Y_1$ of Y_1, which follows from the universal property of Z_1. □

Prop. (6.4.4.64). Let $f : X \to Y$ be a qc morphism of schemes and Z be the scheme-theoretical image, then

- the kernel $\mathcal{I} = \ker(\mathcal{O}_Y \to f_*\mathcal{O}_X)$ is Qco, thus Z is the closed subscheme determined by $\mathcal{I}$.
- For any open subscheme $U \subset Y$, the scheme-theoretical image of $f|_{f^{-1}(U)}$ is equal to $Z \cap U$.
- $f(X)$ is dense in Z.

⌟

Proof: 1: As being Qco is local, it suffices to show for Y affine. Then $X = \cup U_i$ is a finite union of affine schemes. Now take $X' = \coprod U_i$, then there are maps $X' \xrightarrow{f'} X \to Y$. Then $\mathcal{O}_X$ is a subsheaf of $f'_*\mathcal{O}_X$. So $\mathcal{I} = \ker(\mathcal{O}_Y \to f_*f'_*\mathcal{O}_{X'})$. Now $f \circ f'$ is qcqs, thus by(6.5.1.6), $f_*f'_*\mathcal{O}_{X'}$ is Qco, thus also $\mathcal{I}$ is Qco.

2 follows from 1 as the formation of $\mathcal{I}$ commutes with restriction to open subschemes.

3 follows from 2 as the scheme-theoretical image of empty set is empty. □

Prop. (6.4.4.65). If $f : X \to Y$ is a morphism and X is reduced, then the scheme-theoretical image of f is the induced-reduced structure(6.4.1.14) of $\overline{f(X)} \subset Y$. ⌟

Proof: This is clear. □

Def. (6.4.4.66) [Scheme-Theoretically Dense]. An open subscheme $U \subset X$ is called **scheme-theoretically dense** if for any open subscheme V of X, the scheme-theoretical closure of $U \cap V$ in V is equal to V. ⌟

Prop. (6.4.4.67). If the inclusion $U \to X$ is qc, then U is scheme-theoretically dense in X iff the scheme-theoretical closure of U is X, by(6.4.4.64). ⌟

Prop. (6.4.4.68). Let $j : U \to X$ be an open immersion of schemes, then U is scheme-theoretically dense in X iff $\mathcal{O}_X \to j_*\mathcal{O}_U$ is injective. ⌟

Proof: If it is not injective, then we can find an open subscheme V of X that the kernel is non-zero, thus it contains a non-zero Qco ideal sheaf, which means the scheme-theoretical closure of $U \cap V$ is not V. □

Cor. (6.4.4.69). If U, V are open subschemes of X scheme-theoretically dense in X, then $U \cap V$ is also scheme-theoretically dense in X. ⌟

Proof: $\mathcal{O}_X \to \mathcal{O}_X(U) \to \mathcal{O}_X(U \cap V)$ is injective. □

Prop. (6.4.4.70) [Scheme-Theoretical Image of Immersions]. Let $f: Z \to X$ be an immersion and either f is qc or Z is reduced. Let $\overline{Z}$ be the scheme-theoretically image of f, then the morphism $Z \to \overline{Z}$ is an open immersion that identifies Z with a scheme-theoretical dense open subscheme of $\overline{Z}$, and also Z is dense in $\overline{Z}$. ⌟

Proof: Cf.[Sta]01RG. □

Prop. (6.4.4.71) [Immersion to be Closed]. An immersion f is a closed immersion iff the image is closed. ⌟

Proof: Let $i: Y \to U$ be a closed immersion where $j: U \subset X$ is an open subscheme, then i is associated to an ideal sheaf $\mathcal{I}$ of $\mathcal{O}_U$. Now because $\mathcal{I}|_{U\setminus f(Y)} = \mathcal{O}_{U\setminus f(Y)}$, we can glue $\mathcal{I}$ and $\mathcal{O}|_{X\setminus f(Y)}$ to a sheaf of ideals $\mathcal{J} \subset \mathcal{O}_X$. Now $j^*O_X/\mathcal{J} = \mathcal{O}_U/\mathcal{I} \cong i_*\mathcal{O}_Y$, thus $\mathcal{O}_X \to f_*\mathcal{O}_Y = j_*(\mathcal{O}_U/\mathcal{I}) = j_*j^*(\mathcal{O}_X/\mathcal{J})$ is surjective, because $\mathcal{O}_U/\mathcal{I}$ is supported on a closed subset of U. Thus f is a closed immersion by(6.4.4.57). □

Prop. (6.4.4.72). Immersions are monomorphisms. ⌟

Proof: It is easy to check(6.4.4.5) for both open and closed immersions. □

Prop. (6.4.4.73) [Equivalent Definitions of Closed Immersion]. The following are equivalent for a morphism f:

- f is a closed immersion.
- f is a proper monomorphism.
- f is proper, unramified and u.i..
- f is a u.c., unramified monomorphism.
- f is u.c., unramified and u.i..
- f is u.c., locally of f.t. and a monomorphism.
- f is u.c., u.i., locally of f.t. and formally unramified.

⌟

Proof: $4-7$ are equivalent by(6.6.5.13). For the rest, Cf. [Sta], 04XV. □

Universal Homeomorphism

Prop. (6.4.4.74). A morphism is a universally homeomorphism iff it is integral, surjective and universally injective. ⌟

Proof: A universally homeomorphism is affine by(6.4.4.15). It is clearly u.c, so it is integral by(6.4.4.39). Conversely, it is integral hence u.c, and universally bijective, so it is universally homeomorphism. □

Cor. (6.4.4.75). The reduction $X_{\text{red}} \to X$ is a universal homeomorphism, as closed immersion is u.c.. ⌟

Separatedness

Def. (6.4.4.76) [Separatedness]. A map $f : X \to Y$ is called **separated** if the diagonal $\Delta : X \to X \times_Y X$ is a closed immersion. It is called **quasi-separated** if the diagonal is quasi-compact.

In fact Δ is always an immersion because maps between affine scheme is separated so $\Delta(X)$ is closed in $\cup U_{ij} \otimes_{V_i} U_{ij}$ where U, V are affine open, hence it suffice to check the image is closed. ⌟

Prop. (6.4.4.77). (Quasi-)Separateness is local on the target because closed immersion and quasi-compact is local on the target(6.4.1.5).

(Quasi-)Separatedness satisfies base change trick by(6.4.4.2). ⌟

Prop. (6.4.4.78) [Graph]. By(4.1.1.50), for $X \to S$ and $Y \to S$, the map $X = X \times_Y Y \to X \times_S Y$ is an immersion. It is closed immersion if $Y \to S$ is separated, and it is qc if $Y \to S$ is quasi-separated. ⌟

Cor. (6.4.4.79). for $X \to Y$ is a morphism of schemes over S, the map $X = X \times_Y Y \to X \times_S Y$ is an immersion. It is closed immersion if $Y \to S$ is separated, and it is qc if $Y \to S$ is quasi-separated. ⌟

Cor. (6.4.4.80). If $s : S \to X$ is a section of $f : X \to S$, the above proposition applies to this case, because $S = S \times_X X \to S \times_S X = X$. ⌟

Prop. (6.4.4.81) [Characterization of Separatedness]. A morphism is quasi-separated iff for any two affine open that mapped into an affine open, their intersection is quasi-compact. This is because quasi-compact is local on the target.

A morphism is separated iff for any two affine open that mapped into an affine open, their intersection is affine and $\mathcal{O}(U) \otimes_{\mathcal{O}(W)} \mathcal{O}(V) \to \mathcal{O}(U \cap V)$ is surjective. This is because closed immersion is local on the target(6.4.1.5). ⌟

Cor. (6.4.4.82). A locally Noetherian scheme is quasi-separated. ⌟

Cor. (6.4.4.83). If $g \circ f$ is (quasi-)separated, then so is f. ⌟

Cor. (6.4.4.84). If X is (quasi-)separated, then $X \to Y$ is (quasi-)separated. ⌟

Prop. (6.4.4.85) [Injective Maps are Separated]. Injective maps of schemes are separated. ⌟

Proof: Let $f : X \to Y$ be an injective map. Firstly $X \times_Y X$ is a union of affine subschemes of the form $U \times_V U$ where U, V are affine and $f(U) \subset V$: let $z \in X \times_Y X$, then $\pi_1(z) = \pi_2(z)$, because they map to the same point in Y, thus we can choose affine nbhds U, V of $\pi_1(z)$ and $f(\pi_1(z))$. Now for each of these $U \times_V U$, $\Delta : U \to U \times_V U$ is closed immersion, thus Δ_X is also closed immersion(6.4.1.5). □

Cor. (6.4.4.86). monomorphisms are separated because they are universal injective(6.4.4.4), and immersions are separated. ⌟

Prop. (6.4.4.87). (Quasi-)Affine morphism is separated (Check closed immersion directly). ⌟

Prop. (6.4.4.88). if $f : X \to S$ is affine, $h : Y \to S$ is separated, and $g : X \to Y$ is a morphism over S, then g is affine. ⌟

Proof: Decompose g as $X \to X \times_S Y \to Y$, where the first map is base change of Δ_Y and the second map is base change of f, so they are both affine. □

Prop. (6.4.4.89) [Scheme-Theoretic Equalizer]. If X, Y are schemes over S and $a, b : X \to S$ are morphisms, then there is a largest locally closed subscheme Z of X that $a|_Z = b|_Z$. And if Y/S is separated, Z is a closed subscheme of X. ⌟

Proof: By definition, Z should be the fibered product:

$$\begin{array}{ccc} Z & \longrightarrow & X \\ \downarrow & & \downarrow{\scriptstyle (a,b)} \\ Y & \xrightarrow{\Delta_Y} & Y \times_S Y \end{array}$$

then the theorem follows from the definition and base change trick of locally closed morphisms. □

Prop. (6.4.4.90) [Qsqc Lemma]. Let X be a qcqs scheme and $s \in \Gamma(X, \mathcal{O}_X)$, then there is a natural isomorphism $\Gamma(X, \mathcal{O}_X)_s \cong \Gamma(X_s, \mathcal{O}_X)$. ⌟

Proof: Firstly this is true for X affine by definition(6.2.7.1). In general, let U_i be an affine open cover of X that $U_i \cap U_j = \cup_{k=0}^{c_{ij}} U_{ijk}$ be a finite cover by affine opens, then there is an exact sequence

$$\Gamma(X, \mathcal{O}_X) \to \prod_i \Gamma(U_i, \mathcal{O}_X) \to \prod_{ijk} \Gamma(U_{ijk}, \mathcal{O}_X).$$

Then we can take localization by s to get an exact sequence

$$\Gamma(X, \mathcal{O}_X)_s \to \prod_i \Gamma(D(s, U_i), \mathcal{O}_X)_s \to \prod_{ijk} \Gamma(D(s, U_{ijk}), \mathcal{O}_X)_s.$$

but $D(s, U_i)$ is an open cover of X_s with $D(s, U_i) \cap D(s, U_j) = \cup_k D(s, U_{ijk})$, thus we get a natural isomorphism $\Gamma(X, \mathcal{O}_X)_s \cong \Gamma(X_s, \mathcal{O}_X)$. □

5 Proper & Projective

Prop. (6.4.5.1) [Proper]. A morphism that is separated, of finite type and universally closed is called **proper**.

Properness is local on the target, because all these three properties do(6.4.1.5). Properness satisfies the base change trick(6.4.4.2). ⌟

Prop. (6.4.5.2). The class of proper morphisms satisfies the base change trick(6.4.4.1), by valuation criterion(6.4.5.13) and fibered products tricks. ⌟

Proof: Closed immersion is proper because it is f.t. and is affine so separated(6.4.4.76), and it is universally closed because immersions are stable under base change(6.4.4.60). □

Prop. (6.4.5.3) [Image of Proper Map]. If $f : X \to Y$ is morphism between separated schemes f.t over S, then if X is proper, then f is proper(by base change trick) thus the image is closed, and is proper over S in its scheme-theoretic structure. ⌟

Proof: Notice proper is qc, so by(6.4.4.62), the scheme-theoretic closure has the same underlying space as the image. Then use(6.4.4.8) to show it is u.c.. □

Cor. (6.4.5.4) [Connected Proper to Affine Constant]. A morphism from a connected proper scheme to an Noetherian affine scheme Spec A is constant. ⌟

Proof: Because the image is proper, by(6.7.4.12), the global section of its image is a finite module over k thus Artinian(5.1.3.4) so has finitely many points and is discrete. But X is connected, thus it is constant. □

Prop. (6.4.5.5) [Chevalley]. Let $f : X \to Y$ be a morphism of schemes, the following are equivalent:

- f is finite.
- f is proper and affine.
- f is proper with finite fibers.
- f is proper and locally quasi-finite.
- f is separated, u.c., locally of f.t. and has finite fibres.

⌟

Proof: The fiber of $f : X \to S$ is $\mathrm{Spec}(k(y) \otimes_A B)$, which is Artinian(5.1.3.4), so it has finitely many primes and they are all closed. Finite morphism is proper because it is integral(6.4.4.39).

The converse follows from Zariski's main theorem(6.4.4.49).

Cf.[Sta]02LS. □

Cor. (6.4.5.6) [Quasi-Affine+Proper imply Affine]. Let $f : X \to \mathrm{Spec}\, A$ be a quasi-affine and proper map, then f is affine. ⌟

Proof: This follows from(6.7.2.8)(6.4.4.20) and the fact $H^p(X, \mathcal{O}_X) = 0$ for $p > 0$. □

Prop. (6.4.5.7) [Quasi-Finite+Proper Imply Finite]. Let $f : X \to S$ be a proper morphism of schemes and $s \in S$ that $f^{-1}(s)$ is a finite set, then there exists a nbhd V of $s \in S$ that $f^{-1}(V) \to V$ is finite. ⌟

Proof: By(6.4.4.46), f is quasi-finite at the points of $f^{-1}(s)$. By(6.4.4.48) the set U of points that f is quasi-finite is open. Denote $Z = X \backslash U$, then $f(Z)$ is closed in S and doesn't contain s. Then $V = S \backslash f(Z)$ satisfies the requirement by(6.4.5.5). □

Prop. (6.4.5.8) [Generically Finite+Proper Imply Finite]. Let $f : X \to S$ be a proper morphism of locally Noetherian schemes and $y \in Y$ satisfies $\dim \mathcal{O}_{Y,y} \leq 1$, and if one of the following holds:

- For every generic point η of X s.t. $f(\eta)$ generalizes y, $k(\eta)/k(f(\eta))$ is algebraic.
- f is quasi-finite at every generic point of x.
- f is quasi-finite on a dense subset of X.

then there exists an open nbhd V of $y \in Y$ s.t. $f^{-1}(V) \to V$ is finite. ⌟

Proof: Cf.[Sta]0AB7. □

Prop. (6.4.5.9). If X is a separated scheme over a field k of dimension> 0 and $x \in X$ is a closed point, then $X \backslash \{x\}$ is not proper over k. ⌟

Proof: Cf.[Sta]0A24. □

Def. (6.4.5.10) [Modification and Alteration]. A **modification** of $X \in \mathcal{S}\mathrm{ch}$ is a scheme X' together with a proper birational map $X' \to X$.

A **alteration** of X is a scheme X' together with a proper dominant morphism $f : X' \to X$ that for some non-empty open U of X, $f^{-1}(U) \to U$ is finite. ⌟

Prop. (6.4.5.11) [Modifications and Alterations]. Any modification is an alteration. And if $Y \to X \in \mathcal{S}ch$ be an alteration, then it can be decomposed into $Y \to W \to X$ where $Y \to X$ is a modification and $W \to X$ is finite surjective. ⌟

Proof: ?Use Stein factorization. □

Valuation Criteria

Lemma (6.4.5.12) [Valuation Criteria Lemma]. If X is a scheme and $x \to y$ is a specialization of pts, then for any field extension $K/k(x)$, there is a valuation ring $A \subset K$ and a morphisms $\operatorname{Spec} A \to X$ that maps the generic pt η to x and the unique closed pt to y.

Moreover, if X is locally Noetherian, then A can be chosen to be a DVR. ⌟

Proof: There is a morphism $\mathcal{O}_{X,y} \to k(x) \to K$, so there is a valuation ring A with field of fractions K that dominate the image of $\mathcal{O}_{X,y}$ by(11.2.2.1), which is also a local ring(5.1.1.10). Then this is what we desire.

For the locally Noetherian case, add(11.2.3.7). □

Prop. (6.4.5.13) [Valuation Criteria]. The valuation criterion for $\operatorname{Spec} K \to \operatorname{Spec} R$ where R is a valuation ring with field of fractions K: Given a morphism $f : X \to S$,

1. If it is qc, then it is universally closed iff there is at least one lifting.
2. it is separated iff it is quasi-separated and there is at most one lifting.
3. it is proper iff it is finite type, quasi-separated and lifting exists uniquely.

⌟

Moreover, if S is locally Noetherian and f is locally of f.t., then it suffices to check for discrete valuation rings. *Proof:*

1. Firstly, in this case, by(6.4.4.9), it suffices to prove that: specializations lift along any base change of f iff it has has least one lifting. If specializations lift along any base change of f, change S to $\operatorname{Spec} A$ and X to $X \times_S \operatorname{Spec} A$. Let x' be the image of $\operatorname{Spec} K \to X$, then by hypothesis there is a specialization $x' \to x$ where x mapsto the closed pt of $\operatorname{Spec} A$. Then we get a map $A \to \mathcal{O}_{X,x} \to k(x') \to K$, which is exactly the quotient map $A \to K$. So the image of $\mathcal{O}_{X,x}$ in K dominates A, which means it is just A. Thus we get a map $\mathcal{O}_{X,x} \to A$, which gives a map $\operatorname{Spec} A \to X$ that commutes $\operatorname{Spec} K$.
   Converly, if f has at least one lifting, then any base change of f also has at least one lifting by categorial reason. Thus it suffices to show specializations lift along f. Let $s' \to s$ be a specialization in S and $x' \in X$ maps to s', we can apply(6.4.5.12) to $k(s') \subset k(x') = K$, then we get a lifting diagram, and the image of the closed pt of $\operatorname{Spec} A$ under the lifting is a point mapping to s.
2. If it is separated, then if there are two lifting, then consider their equalizer, it is a closed subscheme of $\operatorname{Spec} A$ by(6.2.7.18), and it contains the generic pt, so it equals $\operatorname{Spec} A$, as desired. Conversely, if there are at most one lifting, then we want to prove the diagonal is closed. But by (6.4.4.76) and(6.4.4.71) and the valuation criterion for u.c., it suffices to prove the existence of a lifting for the diagonal map(6.4.5.13). But in fact, a valuation digram for the diagonal correspond to two lifting of a valuation criterion for $X \to S$, then they are the same, and $\operatorname{Spec} A \to X \times_S X$ lifts along the diagonal.
3. follows from the above two.

□

Prop. (6.4.5.14)[Extension of Rational Maps]. Let X, Y be schemes over S, X is locally Noetherian and Y/S is proper. If there is a morphism from an open subset U of X to Y, and there is a point x in the closure of U with the stalk being a valuation ring, then the morphism can be extended to an open set containing x. ⌟

Proof: We can replace X by an affine open nbhd of X. By(6.4.6.1), we assume X is affine and $\Gamma(X, \mathcal{O}_X) \subset \mathcal{O}_{X,x}$. In particular X is integral with generic pt ξ with residue field K. Then U contains ξ. By the valuation criterion(6.4.5.13), the morphism $\operatorname{Spec} K \xrightarrow{\xi} U \to Y$ can be lifted to a morphism $\operatorname{Spec} \mathcal{O}_{X,x} \to Y$, thus lemma(6.4.6.2) shows there is a morphism on a nbhd V of X spreading this morphisms.

Now because Y/S is separated, the equalizer of this morphism and f on their intersection is a closed subscheme by(6.4.4.89), but it contains ξ, so they coincide on the intersection, so we are done. □

Prop. (6.4.5.15) [Singularity in Codimension1]. Let $\varphi : X \to X'$ be a rational map from a locally Noetherian scheme X/K regular in codimension1 to a proper scheme X'/K with maximal domain U, then

$$\operatorname{codim}(X \backslash U, X) \geq 2.$$

In particular, if X is non-singular curve, then φ is a morphism. ⌟

Proof: Use(6.4.5.14), noticing that the stalk at a point of codimention1 is a DVR(5.3.5.20). □

Projective Morphism

Def. (6.4.5.16) [Projective Morphisms]. A **projective morphism** $X \to Y$ is a closed immersion $X \to \operatorname{Proj}(\mathcal{E})$ for some $\mathcal{E} \in \mathfrak{QCoh}^{\mathrm{ft}}/Y$.

A **strongly projective morphism** $X \to Y$ is a closed immersion $X \to \operatorname{Proj}(\mathcal{E})$ for some $\mathcal{E} \in \mathfrak{QCoh}^{\mathrm{lf,ft}}/Y$.

An **H-projective morphism** $X \to Y$ is a closed immersion $X \to \mathbb{P}^n_Y$ for some $n \in \mathbb{Z}_+$.

An **H-quasi-projective morphism** is an H-projective morphism composed with a quasi-compact open immersion.

A **locally projective morphism** is a morphism $f : X \to Y \in \mathfrak{Sch}$ s.t. there exists a covering U_i of Y that $f^{-1}(U_i) \to U_i$ is projective. ⌟

Prop. (6.4.5.17). For a morphism $f : X \to S$, he following are equivalent:

- f is locally projective.
- There is a covering U_i of S that $f^{-1}(U_i) \to U_i$ is H-projective.

⌟

Proof: Clearly 2 implies 1, and for the converse, it suffices to show that projective morphism is locally H-projective. Locally on each affine open nbhd $U = \operatorname{Spec} R$, X_U is isomorphic to a closed subscheme of $P(\mathcal{E})$ for some f.t. Qco sheaf of $\mathcal{O}_U$-modules $\mathcal{E}$. Write $\mathcal{E} = \widetilde{M}$ for some f.t. R-module M, and choose a set of generators $x_1, \ldots, x_n$ for M, which induces a surjection of graded R-algebra $R[X_0, \ldots, X_n] \to \operatorname{Sym}_R(M)$, then the corresponding morphism $P(\mathcal{E}) \to \mathbb{P}^n$ is a closed immersion, so $f^{-1}(U)$ is a H-projective scheme over U. □

Prop. (6.4.5.18). H-(quasi-)projectiveness is stable under base change and composition. (because Segre embedding is closed). Disjoint union of f.m. projective morphisms is projective (embed into the Segre embedding). ⌟

Proof: [Sta]01WE. □

Cor. (6.4.5.19) [Projective Maps are Proper]. Projective morphisms are locally projective and locally projective morphisms are proper. Thus a quasi-projective morphism is locally of f.t. and separated(6.4.4.86). ⌟

Proof: Because locally projective and proper are both local on the base(6.4.4.2), it suffices to show that H-projective morphism is proper by(6.4.5.17).

Because properness satisfies base change trick(6.4.4.2), it suffices to show $\mathbb{P}^n_S \to S$ is proper. Also this is base change of $\mathbb{P}^n_{\mathbb{Z}} \to \mathbb{Z}$, it suffices to check this one. $\mathbb{P}^n_{\mathbb{Z}}$ is clearly separated by(17.5.3.20)(looking at the natural affine covering), and qc. Finally we show it is u.c. using valuation criterion(6.4.5.13):

Let $\begin{array}{ccc} \operatorname{Spec} K & \longrightarrow & X \\ \downarrow & \nearrow & \downarrow \\ \operatorname{Spec} R & \longrightarrow & \operatorname{Spec} \mathbb{Z} \end{array}$ be a diagram, by induction on n, we may assume the image ξ_1 of $\operatorname{Spec} K$ is not contained in any of the hypersurface $V(x_i)$, then x_i are all invertible in $\mathcal{O}_{\xi_1}$, and there is a morphism $\varphi : k(\xi_1) \to K$. Let f_{ij} be the image of x_i/x_j under φ, and choose k which f_{k0} has the minimal valuation, then $f_{ik} \in R$ for any i, which means the there is a map

$$\mathbb{Z}[x_0/x_k, \ldots, x_n/x_k] \to R$$

compatible with φ, or equivalently a map $\operatorname{Spec} R \to D(x_k) \subset X$ commuting the diagram. □

Prop. (6.4.5.20) [Descent for Projectiveness]. Let X be a scheme over a field k, and K/k is a field extension, then X_k is (quasi-)projective iff X_K is (quasi-)projective. ⌟

Proof: This follows from(6.5.4.21) and f.f. descent. □

Prop. (6.4.5.21). H-Projective scheme over $\operatorname{Spec} A$ is of the form $\operatorname{Proj} S$ where $S_0 = A$ and S is f.g over S_0 by S_1(6.5.2.11). ⌟

Proof: □

Prop. (6.4.5.22) [Projective Morphisms and Closed Embeddings]. Let k be an alg.closed field and $\pi : X \to Y$ is a projective morphism of algebraic schemes over k that is injective on closed points and injective on tangent vectors at closed points, then π is a closed embedding. ⌟

Proof: Cf.[Vak17]P506. □

Prop. (6.4.5.23) [Chow's Lemma]. Let $X \to S$ be separated of f.t over a qcqs S, then there is a birational, H-projective map $\pi : X' \to X$ over S that X' is quasi-projective over S.

If X is proper, then X' is projective over S. And if X is integral/irreducible/reduced over S, X' can also be chosen to be so. ⌟

Proof: We only prove for S Noetherian, for the general case, Cf.[Sta]0203.

In this case all schemes here are Noetherian. Suppose $X_i, i \leq r$ are irreducible components of X with generic points η_i, by(6.4.6.5) and the fact X is qc we can find a finite affine cover $X = \cup U_i$ that each U_i contains all the generic points of X, thus $U = U_1 \cap \ldots \cap U_n$ is dense in X. Let X^* be the schematic-closure of U in X, and $U_i^* = U_i \cap X^*$, then we may replace X by X^* and assume that U is schematically dense in X by(6.4.4.67) as X is qs. By(6.5.4.24) and(6.4.4.19), there are immersions $U_i \to \mathbb{P}_S^{n_i}$ together with a closed subscheme $Z_i \subset \mathbb{P}_S^{n_i}$ that $U_i \to Z$ is a scheme-theoretically dense open immersion(6.4.4.70).

Consider the map $(j_1, \ldots, j_m) : U \to \mathbb{P}_S^{n_i} \times \ldots \times \mathbb{P}_S^{n_m}$ with scheme-theoretic image Z, and the commutative diagrams

$$\begin{array}{ccc} U & \xhookrightarrow{(j_1,\ldots,j_m)} & \mathbb{P}_S^{n_i} \times \ldots \times \mathbb{P}_S^{n_m} \\ \big\downarrow & & \big\downarrow \pi_i \\ U_i & \xhookrightarrow{\quad j_i \quad} & \mathbb{P}_S^{n_i} \end{array},$$

which induces a map $p_i : Z \to Z_i$(6.4.4.63) which is proper.

Consider $p_i^{-1}(j_i(U_i)) = V_i$ and $X' = \cup_i V_i$ which is an open subscheme of $Z \subset \mathbb{P}_S^{n_i} \times \ldots \times \mathbb{P}_S^{n_m}$ thus quasi-projective over S.

Finally, we prove that the morphism $p_i : V_i \to U_i$ glue together to a proper birational morphism $\pi : X' \to X$: this is because they are compatible on U, which is scheme-theoretically dense in V_i for each i thus also also scheme-theoretically dense in $V_i \cap V_j$, thus p_i and p_j are compatible on $V_i \cap V_j$ as the target X is separated over S.

To show π is proper, firstly notice $\pi^{-1}(U_i) = V_i$: there are decompositions $V_i \to \pi^{-1}(U_i) \to U_i$, where $V_i \to U_i$ is proper, thus $V_i \to \pi^{-1}(U_i)$ is also proper and V_i is schematically dense in $\pi^{-1}(U_i)$ because it contains U, so it is and isomorphism.

For the same reason $U \to \pi^{-1}(U)$ is an isomorphism. Finally π is projective because it factors through some map $X' \to X \times_S \mathbb{P}_S^n = \mathbb{P}_X^n$ and it is proper.

If X is reduced, then X' is reduced by(6.4.4.65), and if X is irreducible, then $X' = Z$ is the closure of $j(X)$ by(6.4.4.70), which is irreducible. □

6 Technical Lemmas

Lemma (6.4.6.1). Let X be a scheme and x a point, then there exists an open affine nbhd U of x that $\mathcal{O}_X(U) \to \mathcal{O}_{X,x}$ is injective, if any of the follows holds:

- X is integral.
- X is locally Noetherian.
- X is reduced with f.m. irreducible components.

⌟

Proof: This problem is clearly local hence follows from the algebra case(5.1.1.35). □

Lemma (6.4.6.2) [Spread Out Stalk Morphism]. Let X, Y be schemes over S, $s \in S$ and x, y be pts over S, then:

- Let $f, g : X \to Y$ be morphisms over S that $f(x) = g(x) = y$ and $f_x^\sharp = g_x^\sharp$, then $f = g$ on a nbhd U of x if any of the following holds:
  (a) Y/S is locally of f.t..

(b) X is integral.

(c) X is locally Noetherian.

(d) X is reduced with f.m. irreducible components.

- Let $\varphi:\mathcal{O}_{Y,y}\to\mathcal{O}_{X,x}$ be a local ring map over $\mathcal{O}_{S,s}$, then there is a morphism f from a nbhd U of x mapping to Y that $f(x)=y$, and $f_x^\sharp=\varphi$, if any of the following holds:
  (a) Y/S is locally of f.p..
  (b) Y/S is locally of f.t. and X is integral.
  (c) Y/S is locally of f.t. and X is locally Noetherian.
  (d) Y/S is local of f.t. and X is reduced with f.m. irreducible components.

⌟

Proof: Cf.[[Sta]0BX6]. □

Prop. (6.4.6.3) [Base Change of Fields is Quotient Map]. For any scheme X over a field k and algebraic extensions K/k, $X_K\to X$ is a quotient map, as it is surjective(6.6.2.1), continuous and closed(6.4.4.39). ⌟

Lemma (6.4.6.4). Let X be a qs scheme and Z_i be a finite set of irreducible components of X. Let η_i be the generic point of Z_i, then there are open affine subsets $\eta_i\in U_i$ that $U_1,\ldots,U_n$ are pairwise disjoint. ⌟

Proof: □

Lemma (6.4.6.5). Let X be a qs scheme and Z_i be a finite set of irreducible components of X. Let η_i be the generic point of Z_i and $x\in X$, then there is an affine open subset of X containing x and η_i. ⌟

Proof: Let $x\in Z_1,\ldots,Z_r$ but $x\notin Z_{r+1},\ldots,Z_n$, then we can find an arbitrary affine open nbhd W of x that contains $\eta_1,\ldots,\eta_r$ but not $\eta_{i+1},\ldots,\eta_n$. By(6.4.6.4), we may choose pairwise disjoint affine open nbhds $\eta_{r+1}\in U_{r+1},\ldots,\eta_m\in U_n$. Now $U_i\cap W$ is quasi-compact and doesn't contain η_i, so we can shrink U_i s.t. $W\cap U_i=\varnothing$ by(5.1.7.24). Then $U=W\coprod(\coprod U_i)$ satisfies the desired condition. □

Main references are [Sta]and [Vak17].

6.5 Quasi-Coherent Sheaves on Schemes

1 (Quasi-)Coherent Sheaves

Lemma (6.5.1.1) [Associated Qco Sheaves on Affine Scheme]. On an affine scheme $\operatorname{Spec} A$, there is a sheaf $\widetilde{M}$, that is M_f on $\operatorname{Spec} A_f$. To check it is a sheaf, we only need to check to affine coverings, and this follows from(5.4.2.2). ⌟

Prop. (6.5.1.2) [Qco Sheaves on Affine Schemes]. $M \mapsto \widetilde{M}$ is an equivalence to the category of quasi-coherent sheaves over $\operatorname{Spec} A$. In particular,

$$\operatorname{Hom}_A(M, \Gamma(X, \mathcal{G})) \cong \operatorname{Hom}_{\mathcal{O}_X}(\widetilde{M}, \mathcal{G}),$$

so $M \mapsto \widetilde{M}$ commutes with colimits and is exact, and commutes with pullbacks.

When A is Noetherian, this also induces an equivalence between finite A-modules and coherent sheaves over $\operatorname{Spec} A$, because finiteness for modules is local(6.4.1.5). ⌟

Proof: For any A-module M, there is a sheaf of modules $\mathcal{F}_M$ on $X = \operatorname{Spec} A$ by(6.2.2.26). This is left adjoint to Γ and defines a functor from the category of A-modules to the category of $\mathcal{O}_{\operatorname{Spec} A}$-modules.

By universal property of $\mathcal{F}_M$(6.2.2.26), there is a natural map $\mathcal{F}_M \to \widetilde{M}$ corresponding to the ring map $M \mapsto \Gamma(\operatorname{Spec} A, \widetilde{M}) = M$. The induced maps on the stalk at a point x is $M \otimes_A \mathcal{O}_{X,x} \to M_{\mathfrak{p}}$, which is isomorphism, so $\mathcal{F}_M \cong \widetilde{M}$.

From the universal property of $\widetilde{M} = \mathcal{F}_M$, $\operatorname{Hom}(\widetilde{M}, \widetilde{N}) = \operatorname{Hom}(M, N)$, thus $\sim$ is fully faithful, to show it is an equivalence, it suffices to show for any Qco sheaf $\mathcal{F}$ on $\operatorname{Spec} A$, the natural map $\widetilde{\Gamma(X, \mathcal{F})} \to \mathcal{F}$ is an isomorphism:**?** Cf.[Sta]01IA.

If $0 \to M_1 \to M \to M_2 \to 0$ is exact, then $0 \to \widetilde{M_1} \to \widetilde{M} \to \widetilde{M_2} \to 0$ is exact, because localization is exact. □

Prop. (6.5.1.3) [properties of (Quasi-)Coherent Sheaves on Schemes].

- $\mathfrak{QCoh}(X)$ and $\mathfrak{Coh}(X)$ are weak Serre subcategories of $\mathfrak{Mod}_{\mathcal{O}_X}$, and $\mathfrak{Coh}(X)$ is a Serre subcategory of $\mathfrak{QCoh}(X)$.
- Colimits in $\mathfrak{Mod}(\mathcal{O}_X)$ preserves $\mathfrak{QCoh}(X)$, because localization is exact.
- Tensor product of two (Q)co sheaf is (Q)co, and locally free if they are locally free. More explicitly, $\widetilde{M \otimes_A N} \cong \widetilde{M} \otimes_{\mathcal{O}_X} \widetilde{N}$ as tensor product commutes with π^*.
- If $\mathcal{F}$ is Qco, then so does $T(\mathcal{F}), \operatorname{Sym}(\mathcal{F})$ and $\wedge(\mathcal{F})$, by(6.2.3.12).
- Given $\mathcal{F}, \mathcal{G} \in \mathfrak{QCoh}(\mathcal{F})$ that $\mathcal{F}$ is f.p., $\mathcal{H}om(\mathcal{F}, \mathcal{G}) \in \mathfrak{QCoh}(X)$, by(6.2.3.2) and(6.5.1.2). More explicitly, affine locally $\mathcal{H}om_X(\widetilde{M}, \widetilde{N}) = \widetilde{\operatorname{Hom}_A(M, N)}$.
- pullback preserves $\mathfrak{QCoh}(X)$ and $\mathfrak{Coh}(X)$, by(6.2.2.29). More explicitly, if $\operatorname{Spec} B \subset Y$ is mapped into $\operatorname{Spec} A \subset X$, then $f^*(\mathcal{F})(\operatorname{Spec} B) = \mathcal{F}(\operatorname{Spec} A) \otimes_A B$, using the fact $\widetilde{M} = \mathcal{F}_M = \pi^* M$.

⌟

Proof: 1: $\mathfrak{Coh}(X)$ follows from(6.2.2.28). For $\mathfrak{QCoh}(X)$, it follows from(6.5.1.2) that the kernel and cokernel of $\varphi : \widetilde{M} \to \widetilde{N}$ is just $\widetilde{\ker\varphi}$ and $\widetilde{\mathrm{Coker}\,\varphi}$ which is Qco, for the extension of Qco, use(6.7.1.3) that the global section is exact, so there is a morphism of exact sequences $\widetilde{\Gamma(X,\mathcal{F}_i)}(U) \to \mathcal{F}_i(U)$, and five lemma gives the result. □

Prop. (6.5.1.4) [Qco Sheaves of F.T./F.P]. Let $X = \operatorname{Spec} A$ and $\mathcal{F} = \widetilde{M}$ a Qco sheaf on X, then $\mathcal{F}$ is of f.t./f.p. if M is of f.t/f.p. over A. ⌟

Proof: These follows from the fact finiteness/f.p. are local properties for modules over a ring(5.1.4.4). □

Def. (6.5.1.5) [Locally Projective Qco Sheaves]. Let X be a scheme, then a **locally projective Qco sheaf** is a Qco sheaf $\mathcal{F}$ on X that is affine locally a locally projective module sheaf.

Being locally projective for Qco sheaves satisfies fpqc descent, by(5.4.2.1). ⌟

Prop. (6.5.1.6) [Qcqs Pushforward]. If f is qcqs, then the pushforward of of a Qco sheaf is Qco. (Used in**??**). ⌟

Proof: The question is local so we let Y be affine, and then X is qcqs, so we cover it with affine opens U_i and their intersections are U_{ijk}. Then we see by sheaf property

$$0 \to f_*\mathcal{F} \to \oplus_i f_*(\mathcal{F}|_{U_i}) \to \oplus_{ijk} f_*(\mathcal{F}|_{U_{ijk}})$$

The last two are Qco because two are maps between affine schemes, so the first is Qco. □

Prop. (6.5.1.7) [Qco Sheaves on Qcqs Schemes]. For a qcqs scheme X and $s \in \Gamma(X, \mathcal{O}_X)$, and a Qco module $\mathcal{F}$, $(\Gamma(X,\mathcal{F}))_s \cong \Gamma(X_s, \mathcal{F})$. ⌟

Proof: The canonical map $f : X \to \operatorname{Spec}\Gamma(X, \mathcal{O}_X)$(6.2.7.5) is qcqs, so $f_*\mathcal{F}$ is Qco on $\operatorname{Spec}\Gamma(X,\mathcal{O}_X)$ by(6.5.1.6). Then the result follows from the fact $f^{-1}(\operatorname{Spec}(\Gamma(X, \mathcal{O}_X)_s)) = X_s$ and the definition of f_*. □

Lemma (6.5.1.8) [Extending Qco Sheaves]. Let $i : U \to X$ be a quasi-compact open immersion of schemes, $\mathcal{F}$ a Qco $\mathcal{O}_X$-module and $\mathcal{G} \subset \mathcal{F}|_U$ a Qco $\mathcal{O}_U$-submodule, then there exists a Qco $\mathcal{O}_X$-submodule $\mathcal{G}' \subset \mathcal{F}$ that $\mathcal{G}'|_U = \mathcal{G}$ ⌟

Proof: immersion is separated(6.4.4.86), so $i_*\mathcal{G}$ is a Qco $\mathcal{O}_X$-sheaf by(6.5.1.6), and it is a submodule of $i_*i^*\mathcal{F}$, so the kernel

$$\mathcal{H} = \ker(\mathcal{F} \oplus i_*\mathcal{G} \to i_*i^*\mathcal{F})$$

is also Qco by(6.5.1.3), and $\mathcal{H} \subset \mathcal{F}$, $\mathcal{H}|_U = \mathcal{G}$. □

Prop. (6.5.1.9) [Extending Qco Sheaves of F.T.]. Let X be a qcqs scheme, and $U \subset X$ a qc open subset, $\mathcal{F}$ a Qco $\mathcal{O}_X$-module and $\mathcal{G} \subset \mathcal{F}|_U$ a Qco $\mathcal{O}_U$-submodule of f.t., then there exists a Qco $\mathcal{O}_X$-submodule $\mathcal{G}' \subset \mathcal{F}$ of finite type that $\mathcal{G}'|_U = \mathcal{G}$. ⌟

Proof: Let n be the minimal number of affine open subsets U_i that $X = U \bigcup \cup U_i$, by induction on n, it suffices to prove for $n = 1$. Thus we may assume $X = U \cup V$ where U, V are affine opens. Now $U \cap V$ is qc because X is qs. Then we can change (X, U) to $(V, U \cap V)$, because we can glue the resulting sheaf. Then we reduce to the case X is affine.

Let $X = \operatorname{Spec} R$ and $\mathcal{F} = \widetilde{M}$, then by(6.5.1.8), there exists a Qco sheaf $\widetilde{N}$ that $\widetilde{N}|_U = \mathcal{G}$. By hypothesis we can cover U by f.m. open affine $D(f_i)$ that N_{f_i} is f.g., by element $x_{ij}/f_j^{n_i}$. Let N' be the submodule of N generated by these elements x_{ij}, then $\widetilde{N'}$ meets our requirement. □

Cor. (6.5.1.10) [Qco Sheaf is a Direct Union of Qco Sheaves of F.T.]. Let X be a qcqs scheme, then any Qco sheaf $\mathcal{F}$ on X is a direct colimit of its Qco subsheaves of f.t.. ⌟

Proof: It is a direct colimit because the sum of two Qco sheaves of f.t. is also Qco of f.t.. Now for any affine open $U \subset X$ and $s \in \mathcal{O}_X(U)$, s generates a Qco $\mathcal{O}_U$-submodule of f.t. of $\mathcal{F}|_U$, and by(6.5.1.9) this extends to a Qco $\mathcal{O}_X$-submodule of $\mathcal{F}$. Then we see that the direct colimit of Qco subsheaves of f.t. of $\mathcal{F}$ contains elements of $\mathcal{F}(U)$ for any affine open subset U, thus it is just $\mathcal{F}$. □

Def. (6.5.1.11) [Rank of Sheaves]. Let X be a scheme and $\mathcal{F}$ a Qco sheaf on X, $p \in X$, then the **rank of $\mathcal{F}$ at p** is $\mathrm{rank}_p(\mathcal{F}) = \dim_{k(p)} \mathcal{F}_p/\mathfrak{m}_p\mathcal{F}_p$. ⌟

Prop. (6.5.1.12) [Maximal Qco Submodule]. For X a scheme and any $\mathcal{O}_X$-module $\mathcal{F}$, there is a Qco submodule of $\mathcal{F}$ maximal among all Qco submodules of $\mathcal{F}$. This is because a direct colimit of Qco sheaves is Qco(6.5.1.3). ⌟

Prop. (6.5.1.13) [Integral and Finite Modules]. Let X be a qcqs scheme and $\mathcal{A}$ an integral Qco $\mathcal{O}_X$-submodule, then

- $\mathcal{A}$ is the directed colimits of its finite Qco $\mathcal{O}_X$-modules.
- $\mathcal{A}$ is a direct colimit of finite and finitely presented Qco $\mathcal{O}_X$-modules.

⌟

Proof: Cf.[Sta]0817. □

Def. (6.5.1.14). ?

- for a closed immersion $Y \to X$, there is $i^! : \mathfrak{QCoh}(X) \to \mathcal{Q}co(Y)$ that is right adjoint to i_*: $i^!\mathcal{G} = i^*((\mathcal{H}_Z(\mathcal{G}))')$, where $\mathcal{H}_Z(\mathcal{G})$ is the sheaf of sections annihilated by $\mathcal{I}$ and $\mathcal{F}'$ is the maximal Qco sheaf of $\mathcal{F}$.
- For f proper between locally Noetherian scheme, there is a inverse sheaf $f^!\mathcal{G} = \mathcal{H}om_Y(f_*\mathcal{O}_X, \mathcal{G})$, which maps $\mathcal{Q}co(Y)$ to $\mathfrak{QCoh}(X)$ by(6.5.1.33) and**??**. When f is affine, in particular when it is finite, then $f^!$ is right adjoint to f_* on Qco(6.8.6.13).

⌟

Associated Points

Def. (6.5.1.15) [Weakly Associated Points]. Let $X \in \mathfrak{Sch}$ and $\mathcal{F} \in \mathfrak{QCoh}(X)$, then a **weakly associated point of $\mathcal{F}$** is the set of points $x \in X$ that $\mathfrak{m}_x \subset \mathcal{O}_{X,x}$ is weakly associated to the module $\mathcal{F}_x$. The set of w.ass points are denoted by $\mathrm{WeakAsso}(\mathcal{F})$. The **weakly associated points of X** is the weakly associated points of $\mathcal{O}_X$.

Similarly we can stalkwise define the set of **associated points** of X. ⌟

Def. (6.5.1.16) [Embedded Points]. Let X be a scheme and $\mathcal{F}$ a Qco sheaf on X, then an **embedded point** of $\mathcal{F}$ is an associated point that is a specialization of another associated point. ⌟

Prop. (6.5.1.17) [Properties of Associated Points]. Let X be a scheme and $\mathcal{F}_i$ be Qco sheaves on X, then

1. $Ass(\mathcal{F}) \subset \mathrm{WeakAsso}(\mathcal{F}) \subset \mathrm{Supp}(\mathcal{F})$.
2. If $0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0$ is an exact sequence, then $WeakAss(\mathcal{F}_1) \subset WeakAss(\mathcal{F}_2)$, and $WeakAss(\mathcal{F}_2) \subset \mathrm{WeakAsso}(\mathcal{F}_1) \cup \mathrm{WeakAsso}(\mathcal{F}_3)$.
3. $WeakAss(\mathcal{F}) = \varnothing$ iff $\mathcal{F} = 0$.

4. The generic points of $\mathrm{Supp}(\mathcal{F})$ are in $\mathrm{WeakAsso}(\mathcal{F})$. In particular, generic points of X are in $WeakAss(X)$.
5. If X is locally Noetherian, then $Ass(\mathcal{F}) = \mathrm{WeakAsso}(\mathcal{F})$.
6. If X is reduced, then $\mathrm{WeakAsso}(X)$ is just the generic points of X. In particular, X has no embedded points.
7. If X is locally Noetherian, then an associated point is an embedded point iff it is not a generic point of $\mathrm{Supp}(\mathcal{F})$.
8. If X is locally Noetherian and $\mathcal{F}$ is coherent, then $\mathcal{F}$ has no embedded points iff it satisfies (S_1).
9. If X is locally Noetherian of dimension≤ 1, then X is C.M. iff it has no embedded points.

⌟

Proof: By(5.2.5.21), these reduces to the affine case, so they follows from

- (5.2.5.13)(5.2.5.16).
- (5.2.5.14).
- (5.2.5.16).
- (5.2.5.16).
- (5.2.5.21).
- (5.2.5.24).
- (5.2.5.23).
- [Sta]031Q.
- [Sta]0BXG.

□

Prop. (6.5.1.18). Let X be a scheme and $\mathcal{F} \in \mathfrak{QCoh}(X)$. If U is an open subset of X that contains $\mathrm{WeakAsso}(\mathcal{F})$, then $\Gamma(X,\mathcal{F}) \to \Gamma(U,\mathcal{F})$ is injective. ⌟

Proof: If $s \subset \Gamma(X,\mathcal{F})$ be a section that restricts to 0 on U, let $\mathcal{F}'$ be the subsheaf generated by s, then $WeakAss(\mathcal{F}') \subset \mathrm{WeakAsso}(\mathcal{F})$, but $\mathrm{Supp}(\mathcal{F}') \subset X\backslash U$, thus $WeakAss(\mathcal{F}') = 0$, so $\mathcal{F}' = 0$ by(6.5.1.17). □

Prop. (6.5.1.19) [Schematically Dense and Associated Points]. Let X be a locally Noetherian scheme and $U \subset X$ an open subset, then the following are equivalent:

- U is schematically dense in X.
- U is dense in X and contains all the embedded points of X.
- U contains $Ass(X)$.

⌟

Proof: The problem is local, so we assume $X = \mathrm{Spec}\, A$, then $2, 3$ are clearly equivalent.

Let $U = \cup_i D(f_i)$, then by(6.4.4.64), U is schematically dense in A iff $A \to \prod A_{f_i}$ is injective. If $\mathfrak{p} = Ann(x)$ for some $x \in A$, then x maps to some non-zero element of A_{f_i}, then $f_i \notin \mathfrak{p}$, so $\mathfrak{p} \subset D(f_i) \subset U$. Conversely, if $Ass(X) \subset U$, then every map $A \to A_\mathfrak{p}$ factors through $A \to A_{f_i}$ for some i, so injectivity of $A \to \prod_{\mathfrak{p}\in Ass(X)} A_\mathfrak{p}$ implies injectivity of $A \to \prod_i A_{f_i}$. □

Prop. (6.5.1.20). Let X be a scheme and $\varphi : \mathcal{F} \to \mathcal{G} \in \mathfrak{QCoh}(X)$ that $\mathcal{F}_x \to \mathcal{G}_x$ is injective for any $x \in WeakAss(\mathcal{F})$, then φ is injective. ⌟

Proof: The hypothesis says $WeakAss(\ker(\varphi)) = 0$, so $\ker(\varphi) = 0$ by(6.5.1.17). □

Fitting Ideals

Def. (6.5.1.21) [Fitting Ideals]. Let $X \in \mathfrak{Sch}$ and $\mathcal{F} \in \mathfrak{QCoh}^{\mathrm{ft}}(X)$, the **fitting ideal** of $\mathcal{F}$ is defined to be**?** Cf.[Sta]0C3C. ⌟

Locally Free Sheaves

Prop. (6.5.1.22) [Locally Free is Stalkwise]. $\mathcal{F} \in \mathfrak{QCoh}^{\mathrm{pf}}(X)$ is locally free iff its stalks are all free, by(5.3.1.7). ⌟

Def. (6.5.1.23) [Locally Free Sheaves]. Let $X \in \mathfrak{Sch}$ and $\delta : X \to \mathbb{N}$ a locally constant function, then the category of locally free sheaves of rank δ is denoted by $\mathfrak{Coh}^{\mathrm{free},\delta}(X)$. The category of locally free sheaves is denoted by $\mathfrak{Coh}^{\mathrm{free}}(X)$. ⌟

Prop. (6.5.1.24) [Locally Free Sheaves]. Suppose $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$ is an exact sequence of sheaves on a scheme X, then

- If $\mathcal{F}', \mathcal{F}''$ are both locally free, then so is $\mathcal{F}$.
- If $\mathcal{F}, \mathcal{F}'$ are both locally free of finite rank, then so is $\mathcal{F}'$.

⌟

Proof: Firstly of all in each case all sheaves are Qco by(6.5.1.3).

1: on an affine open $U = \operatorname{Spec} A \subset X$, the exact sequence is induced by $0 \to A^I \to \Gamma(U, \mathcal{F}) \to A^J \to 0$, so it splits and $\Gamma(U, \mathcal{F}) \cong A^{I+J}$ is free.

2: on an affine open $U = \operatorname{Spec} A \subset X$, the exact sequence is induced by $0 \to \Gamma(U, \mathcal{F}') \to A^m \to A^n \to 0$, where the map $A^m \to A^n$ is represented by a $n \times m$ matrix M. Then U is covered by open subsets U_i that some $n \times n$ minor of M is invertible. Then after a change of coordinates on each subset, $\mathcal{F}(U_i) \cong A^{m-n}$. □

Prop. (6.5.1.25). For a exact sequence $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$ in $\mathfrak{QCoh}^{\mathrm{free}}(X)$, there is a filtration of $\operatorname{Sym}^r \mathcal{F}$:

$$0 = \mathcal{G}^{r+1} \subset \mathcal{G}^r \subset \ldots \subset \mathcal{G}^0 = \operatorname{Sym}^r \mathcal{F}$$

that

$$\mathcal{G}^p / \mathcal{G}^{p+1} \cong \operatorname{Sym}^p \mathcal{F}' \otimes \operatorname{Sym}^{r-p} \mathcal{F}''.$$

⌟

Proof: On any affine open subset, choose a splitting of the exact sequence, then use coordinates. □

Prop. (6.5.1.26). For a exact sequence $0 \to \mathcal{F}' \to \mathcal{F} \to \mathcal{F}'' \to 0$ in $\mathfrak{Coh}^{\mathrm{free}}(X)$, there is a filtration of $\wedge^r \mathcal{F}$:

$$0 = \mathcal{G}^{r+1} \subset \mathcal{G}^r \subset \ldots \subset \mathcal{G}^0 = \wedge^r \mathcal{F}$$

that

$$\mathcal{G}^p / \mathcal{G}^{p+1} \cong \wedge^p \mathcal{F}' \otimes \wedge^{r-p} \mathcal{F}''.$$

In particular,

$$\wedge\mathcal{F}'\otimes\wedge\mathcal{F}''\cong\wedge\mathcal{F}.$$

and when $\mathcal{F}''\cong\mathcal{L}$ is a line bundle, there is an exact sequence

$$0\to\wedge^r(\mathcal{F}')\to\wedge^r(\mathcal{F})\to\wedge^{r-1}(\mathcal{F}')\otimes\mathcal{L}\to 0$$

⌟

Proof: On any affine open subset, choose a splitting of the exact sequence, then use coordinates. □

Prop. (6.5.1.27) [Perfect Pairing Wedge Product Sheaf]. Let $\mathcal{F}$ be a locally free sheaf of rank n, then there is a perfect pairing $\wedge^r\mathcal{F}\otimes\wedge^{n-r}\mathcal{F}\to\wedge\mathcal{F}$ which is a perfect pairing, i.e. it induces an isomorphism $\wedge^r\mathcal{F}\cong(\wedge^{n-r}\mathcal{F})^\vee\otimes\wedge\mathcal{F}$. ⌟

Proof: The map is natural, and the isomorphism can be seen at the level of stalls, by(6.2.3.11). □

Prop. (6.5.1.28). Let $0\to\mathcal{F}\to\mathcal{G}\to\mathcal{H}\to 0$ is an exact sequence in $\mathfrak{QCoh}(X)$ where $\mathcal{H}$ is a locally free sheaf, then for any Qco sheaf $\mathcal{E}$ of X, then for any Qco sheaf $\mathcal{E}$ on X, there is an exact sequence of sheaves

$$0\to\mathcal{H}om(\mathcal{H},\mathcal{E})\to\mathcal{H}om(\mathcal{G},\mathcal{E})\to\mathcal{H}om(\mathcal{F},\mathcal{E})\to 0.$$

In particular, $0\to\mathcal{H}^\vee\to\mathcal{G}^\vee\to\mathcal{F}^\vee\to 0$ is exact. ⌟

Proof: As $\mathcal{H}om(-,\mathcal{E})$ is left exact, it suffices to show the last one is surjective. This is local, so we may assume $0\to\mathcal{F}\to\mathcal{G}\to\mathcal{H}\to 0$ is $0\to M\to N\to A^n\to 0$, so this sequence splits, and the then $\mathcal{H}om(\mathcal{G},\mathcal{E})\to\mathcal{H}om(\mathcal{F},\mathcal{E})$ is surjective, by(6.5.1.3). □

Prop. (6.5.1.29) [Grothendieck]. Every object in $\mathfrak{Coh}^{\mathrm{free},r}(\mathbb{P}^1_k)$ is isomorphic to $\bigoplus_{i=1}^r\mathcal{O}(a_i)$ for a unique non-decreasing sequence of integers $a_1,\ldots,a_r$. ⌟

Proof: Use induction on r. The $r=1$ case follows from(6.5.3.16). For a general r, let $\mathcal{E}\in\mathfrak{Coh}^{\mathrm{free},r}(\mathbb{P}^1_k)$, then $\mathcal{E}(m)$ is generated by global sections for m large as $\mathcal{O}_{\mathbb{P}^1}$ is ample, and $H^0(\mathcal{E}(-m))=H^1(\mathcal{E}^\vee(m))=0$ by Serre duality and(6.7.2.5), so there is a maximal m s.t. there is a non-zero map $\mathcal{O}(m)\to\mathcal{E}$. The image of this map is also locally free and has degree$\geq m$ by(6.12.2.8), so it must has degree m and $\mathcal{O}_X(m)\to\mathcal{E}$ is injective by(6.12.2.8). Now the cokernel $\mathcal{F}$ is also locally free, because otherwise let $\mathcal{F}_{\mathrm{tor}}$ be the torsion part of $\mathcal{F}$(6.12.2.16), and let $\mathcal{N}$ be the inverse image of $\mathcal{F}_{\mathrm{tor}}$ in $\mathcal{E}$, then it is locally free thus invertible, and $\mathcal{O}(m)\hookrightarrow\mathcal{N}$, so $N=\mathcal{O}(m)$ by(6.12.2.8), and $\mathcal{F}_{\mathrm{tor}}=0$.

There is an exact sequence

$$0\to\mathcal{O}(-1)\to\mathcal{E}(-m-1)\to\mathcal{F}(-m-1)\to 0$$

which induces $H^0(\mathcal{E}(-m-1))=H^0(\mathcal{F}(-m-1))=0$ as $H^1(\mathbb{P}^1_k,\mathcal{O}(-1))=0$, so by induction hypothesis $\mathcal{F}=\oplus_{i=1}^{r-1}\mathcal{O}(a_i)$ and $a_i\leq m$. To show this sequence splits, notice $\mathrm{Ext}^1(\mathcal{F}(-m-1),\mathcal{O}(-1))=\oplus_{i=1}^{r-1}H^1(\mathcal{O}(m-a_i))=0$. □

Prop. (6.5.1.30) [Splitting Principal]. Let X be an integral scheme and $\mathcal{E}\in\mathfrak{Coh}^{\mathrm{free}}(X)$, then there exists a modification $X'\to X$ s.t. $f^*\mathcal{E}$ has a filtration by invertible sheaves. ⌟

Proof: Use induction on $\mathrm{rank}(\mathcal{E})$. If $\mathrm{rank}(\mathcal{E})\leq 1$, this is trivial, otherwise let $\mathrm{rank}(\mathcal{E})=r$, $P=\mathbf{P}(\mathcal{E})$, then $\pi:P\to X$ is proper and there is a canonical surjection $\pi^*\mathcal{E}\to\mathcal{O}_P(1)$, with kernel in $\mathfrak{Coh}^{\mathrm{free},r-1}(P)$. Let U be an open subset of X s.t. E is trivial, then $\pi^{-1}(U)\cong\mathbb{P}^{r-1}_U$. Let $s:U\to\mathbb{P}^{r-1}(U)$ be a section, and let X' be the scheme-theoretic closure of U, which is integral. Then $X'\to X$ is proper and thus a modification. Now $f^*\mathcal{E}$ has an invertible quotient, and we are done by induction hypothesis. □

Coherent Sheaves

Prop. (6.5.1.31) [$\mathfrak{Coh}(X)$]**.** The category of coherent sheaves on a scheme X is denoted by $\mathfrak{Coh}(X)$. When $\mathcal{O}_X \in \mathfrak{Coh}(X)$, $\mathfrak{Coh}(X) = \mathfrak{QCoh}^{\mathrm{pf}}(X)$(6.2.2.28).

In particular when X is locally Noetherian, $\mathfrak{Coh}(X) = \mathfrak{QCoh}^{\mathrm{ft}}(X)$. And the notion of coherence are used usually only when X is locally Noetherian.

(Quasi-)coherence is an affine local property by(6.2.2.30). $\mathfrak{QCoh}(X)$ is an Abelian category, by(6.2.2.28). ⌟

Lemma (6.5.1.32). If f is finite, then f_* maps coherent sheaves to coherent sheaves. ⌟

Proof: This is trivial. □

Prop. (6.5.1.33) [Proper Pushforward]. If f is a proper morphism between locally Noetherian schemes, then f_* maps coherent sheaves to coherent sheaves. ⌟

Proof: Immediate from Grothendieck's coherence theorem(6.7.4.11). □

Prop. (6.5.1.34) [Artin-Rees]. Let X be a Noetherian scheme, $\mathcal{F}$ a coherent $\mathcal{O}_X$-module, $\mathcal{G}$ a Qco subsheaf of $\mathcal{F}$, $\mathcal{I} \subset \mathcal{O}_X$ a Qco sheaf of ideals, then there exists some $c > 0$ that for all $n \geq c$

$$\mathcal{I}^{n-c}(\mathcal{I}^c\mathcal{F} \cap \mathcal{G}) = \mathcal{I}^n\mathcal{F} \cap \mathcal{G}.$$

⌟

Proof: Cover X by f.m. affine open subsets, then this follows from the affine case(5.2.2.13). □

Cor. (6.5.1.35) [Vanish Analytically]. Let X be a Noetherian scheme, $\mathcal{F}$ a coherent $\mathcal{O}_X$-module, for any element $f \in \bigcap_n \mathfrak{m}_x^n\mathcal{F}$, f vanishes at a nbhd of x. ⌟

Proof: This follows from the intersection theorem(5.2.2.14). □

Prop. (6.5.1.36) [Deligne]. On a Noetherian scheme X, let $\mathcal{F}$ be a Qco sheaf, $\mathcal{G}$ be a coherent sheaf and $\mathcal{I}$ be a Qco sheaf of ideals correspongding to Z, $U = X - Z$, then we have

$$\varinjlim \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{I}^n\mathcal{G}, \mathcal{F}) \cong \mathrm{Hom}_{\mathcal{O}_U}(\mathcal{G}|_U, \mathcal{F}|_U).$$

In particular,

$$\varinjlim \mathrm{Hom}_{\mathcal{O}_X}(\mathcal{I}^n, \mathcal{F}) \cong \Gamma(U, \mathcal{F}).$$

⌟

Proof: Cf.[Sta]01YB. □

Prop. (6.5.1.37) [Kleinmann]. If X is a Noetherian integral separated locally factorial scheme, then every coherent sheaf on X is a quotient of a finite locally free sheaf. ⌟

Proof: Cf.[Hartshorne P238].**?** □

Prop. (6.5.1.38) [Support of Modules]. For $X \in \mathfrak{Sch}$ and $\mathcal{F} \in \mathfrak{QCoh}^{\mathrm{ft}}(X)$, the support(6.2.2.2) $\mathrm{Supp}(\mathcal{F})$ is closed by(6.2.2.24).

For a flat morphism f, $\mathrm{Supp}(f^*(\mathcal{F})) = f^{-1}(\mathrm{Supp}\,\mathcal{F})$, by(6.2.2.18). ⌟

Proof: because affine locally, for a set of generators x_i of M, $\mathrm{Ann}(\mathcal{F}) = \cup \mathrm{Ann}(x_i)$, and $\mathrm{Ann}(x_i)$ is closed. □

Cor. (6.5.1.39). Any coherent sheaf on an integral scheme is locally free over a dense open subset. ⌟

Cor. (6.5.1.40)[Geometric Nakayama]. If $\mathcal{F} \in \mathfrak{QCoh}^{\mathrm{ft}}(X)$ and for some $p \in U \subset X$ and $a_1, \ldots, a_n \in \mathcal{F}(U)$ generate $\mathcal{F}_p \otimes k(p)$, then there is an affine nbhd $V \subset U$ that $a_1, \ldots, a_n$ generate $\mathcal{F}(V)$. ⌟

Cor. (6.5.1.41) [Upper-Semicontinuity of Ranks]. For a Qco sheaf $\mathcal{F}$ of f.t. over X, the rank function $p \mapsto \mathrm{rank}_p(\mathcal{F})$ is an upper semicontinuous function on X. ⌟

Proof: By Nakayama, $\varphi(y)$ is equal to the minimal number of generators of the $\mathcal{O}_y$-module $\mathcal{F}_y$. But these generators extends to a nbhd of y, so $\varphi \leq n$ on this nbhd. □

Def. (6.5.1.42)[Schematic Support]. Let X be a scheme and $\mathcal{F}$ a Qco sheaf of f.t. over X, then the **annihilating ideal** is the ideal $\mathcal{I} \subset \mathcal{O}_X$ that is affine-locally defined by $\mathrm{Ann}(\mathcal{F}(U)) \subset \mathcal{O}_X(U)$, and the **schematic support** $\mathrm{Supp}(\mathcal{F})$ of $\mathcal{F}$ is the closed subscheme of X corresponding to $\mathrm{Ann}(\mathcal{F})$. ⌟

Prop. (6.5.1.43). Let $\mathcal{F}$ be a Qco sheaf of f.t. over a reduced scheme that the rank function $\mathrm{rank}_p(\mathcal{F})$ is locally constant, then it is locally free. ⌟

Proof: Let $\mathrm{rank}_p(\mathcal{F}) = n$, by(6.5.1.38), for any $x \in X$, there exists an affine nbhd $U = \mathrm{Spec}\, A$ of x and a surjection $f : \mathcal{O}_U^n \to \mathcal{F}_U$. Consider the kernel of f. If $(r_1, \ldots, r_n)$ is in the kernel and $r_1 \neq 0$, then $r_1 \notin \mathfrak{p}$ for some prime $\mathfrak{p}$ of A, as A is reduced. Then $\mathrm{rank}_{x_\mathfrak{p}}(\mathcal{F}) < n$, contradiction. □

Torsion-Free Sheaves

Def. (6.5.1.44)[Torsion Sheaves]. Let X be an integral scheme, then a **torsion sheaf** is a Qco sheaf that its stalk at the generic point of X vanishes. Equivalently, for any affine open $U \subset X$, $\mathcal{F}(U)$ is a torsion $O_X(U)$-module. ⌟

Prop. (6.5.1.45). Any ⌟

Prop. (6.5.1.46). A torsion $\mathcal{O}_X$-module of f.t. on an integral scheme vanish on a dense open subset. ⌟

Prop. (6.5.1.47). For X integral, any $\mathcal{F} \in \mathfrak{QCoh}(X)$ factors as $0 \to \mathcal{F}_{\mathrm{tor}} \to \mathcal{F} \to \mathcal{F}_{tf} \to 0$, where $\mathcal{F}$ is a torsion sheaf(6.5.1.44) and $\mathcal{F}_{tf}$ is Qco and torsion-free. ⌟

Cor. (6.5.1.48). The subpresheaf $U \mapsto \{s \in \mathcal{F}(U) | s_\eta = 0\}$ is a sheaf, and it is also Qco as on an affine open $U \subset X$, it is just $\mathcal{F}(U)_{\mathrm{tor}}$. So the quotient is clearly Qco and torsion-free. ⌟

Devissage of Coherent Sheaves

Lemma (6.5.1.49). Let X be a Noetherian scheme and $\mathcal{F} \in \mathfrak{Coh}(X)$, let $\mathcal{I}$ be a sheaf of ideals that correspond to Z, then $\mathrm{Supp}(\mathcal{F}) \subset Z$ iff $\mathcal{I}^n \mathcal{F} = 0$ for some n. (This follows easily from Noetherian and(5.2.5.8)). ⌟

Lemma (6.5.1.50). Let X be a Noetherian scheme and $\mathcal{F} \in \mathfrak{Coh}(X)$ s.t. $\mathrm{Supp}(\mathcal{F}) = Z_1 \cup Z_2$ where Z_1, Z_2 are closed, then there is an exact sequence of coherent sheaves $0 \to \mathcal{G}_1 \to \mathcal{F} \to \mathcal{G}_2 \to 0$ that $\mathrm{Supp}(\mathcal{G}_i) \subset Z_i$. ⌟

Proof: Let $\mathcal{I}$ be the ideal defining the induced reduced structure of Z_2, we use the exact sequence $0 \to \mathcal{I}^n\mathcal{F} \to \mathcal{F} \to \mathrm{Coker} \to 0$ and use (6.5.1.49) on $X \backslash Z_2$ to find n large that $\mathrm{Supp}(\mathcal{I}^n\mathcal{F}) \subset Z_1$, and notice Coker has support in Z_2. □

Lemma (6.5.1.51). Let X be an integral scheme and $Z \subset X$ an integral closed subscheme with generic point Z. If $\mathcal{F} \in \mathfrak{Coh}(X)$ satisfies $\mathcal{F}_\xi$ is annihilated by $\mathfrak{m}_\xi$, then there exists some $r \geq 0$ and sheaf of ideals $\mathcal{I}$ on Z and an injection $i_*(\mathcal{I}^{\oplus r}) \hookrightarrow \mathcal{F}$ that is an isomorphism at ξ. ⌟

Proof: Cf.[Sta]01YE. □

Prop. (6.5.1.52). Let X be a Noetherian scheme and $\mathcal{F} \in \mathfrak{Coh}(X)$, then there is a filtration of coherent sheaves that the quotients are pushforward of ideal sheaves on integral subschemes of X. This is analogous to the filtration in the module case. ⌟

Proof: We consider the set of these counterexamples and their Supp, then use Noetherian induction. The minimal one Z is irreducible, otherwise from(6.5.1.50) we find a filtration for it. Let the ideal of sheaf of the induced reduced structure of Z be $\mathcal{I}$, then $\mathcal{I}^n\mathcal{F} = 0$ for some n by(6.5.1.49), then we may assume $\mathcal{I}\mathcal{F} = 0$. Then we use(6.5.1.51) to finish the proof. □

Cor. (6.5.1.53) [Basic Dévissage]. Let X be a Noetherian scheme and P be a property of coherent sheaves on X s.t.

(1) for an exact sequence of sheaves:$0 \to \mathcal{F}_1 \to \mathcal{F} \to \mathcal{F}_2 \to 0$, if $\mathcal{F}_i$ has P, then $\mathcal{F}$ has P.

(2) for any integral closed subscheme $i : Z \subset X$ and any Qco sheaf of ideals $\mathcal{I}$ on Z, P holds for $i_*\mathcal{I}$.

then P holds for any coherent sheaf of X. ⌟

Lemma (6.5.1.54). Cf.[Sta]01YH. ⌟

Prop. (6.5.1.55) [Dévissage of Coherent Sheaves I]. Let X be a Noetherian scheme and P be a property of coherent sheaves on X s.t.

(1) for an exact sequence $0 \to \mathcal{F}_1 \to \mathcal{F} \to \mathcal{F}_2 \to 0 \in \mathfrak{Coh}(X)$, if two of them have P, then the third also has P.

(2) For every integral closed subscheme Z of X with generic point ξ, there is a $\mathcal{G} \in \mathfrak{Coh}(X)$ that

 (a) $\mathrm{Supp}\,\mathcal{G} = Z$.

 (b) $\mathcal{G}_\xi \cong \mathcal{O}_X/\mathfrak{m}_x$.

 (c) P holds for $\mathcal{G}$.

Then P holds for every coherent sheaf on X. ⌟

Proof: Suppose otherwise, let Z be the minimal couterexample of item2 of(6.5.1.55). Then it is easily seen that P holds for any $\mathcal{F}$ with support strictly contained in $\mathbb{Z}$. Then take $\mathcal{G}$ as in item2, and let $0 \to i_*(\mathcal{I}^{\oplus r}) \hookrightarrow \mathcal{G} \to \mathrm{Coker} \to 0$, then Supp(Coker) is strictly contained in Z, and $r = 1$ by hypothesis, so $i_*(\mathcal{I})$. Then for any other sheaf of ideals $\mathcal{I}'$ on Z, if $\mathcal{I}'$ is supported on a smaller subscheme, then it has P, otherwise there are two exact sequences

$$0 \to i_*\mathcal{I} \to i_*(\mathcal{I} + \mathcal{I}') \to \mathcal{Q} \to 0,$$

$$0 \to i_*\mathcal{I}' \to i_*(\mathcal{I} + \mathcal{I}') \to \mathcal{Q} \to 0,$$

where $\mathcal{I}, \mathcal{Q}$ are supported on smaller subschemes, so P also holds for $\mathcal{I}'$. □

Prop. (6.5.1.56) [Dévissage of Coherent Sheaves II]. Let X be a Noetherian scheme and P be a property of coherent sheaves on X s.t.

(1) for an exact sequence of sheaves:$0 \to \mathcal{F}_1 \to \mathcal{F} \to \mathcal{F}_2 \to 0$, if $\mathcal{F}_i$ has P, then $\mathcal{F}$ has P.

(2) If $\mathcal{F}^{\oplus r}$ has P, then $\mathcal{F}$ has P.

(3) For every integral closed subscheme Z of X with generic point ξ, there is a $\mathcal{G} \in \mathfrak{Coh}(X)$ that

 (a) $\operatorname{Supp} \mathcal{G} = Z$.

 (b) $\mathcal{G}_\xi$ is annihilated by $\mathfrak{m}_\xi$.

 (c) For every sheaf of ideals $\mathcal{I}$ on X that $\mathcal{I}_\xi = \mathcal{O}_{X,\xi}$, there is a Qco subsheaf $\mathcal{G}' \subset \mathcal{I}\mathcal{G}$ that $\mathcal{G}'_\xi = \mathcal{G}_\xi$ and P holds for $\mathcal{G}'$.

Then P holds for every coherent sheaf on X. ⌟

Proof: Cf.[Sta]01YM. □

2 Projective Spaces

Prop. (6.5.2.1). For any graded ideal $I \subset S$, $V_+(I) = \varnothing$ iff $S_+ \subset \sqrt{I}$. ⌟

Proof: □

Def. (6.5.2.2) [Projective Schemes]. For a graded ring S, we have a scheme $\operatorname{Proj}(S)$ that consists of homogenous primes of S minus S_+ and the affine cover is $D(f) = \{p | f \notin p\}$, and $\mathcal{O}(D(f)) = \operatorname{Spec} S_{(f)}$, where $S_{(T)}$ is the degree zero part of $T^{-1}S$. It has $\mathcal{O}_p = S_{(p)}$. ⌟

Proof: Cf.[Sta]01M5**?** □

Cor. (6.5.2.3). For any graded ring S, $\operatorname{Proj}(S)$ is a separated scheme. ⌟

Proof: Check that for standard affine opens $D_+(f)$ and $D_+(g)$, $D_+(f) \cap D_+(g) = D_+(fg)$ is affine open, and $S_{(f)} \otimes_{\mathbb{Z}} S_{(g)} \to S_{(fg)}$ is surjective, which are both clear. □

Prop. (6.5.2.4) [Representing Functor of Projective Schemes]. Let S be a graded ring generated by S_1 over S_0, then $\operatorname{Proj}(S)$ represents the functor that maps a scheme Y to the set of pairs $(\mathcal{L}, \psi)$, where $\mathcal{L}$ is an invertible sheaf on Y, and $\psi : S \to \Gamma_*(Y, \mathcal{L})$ is a graded ring homomorphism that $\mathcal{L}$ is generated by the global sections $\psi(S_1)$, up to strict equivalences. ⌟

Proof: Cf.[Sta]01NA. □

Prop. (6.5.2.5) [Associated Qco Sheaves]. Let M be a graded S-module, then

- there is a unique Qco sheaf $\widetilde{M} \in \mathfrak{QCoh}(\operatorname{Proj}(S))$ s.t. $\Gamma(D_+(f), \widetilde{M}) = M_f$ and the restrictions are compatible with base changes..
- For a point $x \in \operatorname{Proj}(S)$ corresponding to a homogenous prime not containing S_+, $\widetilde{M}_x = M_{(p)}$.
- $M \mapsto \widetilde{M}$ is an exact functor from the category of graded S-modules to $\mathfrak{QCoh}(\operatorname{Proj}(S))$.
- There is a canonical ring map $S_0 \to \Gamma(\operatorname{Proj}(S), \mathcal{O}_{\operatorname{Proj}_S})$ and canonical S_0-module map $M_0 \to \Gamma(\operatorname{Proj}(S), \widetilde{M})$.

⌟

Proof: **?**

4: This follows from the fact short exact sequences can be checked on stalks, and item2. □

Cor. (6.5.2.6). There is a canonical morphism of schemes $\mathrm{Proj}(S) \to \mathrm{Spec}\, S_0$. ⌟

Prop. (6.5.2.7). If $X \subset \mathbb{P}^n_k$ is a closed subvariety disjoint from a d-dimensional subspace $L \subset \mathbb{P}^n_k$, then the projection $\pi : X \to \mathbb{P}^{n-d-1}$ with center L induces a finite map $X \to \pi(X)$. ⌟

Proof: Cf.[Shafarovich 1, P63]. □

Cor. (6.5.2.8). If $F_0, \ldots, F_s$ are forms of degree $m > 0$ on $\mathbb{P}^n_k$ having no common zero on a closed subvariety $X \subset \mathbb{P}^n$, then $\varphi(x) = [F_0(x), \ldots, F_s(x)]$ defines a finite map $\varphi : X \to \varphi(X)$. ⌟

Proof: Let $v_m : \mathbb{P}^n \to \mathbb{P}^N$ be the Veronese embedding of degree m, then $X \to v_m(X)$ is an isomorphism, and φ is a composition of v_m and a projection $\mathbb{P}^N_k \to \mathbb{P}^n_s$, thus it is a finite map, by(6.5.2.7). □

Prop. (6.5.2.9) [Tensor and Proj]. For two graded ring with the same $S_0 = A$, $\mathrm{Proj}(S \times_A T) \cong X \times_A Y$, where $(S \times_A T)_n = S_n \times_A T_n$ ⌟

Proof: □

Def. (6.5.2.10) [Relative Proj]. The **relative Proj** $\mathcal{S}$ over locally Noetherian Y of a Qco graded $\mathcal{O}_Y$-algebra $\mathcal{S}$ f.g. over $\mathcal{S}_0$ by coherent $\mathcal{S}_1$ is the glueing of locally $\mathrm{Proj}\, S$. $\mathrm{Proj}\, \mathcal{S} \to Y$ is locally projective thus proper. It is equipped with invertible sheaf $\mathcal{O}(1)$ by glueing. ⌟

Prop. (6.5.2.11) [Closed Subscheme of Projective Scheme]. The closed scheme of $X = \mathbb{P}^n_A$ corresponds to the saturated homogenous ideal $\mathcal{I}_Y$, (i.e. for any s, if there is an n that for any i, $x_i^n s \in \mathcal{I}_Y$, then $s \in I_Y$).

So projective scheme over $\mathrm{Spec}\, S_0$ corresponds to $\mathrm{Proj}\, S$, where S are f.g. over S_0 by S_1 saturated in the sense above. ⌟

Proof: A closed immersion is proper, thus the kernel $\mathcal{I}_Y$ of the structural map is a Qco(6.5.1.3), so it must be an ideal on every affine open, because Qco is affine local. Then we should use(6.5.3.6), $\Gamma_*(\mathcal{I}_Y)$ will suffice. Cf.[Hartshorne Ex2.5.10]. □

Prop. (6.5.2.12). The global section of a projective space $\mathrm{Proj}\, S \to \mathrm{Spec}\, S_0$ is just S_0, this is by(6.5.3.6). ⌟

Prop. (6.5.2.13). A quasi-projective scheme X over a field k of dimension r can be covered by $r+1$ open affine subsets. This is because there are r hyperplane that intersect X non-empty. This can happen by choosing a hyperplane non-intersecting the generic point of X, otherwise we choose many hyperplane, then their intersection is empty. ⌟

Sheaves on Proj

Def. (6.5.2.14) [Serre Twisting Sheaves]. Let S be a graded ring and $X = \mathrm{Proj}(S)$, there are Qco **Serre twisting sheaves** $\mathcal{O}_X(n) = \widetilde{S(n)}$. For $\mathcal{F} \in \mathfrak{QCoh}(\mathrm{Proj}(S))$, the **Serre twisting sheaf** of $\mathcal{F}$ is the sheaf $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(n)$.

⌟

Prop. (6.5.2.15). Let S be a graded ring and $X = \mathrm{Proj}(S)$,

1. there are canonical maps

$$\mathcal{O}_X(m) \otimes_{\mathcal{O}_X} \mathcal{O}_X(n) \to \mathcal{O}_X(m+n),$$

inducing a map of graded rings $S \to \Gamma_*(X, \mathcal{O}_X) = \oplus_{n \geq 0} \Gamma(X, \mathcal{O}_X(n))$.

2. For any $\mathcal{F} \in \mathcal{S}\mathrm{h}(\mathcal{O}_X)$, there are canonical maps
$$\mathcal{O}_X(n) \otimes_{\mathcal{O}_X} \mathcal{F} \to \mathcal{F}(n).$$
inducing a map of graded module structure of $\Gamma_*(X, \mathcal{O}_X)$ on $\Gamma_*(X, \mathcal{F}) = \oplus_{n\geq 0}\Gamma(X, \mathcal{F}(n))$.
3. There is a canonical map $\widetilde{\Gamma_*(X, \mathcal{F})} \to \mathcal{F}$ that is identity on global sections.
4. For any graded S-module M, let $M(n) = M \otimes_S S(n)$, there are maps $\widetilde{M}(n) \to \widetilde{M(n)}$. (Use property of Qco sheaves).
5. For graded rings M, N over S, there are canonical maps $\widetilde{M} \otimes_{\mathcal{O}_X} \widetilde{N} \to \widetilde{M \otimes_S N}$.

⌟

Proof: □

Prop. (6.5.2.16). Let S be a graded ring s.t. S is generated by S_1 over S_0, then
1. $(M \otimes_S N)_{(f)} \cong M_{(f)} \otimes_{S_{(f)}} N_{(f)}$ for $f \in S_1$.
2. There canonical maps in item1, 4, 5 of(6.5.2.15) are isomorphisms.
3. For a graded ring map $S \to T$, we have the corresponding Proj map $f : U \to T$ that $f^*(\widetilde{M}) \cong (\widetilde{M \otimes_S T})|_U$ and $f_*(\widetilde{N}|_U) \cong \widetilde{N_S}$. That's to say, $f^*(\widetilde{M}(n)) = f^*(\widetilde{M})(n)$ and $f_*(\widetilde{M}(n)) = f_*(\widetilde{M})(n)$.

⌟

Proof: 1:
2: By1 and check locally that tensoring f^n is an isomorphism on $D_+(f)$. □

Cor. (6.5.2.17). $\mathcal{O}_X(n) \otimes \mathcal{O}_X(m) \cong \mathcal{O}_X(n + m)$ for any scheme X projective over Y. ⌟

Prop. (6.5.2.18) [Twisting of Proj]. With notation as in (6.5.2.10), Let $S' = S * \mathcal{L} : S'_d = S_d \otimes \mathcal{L}^d$, then $\varphi : \operatorname{Proj} S' \to \operatorname{Proj} S$ is an isomorphism that induces
$$\mathcal{O}'(1) \cong \varphi^*\mathcal{O}(1) \otimes \pi'^*\mathcal{L}.$$

⌟

Prop. (6.5.2.19). If Y is Noetherian and admits an ample invertible sheaf, then by definition, we have $S_1 \otimes \mathcal{L}^n$ is base point free for some n, thus we have a morphism $\operatorname{Proj}(S * \mathcal{L}^n) \to \mathbb{P}^N_Y$, so $P = \operatorname{Proj} S$ is H-quasi-projective with $\mathcal{O}(1) = \mathcal{O}_P(1) \otimes \pi^*\mathcal{L}^n$. ⌟

Relative Projective Spaces

Def. (6.5.2.20) [Relative Projective Spaces]. ⌟

Def. (6.5.2.21)[Projective Bundles]. Let S be a scheme, $\pi : V \to S$ is called an **Qco vector bundle** if it is affine, and $\pi_*\mathcal{O}_V$ endowed with the structure of a graded $\mathcal{O}_S$-algebra structure $\pi_*\mathcal{O}_V = \oplus\mathcal{E}_n$, where $\mathcal{E}_0 = \mathcal{O}_S$, and $\operatorname{Sym}^n \mathcal{E}_1 \to \mathcal{E}_n$ is an isomorphism for any n. The category of Qco vector bundles on S is denoted by $\mathcal{V}\mathrm{ect}^{\mathcal{QC}\mathrm{oh}}(S)$.

A morphism of affine bundles is a map $E' \to E$ over S that the associated map $f_* : \pi_*\mathcal{O}_V \to \pi'_*\mathcal{O}_{V'}$ is compatible with grading.

For $\mathcal{E} \in \mathfrak{QCoh}(X)$, we can define the **associated vector bundle** $V(\mathcal{E})$ as $\mathbf{Spec}_S \operatorname{Sym}(\mathcal{E})$(6.2.3.10)(6.2.7.12). In this way, the category of Qco vector bundles over S is anti-equivalent to the category of Qco $\mathcal{O}_S$-algebras.

For $\mathcal{E} \in \mathfrak{QCoh}(X)$, we can define the **associated projective bundle** $\mathbf{P}(\mathcal{E})$ as $\mathbf{Proj}_S \operatorname{Sym}(\mathcal{E})$(6.2.3.10)(6.2.7.12). It is equipped with a Serre twisting sheaf $\mathcal{O}(1)$, which is the glue of locally the Serre sheaf in projective space. There is a surjective morphism $\pi^*(\mathcal{E}) \to \mathcal{O}(1)$ (local check).

⌟

Prop. (6.5.2.22). Let $g: Y \to X$ by a scheme over X, a morphism $Y \to \mathbf{P}(\mathcal{E})$ over X is equivalent to an invertible sheaf $\mathcal{L}$ on Y and a surjective map $g^*\mathcal{E} \to \mathcal{L}$.

In particular, giving a morphism $X \to \mathbf{P}^n_A$ is equivalent to a base point free invertible sheaf with n generators on X. ⌟

Proof: If there is a morphism, it will pullback $\pi^*(\mathcal{E}) \to \mathcal{O}(1)$ into $g^*\mathcal{E} \to \mathcal{L}$. For the coverse, construct locally and glue, we have the natural morphisms $A[x_1/x_i, \ldots, x_n/x_i] \to \mathcal{O}_{X_{s_i}} : x_j/x_i \to s_j/s_i$ in a homogenous sense. It is natural hence glue together. For the module, maps $x_i \to s_i$. □

Cor. (6.5.2.23). All automorphisms of $\mathbb{P}^n_k$ is linear. ⌟

Proof: The Picard group of $\mathbb{P}^n_k$ is $\mathbb{Z}$ and is generated by $\mathcal{O}(1)$(6.5.3.16), so the automorphism will map $\mathcal{O}(1)$ to $\mathcal{O}(\pm 1)$ and $\mathcal{O}(-1)$ has no global section(6.5.3.5). And the globals section is n-dimensional and determines the morphism by the prop. □

Def. (6.5.2.24) [Projective Space]. Let A be a ring, the **projective space** $\mathbb{P}^n_A$ is defined to be

$$\mathbf{P}^n_A = \operatorname{Proj}(A[T_0, \ldots, T_n])$$

with $\deg(T_i) = 1$. It represents the functor that maps a scheme T to the equivalence classes of pairs $(\mathcal{L}, (s_0, \ldots, s_n))$, where $\mathcal{L}$ is an invertible sheaf on T, and $s_0, \ldots, s_n \in \Gamma(T, \mathcal{L})$ that generate $\mathcal{L}$ by(6.5.2.22). For any scheme S, $\mathbf{P}^n \times_{\mathbb{Z}} S$ is called the projective space over S. ⌟

Prop. (6.5.2.25). Let R be a ring and $X = \mathbb{P}^n_R$, $\mathcal{F} \in \mathfrak{QCoh}(X)$, then the canonical map $\widetilde{\Gamma_*(X, \mathcal{F})} \to \mathcal{F}$(6.5.2.15) is an isomorphism. ⌟

Proof: Cf.[Sta]03GM.**?** This is a corollary. □

Prop. (6.5.2.26) [Closed Subschemes of $\mathbb{P}^n_R$]. Let Z be a closed subscheme of $\mathbb{P}^n_R$, then it is of the form

$$Z = \operatorname{Proj}(R[X_0, \ldots, X_n]/I) \subset \operatorname{Proj}(R[X_0, \ldots, X_n])$$

where $I = \oplus I_n$ and $I_n = \ker(R[X_0, \ldots, X_n]_d \to \Gamma(Z, \mathcal{O}_Z(d)))$. ⌟

Proof: Cf.[Sta]03GI.**?** □

Prop. (6.5.2.27) [Segre Embedding]. Let S be a scheme, there is a natural closed immersion

$$\mathbf{P}^m_S \times_S \mathbf{P}^n_S \to \mathbf{P}^{mn+m+n}_S$$

called the **Segre embedding**. ⌟

Proof: It suffices to a prove for $S=\mathbb{Z}$, and in this case, it suffices to write down an invertible sheaf on $\mathbf{P}^m_S\times_S\mathbf{P}^n_S$ with $(n+1)(m+1)$ global sections that generate it. Then we take the invertible sheaf $\mathcal{L}=\pi_1^*\mathcal{O}_{\mathbf{P}^m}(1)\otimes\pi_2^*\mathcal{O}_{\mathbf{P}^n}(1)$. and the sections X_iY_j, where $(X_0,\ldots,X_m)$ generate $\mathcal{O}_{\mathbf{P}^m}(1)$ and $(Y_0,\ldots,Y_n)$ generate $\mathcal{O}_{\mathbf{P}^n}(1)$.

It is a closed immersion by[Sta]01WD.**?** □

Prop. (6.5.2.28) [Venerose Embedding]. ⌟

3 Invertible Sheaves

General invertible sheaves on a ringed site is treated in5.

Prop. (6.5.3.1) [Faithfully Flat Descent]. To show a quasi-coherent sheaf is a line bundle, it suffices to show fpqc-locally, by(5.4.2.1). ⌟

Def. (6.5.3.2) [Basepoint-Freene Line Bundles]. Let $\mathcal{L}$ be a line bundle over a scheme X over a field k, then it is called **basepoint free** if the intersections $\{\mathrm{div}(s)|s\in H^0(V)\}$ is empty. ⌟

Prop. (6.5.3.3). If X is qcqs over a field k and K/k is a field extension, then $\mathcal{L}$ is basepoint free iff $\mathcal{L}_K$ is basepoint free over X_K. ⌟

Proof: By flat base change(6.7.5.1), $H^0(X_K,\mathcal{L}_K)=H^0(X,\mathcal{L})\otimes_k K$. □

Prop. (6.5.3.4) [Relative Triviality]. Let $f:X\to Y$ be a finite morphism of schemes and $\mathcal{L}\in\mathrm{Pic}(X)$, then for any $y\in Y$, there exists a nbhd U of $y\in Y$ s.t. $\mathcal{L}|_{f^{-1}(U)}$ is trivial. ⌟

Proof: Cf.[Sta]0BUT. □

Prop. (6.5.3.5) [Global Sections]. Let $\mathcal{L}$ be an invertible sheaf over qcqs scheme X, for $\mathcal{F}\in\mathfrak{QCoh}(X)$, let the **global section functor** $\Gamma_*(\mathcal{F})=\oplus\Gamma(X,\mathcal{F}\otimes\mathcal{L}^n)$, then

$$\Gamma_*(\mathcal{F})_{(f)}\cong\mathcal{F}(X_f).$$

where $s\in\Gamma(X,\mathcal{L})$. In particular that if there is a section f of $\mathcal{F}$ on X_s, then for some n, $f\otimes s^n$ is a global section of $\mathcal{F}\otimes\mathcal{L}^n$. ⌟

Proof: This is nearly the same as the proof that $(\mathrm{Spec}\,A)_f=\mathrm{Spec}\,A_f$, Cf.[Sta]01PW.**?** □

Cor. (6.5.3.6). When $X=\mathrm{Proj}\,S$ projective over $\mathrm{Spec}\,S_0$ and $\mathcal{F}\in\mathfrak{QCoh}(X)$, $\widetilde{\Gamma_*(\mathcal{F})}\cong\mathcal{F}$, where $\Gamma_*(\mathcal{F})=\oplus_{n\in\mathbb{Z}}\Gamma(X,\mathcal{F}(n))$, which is a graded S-module. In particular, Γ_* for projective space $\mathbb{P}^n_A$ equals $A[x_1,\ldots,x_n]$. ⌟

Def. (6.5.3.7) [Regular Sections]. ⌟

Prop. (6.5.3.8) [Complete Series]. Let $H^0(X,\mathcal{L})$ be the sections that corresponds to injective maps $\mathcal{L}^{-1}\to\mathcal{O}_X$, then there is a canonical isomorphism

$$H^0(X,\mathcal{L})_{reg}/H^*(X,\mathcal{O}_X^*)\cong|\mathcal{L}|.$$

Notice when X is not integral, $H^0(X,\mathcal{L})_{reg}$ may not equal $H^0(X,\mathcal{L})$. ⌟

Proof: Cf.[Kle05]P22. □

Prop. (6.5.3.9) [Meromorphic Sections]. Let X be a locally Noetherian scheme having no embedded points, then every invertible sheaf $\mathcal{L}\in\mathrm{Pic}(X)$ has a meromorphic section. In particular, this applies for X integral, by(6.5.1.17). ⌟

Proof: Cf.[Sta]0EMI. □

Picard Groups

Remark (6.5.3.10) [Picard Groups]. The Picard group $\mathrm{Pic}(X)$ of a local ringed space $(X, \mathcal{O}_X)$ is defined in(6.2.5.7), and it is isomorphic to $H^1(X, \mathcal{O}_X^*)$ by(6.3.1.17). ⌟

Prop. (6.5.3.11) [Class Group]. If $X = \mathrm{Spec}\,\mathcal{O}$ where $\mathcal{O}$ is a Dedekind domain, then by(5.2.7.8), the isomorphism class of invertible sheaves on X is equivalent to the isomorphism class of fractional ideals modulo principle ideals. Thus $\mathrm{Pic}(\mathcal{O})$ equals the class group of $\mathcal{O}$(5.2.7.9). In particular, if R is a UFD, then $\mathrm{Pic}(\mathrm{Spec}\,R) = 0$. ⌟

Def. (6.5.3.12) [Invertible Sheaf Associated to Cartier Divisors]. For a Cartier divisor on a scheme X, we can define $\mathcal{O}(D)$ the **Line bundle associated to** D as the sub $\mathcal{O}_X$-module of $\mathcal{K}$ locally generated by (f_i^{-1}), where $D = (f_i)$ locally. Equivalently, it is the line bundle $\mathcal{I}_D^{-1}$. ⌟

Def. (6.5.3.13) [Linear Series]. Let $\mathcal{L} \in \mathrm{Pic}(X)$, then denote $|\mathcal{L}|$ the **complete linear series** of effective Cartier divisors D s.t. $\mathcal{L}(D) \cong \mathcal{L}$. ⌟

Def. (6.5.3.14) [Weil divisor of an invertible Sheaf]. For X a locally Noetherian integral scheme and $\mathcal{L}$ an invertible sheaf in $\mathcal{K}$, if $s \in \Gamma(X, \mathcal{K} \otimes \mathcal{L})$ is a meromorphic section of $\mathcal{L}$(which exists by(6.5.3.9)), for any prime Weil divisor Z with generic pt η, define $\mathrm{ord}_Z(s) = \mathrm{ord}_{\mathcal{O}_{X,\eta}}(s/s_\eta)$(5.1.2.10), for any s_η a generator of $\mathcal{L}_\eta$ over $\mathcal{O}_{X,\eta}$. This is independent of s_η chosen.

The prime Weil divisors that $\mathrm{ord}_Z(s) \neq 0$ is locally finite, the same as in(8.1.2.18). And any two different sections s_i defines Weil divisors up to a difference of $\mathrm{div}(f)$(8.1.2.18). So we can define the **Weil divisor class associated to** $\mathcal{L}$ as $\sum \mathrm{ord}_Z(s)[Z]$ for any meromorphic section s of $\mathcal{L}$.

It is easy to verify that this induces a homomorphism from $\mathrm{Pic}(X)$ to $\mathrm{Cl}(X)$. ⌟

Prop. (6.5.3.15) [Cl-Pic]. For a normal integral locally Noetherian scheme, the above map $\mathrm{Pic}(X) \to \mathrm{Cl}(X)$(6.5.3.14) is an injection. It is an isomorphism iff all local rings of X are UFD.

Explicitly, the inverse image of a prime Weil divisor D is the sheaf $\mathcal{O}_X(D) = \mathcal{H}om(\mathcal{I}_D, \mathcal{O}_X) = \mathcal{I}_D^{-1}$, and there is an exact sequence of sheaves on X:

$$0 \to \mathcal{O}_X(-D) = \mathcal{I}_D \to \mathcal{O}_X \to i_* \mathcal{O}_D \to 0$$

In particular, this applies to non-singular prevarieties over a field k, by(6.4.2.9). ⌟

Proof: If it is not injective, then some meromorphic section on $\mathcal{L}$ has no associated Weil divisors, then it suffices to show $\mathcal{L}$ is trivialized by s. Consider on an affine subscheme $\mathrm{Spec}\,A$, then $\mathrm{ord}_{A_\mathfrak{p}}(s) = 0$ for each minimal prime $\mathfrak{p}$ of A, but $A_\mathfrak{p}$ is DVR by(5.3.5.20), so $s \in A_\mathfrak{p}^*$ for each minimal prime $\mathfrak{p}$, so $s \in A^*$ by(5.3.5.11). This shows s trivialize $\mathcal{L}$.

To show it is surjective, it suffices to show any Weil divisor D is in the image: notice D is an effective Cartier divisor by(6.8.1.4), and by definition(6.8.1.5) the vanishing of the canonical section $1_D \in \mathcal{O}_X(D)$ is exactly D. □

Prop. (6.5.3.16) [Examples of Picard Groups].

- If X is a locally Noetherian normal integral separated scheme, then so are $X \times \mathrm{Spec}\,\mathbb{Z}[T]$ and $\mathbb{P}^n_X$, and $\mathrm{Cl}(X \times \mathrm{Spec}\,\mathbb{Z}[T]) = \mathrm{Cl}(X)$ and $\mathrm{Cl}(\mathbb{P}^n_X) = \mathbb{Z} \oplus \mathrm{Cl}(X)$.
- For a UFD R, $\mathrm{Pic}(\mathbb{A}^n_R) \cong \mathrm{Cl}(\mathbb{A}^n_R) = 0$.
- For a UFD R, $\mathrm{Pic}(\mathbb{P}^n_R) \cong \mathrm{Cl}(\mathbb{P}^n_R) \overset{\deg}{\cong} \mathbb{Z}$, and it is generated by $\mathcal{O}_{\mathbb{P}^n_R}(1)$.
- For any UFD R, $\mathrm{Pic}(\mathbb{P}^1_R \times \mathbb{P}^1_R) \cong \mathrm{Cl}(\mathbb{P}^1_R \times \mathbb{P}^1_R) \cong \mathbb{Z} \oplus \mathbb{Z}$.

- If k is a field and $Y\subset\mathbb{P}^n_k$ is a hypersurface of degree d, then $\mathrm{Pic}(\mathbb{P}^n_k\backslash Y)\cong\mathrm{Cl}(\mathbb{P}^n_k\backslash Y)\cong\mathbb{Z}/d\mathbb{Z}$. ⌟

Proof: By(6.5.3.15) and(8.1.5.7)(8.1.7.10)(8.1.5.8)(8.1.5.9). □

Prop. (6.5.3.17). Let X be a complete prevariety over a field k of characteristic $p>0$, then for any n prime to p and any purely inseparable field extension k'/k, the natural map

$$\mathrm{Pic}(X)[n]\to\mathrm{Pic}(X_{\overline{k}})[n]$$

is an isomorphism. ⌟

Proof: Cf.[Sta]0CD5. □

4 Ample Invertible Sheaves

Prop. (6.5.4.1). Let $X\in\mathcal{S}\mathrm{ch},\mathcal{L}\in\mathrm{Pic}(X),s\in\Gamma(X,\mathcal{L})$, then for any affine open $U\subset X$, $X_s\cap U$ is affine. ⌟

Proof: It suffices to show: If R is a ring, N is an invertible R-module and $s\in N$, then $U=\{\mathfrak{p}|s\notin\mathfrak{p}N\}$ is an affine open subset of $\mathrm{Spec}\,R$. For this, let $R'=\varinjlim_{-\otimes s}N^{\otimes n}$, then in fact $U=\mathrm{Spec}\,R'$. Because locally, R' is just R_s via an isomorphism $N_f\cong R_f$. □

Def. (6.5.4.2) [Ample Invertible Sheaves]. On a quasi-compact scheme X, an **ample invertible sheaf** is a line bundle $\mathcal{L}\in\mathrm{Pic}(X)$ s.t. there is some $n\in\mathbb{Z}_+$ and sections $s_i\in\Gamma(X,\mathcal{L}^n)$ that X_{s_i} is an affine cover of X. In particular, an ample invertible sheaf is globally generated.

For a qc morphism $f:X\to Y$, an invertible sheaf on X is called (relatively)**f-ample** iff it is ample restricted to every open subscheme $f^{-1}(V)$, where V is an affine open in Y. In particular, an invertible sheaf $\mathcal{L}$ on a quasi-compact scheme X is ample iff it is f-ample where $f:X\to\mathrm{Spec}\,Z$. ⌟

Prop. (6.5.4.3). For $m\in\mathbb{Z}_+$, an invertible sheaf $\mathcal{L}$ is (f-)ample iff $\mathcal{L}^m$ is (f-)ample. ⌟

Proof: □

Prop. (6.5.4.4) [Ample Implies Separatedness]. When there is a f-ample invertible sheaf for $f:X\to Y$ qc, then f is separated. In particular, if $X\in\mathcal{S}\mathrm{ch}_{qc}$ has an ample invertible sheaf, then X is separated. ⌟

Proof: [Sta]09MP.**?** □

Prop. (6.5.4.5) [Characterizing Ampleness]. Let $X\in\mathcal{S}\mathrm{ch}_{qc},\mathcal{L}\in\mathrm{Pic}(X),S=\Gamma_*(X,\mathcal{L})$, then the following are equivalent:

1. $\mathcal{L}$ is ample.
2. The open subsets X_s, where $s\in\Gamma_*(X,\mathcal{L})$ homogeneous, cover X, and the associated morphism $X\to\mathrm{Proj}\,S$ is an open immersion.
3. The open subsets X_s where $s\in\Gamma_*(X,\mathcal{L})$ homogeneous, form a topological basis for X.
4. The affine open subsets of the form X_s where $s\in\Gamma_*(X,\mathcal{L})$ homogeneous, form a topological basis for X.
5. For any $\mathcal{F}\in\mathcal{QC}\mathrm{oh}(X)$, the sum of images of the canonical maps $\Gamma(X,\mathcal{F}\otimes\mathcal{L}^n)\otimes\mathcal{L}^{\otimes -n}\to\mathcal{F}$ is surjective.

6. X is quasi-separated, and for any $\mathcal{F}\in\mathfrak{QCoh}^{\mathrm{ft}}(X)$, $\mathcal{F}\otimes\mathcal{L}^{\otimes n}$ is generated by global sections for n sufficiently large.
7. X is quasi-separated, and for any $\mathcal{F}\in\mathfrak{QCoh}^{\mathrm{ft}}(X)$, there exists $n\in\mathbb{Z}$ s.t. $\mathcal{F}$ is a quotient of a direct sum of f.m. copies of $\mathcal{L}^{\otimes -n}$.

⌟

Proof: Cf.[Sta]01Q3.? □

Cor. (6.5.4.6). The pullback of an ample invertible sheaf along a qc immersion is still ample. ⌟

Cor. (6.5.4.7). Let S be a quasi-separated scheme and X,Y be schemes over S. If $\mathcal{L}$ is an ample invertible sheaf over X and $\mathcal{N}$ an ample invertible sheaf over Y, then $\mathcal{M}=\mathrm{pr}_1^*\mathcal{L}\otimes_{\mathcal{O}_{X\times_S Y}}\mathrm{pr}_2^*\mathcal{N}$ is ample over $X\times_S Y$. ⌟

Proof: Because $X\times_S Y\to X\times Y$ is a qc immersion, by(6.5.4.6), it suffices to show for $S=\operatorname{Spec}Z$. Then if X_s is an affine nbhd of x and Y_t is an affine nbhd of Y, then $(X\times Y)_{\pi_1^*s\otimes\pi_2^*t}$ is an affine nbhd of $x\times y$. □

Cor. (6.5.4.8) [Tensor Product of Ample Invertible Sheaves is Ample]. Let $X\in\mathcal{S}\mathrm{ch},\mathcal{L},\mathcal{M}\in\operatorname{Pic}(X)$. If $\mathcal{M}$ is globally-generated and $\mathcal{L}$ is ample, then $\mathcal{L}\otimes\mathcal{M}$ is ample. In particular if $\mathcal{L},\mathcal{M}$ are ample invertible sheaves, then $\mathcal{L}\otimes\mathcal{M}$ is ample. ⌟

Proof: For any $x\in X$ and U a nbhd of x, choose $s\in\Gamma(X,\mathcal{L}^n)$ that $x\in X_s\subset U$, and choose $t\in\Gamma(X,\mathcal{M})$ that $t_x\neq 0$, then $x\in X_{s\otimes t^n}\subset U$, thus X_r form a basis for X where $r\in\Gamma(X,(\mathcal{L}\otimes\mathcal{M})^n)$, so $\mathcal{L}\otimes\mathcal{M}$ is ample. □

Cor. (6.5.4.9). Let $X\in\mathcal{S}\mathrm{ch},\mathcal{L},\mathcal{M}\in\operatorname{Pic}(X)$. If $\mathcal{L}$ is ample, then $\mathcal{M}\otimes\mathcal{L}^{\otimes n}$ is ample for n sufficiently large. ⌟

Proof: This is because $\mathcal{L}\otimes\mathcal{M}^n$ is generated by global sections for n sufficiently large, thus $\mathcal{L}\otimes\mathcal{M}^{n+1}$ is ample, by(6.5.4.8). □

Prop. (6.5.4.10) [Gluing Ample Invertible Sheaves]. Let $X\in\mathcal{S}\mathrm{ch}_{qc}$ s.t. there is an affine open covering of the form X_{s_i} where s_i are sections of $\mathcal{L}_i$ and $\mathcal{L}_i$ are globally generated line bundles in $\operatorname{Pic}(X)$, then X has an ample line bundle. ⌟

Proof: Let X_{s_i} be an affine open covering of X where s_i are sections of globally generated invertible sheaves $\mathcal{L}_i$, $i=1,\ldots,r$. As $\mathcal{L}_i$ are globally generated, let $X=\cup_j X_{t_{ij}}$ for $j=0,1,\ldots,m_i$ where $t_{i0}=s_i$. Then for the line bundle $\otimes_i\mathcal{L}_i$, the sections $t_{1,j_1}\otimes\ldots\otimes t_{r,j_r}$ where at least one of j_i equals 0, covers X, and they are all affine by(6.5.4.1). So $\otimes_i\mathcal{L}_i$ is ample. □

Prop. (6.5.4.11). $f:X\to Y$, let $\mathcal{L}$ be f-ample on X and $\mathcal{M}$ ample on Y, then $\mathcal{L}\otimes f^*\mathcal{M}^n$ is ample for n large. ⌟

Proof: Cf.[Sta]0892? □

Cor. (6.5.4.12). If $f:X\to Y$ is quasi-affine, then the pullback of an ample invertible sheaf is ample, by(6.4.4.19) and(6.5.4.3). ⌟

Prop. (6.5.4.13) [Pullback of Ampleness]. If $f:Y\to X$ is finite and surjective morphism between schemes proper over a Noetherian affine scheme, then for any invertible sheaf $\mathcal{L}$ on X, $\mathcal{L}$ is ample iff $f^*\mathcal{L}$ is ample. ⌟

Proof: Cf.[Sta]0B5V.?

One direction follows from(6.5.4.12), For the other we use Serre criterion(6.7.2.8) and devissage(6.5.1.56). We only verify 3: By(6.4.4.42), there exists such coherent sheaf $f_*\mathcal{F}$ for any integral subscheme, and for a any Qco sheaf of ideals $\mathcal{I}$, $\mathcal{I}f_*\mathcal{F} = f_*(f^{-1}\mathcal{I}\mathcal{F})$ because f is affine, thus

$$H^p(X, \mathcal{I}f_*\mathcal{F}) = H^p(X, f_*(f^{-1}\mathcal{I}\mathcal{F} \otimes \mathcal{L}^n)) = H^p(Y, f^{-1}\mathcal{I}\mathcal{F} \otimes \mathcal{L}^n)$$

by projection formula, and f is affine. This vanish for n large. □

Cor. (6.5.4.14) [Ampleness and Irreducible Components]. Let X be a scheme proper over a Noetherian affine scheme, then an invertible sheaf $\mathcal{L}$ on X is ample iff it is ample on the induced reduced structure of irreducible components of X. ⌟

Proof: This is(6.5.4.13) applied to the case $\coprod_i X_i \to X$. □

Prop. (6.5.4.15) [Ampleness Restricted to Reduced Case]. If $i: Z \to X$ is a closed immersion of schemes that induce homeomorphism on the underlying topology, then $\mathcal{L}$ is ample iff $i^*\mathcal{L}$ is ample.

In particular, this applies to $X_{\text{red}} \to X$. ⌟

Proof: Cf.[Sta]09MW.? □

Prop. (6.5.4.16). Let $f: X \to Y$ be a proper morphism of schemes and $\mathcal{L}$ an invertible sheaf on X. If $y \in Y$ satisfies $\mathcal{L}_y$ is ample on X_y, then there is a nbhd U of $y \in Y$ that $\mathcal{L}|_{f^{-1}(U)}$ is f-ample. ⌟

Proof: Cf.[Sta]0D2S. □

Prop. (6.5.4.17) [Ampleness is Fiberwise]. For $f: X \to T \in \mathcal{S}\text{ch}$ proper and $\mathcal{L} \in \text{Pic}(X)$, $\mathcal{L}$ is f-ample iff for any $t \in T$, $\mathcal{L}_t$ is ample over X_t. ⌟

Proof: [Positivity in Algebraic Geometry]P97.? □

Prop. (6.5.4.18)[Finite Map and Ample]. Let $\mathcal{L}$ be a basepoint-free line bundle on a proper scheme X, then the associated map $X \to P\Gamma(X, \mathcal{L})$ is finite iff $\mathcal{L}$ is ample. ⌟

Proof: Cf.[Positivity in Algebraic Geometry, P28]. □

Prop. (6.5.4.19) [Ampleness is Étale-Local]. Ampleness satisfies étale descent. Cf.[Sta]0D35.? ⌟

Prop. (6.5.4.20). Let X be a scheme. Let $\mathcal{L}$ be an ample invertible $\mathcal{O}_X$-module. Let n_0 be an integer. If $H^p(X, \mathcal{L}^{-n}) = 0$ for $n \geq n_0$ and $p > 0$, then X is affine. ⌟

Proof: Cf.[Sta]0EBD. □

Prop. (6.5.4.21) [Gluing Ample Line Bundles]. Let $K/k \in \texttt{Field}, X \in \mathcal{S}\text{ch}/k$ s.t. X_K has an ample line bundle, then X also has an ample line bundle. ⌟

Proof: Cf.[Sta]0BDC. □

Very Ample Invertible Sheaves

Def. (6.5.4.22) [Very Ampleness]. Let $f : X \to S$ be a morphism, a ***f*-very ample** invertible sheaf on X is the pullback of $\mathcal{O}(1)$ along some immersion $X \to \mathrm{Proj}(\mathcal{E})$ for some Qco module $\mathcal{E}$ over Y, Cf.(6.5.2.14). It is called **H-very ample** iff $\mathcal{E}$ is trivial. Notice when X is proper, this immersion must be closed by(6.4.5.3).

When S is affine and $f : X \to S$ is of f.t., f-very ample is equivalent to H-very ample. ⌟

Proof: Cf.[Sta]02NP. □

Prop. (6.5.4.23) [Tensor Product of Very Ample Line Bundles]. Let $f : X \to \mathrm{Spec}\, A$ be a morphism. If $\mathcal{L}$ is H-very ample and $\mathcal{M}$ is generated by global sections, then $\mathcal{L}\otimes\mathcal{M}$ is H-very ample. In particular, the tensor product of two H-very ample invertible sheaves is H-very ample. ⌟

Proof: The hypothesis means $\mathcal{L} = \varphi^*\mathcal{O}(1)$, where $\varphi : X \to \mathbb{P}^n_A$ is an immersion, and $\mathcal{M} = \psi^*\mathcal{O}(1)$, where $\psi : X \to \mathbb{P}^m_k$ is a morphism. Then the product $T : X \to \mathbb{P}^n_k \times \mathbb{P}^m_k$ is also an immersion, by base change trick(6.4.4.2), as $\mathbb{P}^n_k \times \mathbb{P}^m_k \to \mathbb{P}^n_k$ is separated. Then $S \circ T : X \to \mathbb{P}^{mn+m+n}$, where $S : \mathbb{P}^n_k \times \mathbb{P}^m_k \to \mathbb{P}^{mn+m+n}$ is the Segre embedding, is also an immersion, and $(ST)^*\mathcal{O}(1) \cong \mathcal{L}\otimes\mathcal{M}$, thus it is H-very ample. □

Prop. (6.5.4.24) [Ample and H-Very Ample]. If $f : X \to S$ is locally of f.t. and $\mathcal{L}$ is an ample invertible sheaf on X, then $\mathcal{L}^{\otimes m}$ is H-very ample for m sufficiently large. ⌟

Proof: Choose an affine open cover $\{V_i\}$ of S. By(6.5.4.5), there are f.m. affine opens X_{s_i} that cover X refining a inverse image of $\{V_i\}$. Now $\mathcal{O}_X(X_{s_i})$ is f.g. over $\mathcal{O}_S(V_i)$, so we can find f.m. $f_{ij} \in \mathcal{O}_X(X_{s_i})$ that generates it over $\mathcal{O}_S(V_i)$. By(6.5.3.5), we can write each $f_{ij} = s_{ij}/s_i^{e_{ij}}$ for some a_{ij} homogenous. We can multiply by a factor to make all the $s_i^{e_{ij}}$ the same degree N, and $f_{ij} = s_{ij}s_i^{N/\deg(s_i)-e_{ij}}$, then all the elements s_i, s_{ij} generates the invertible sheaf $\mathcal{L}$, thus inducing a map $j : X \to \mathbb{P}^m_k$. This map is an immersion, because $j^{-1}(D(T_i)) = X_{s_i}$ and the function T_{ij}/T_i on $D(T_i)$ pulls back to s_{ij}/s_j. Thus j is locally a closed immersion, thus an immersion.

Now $\mathcal{L}^{\otimes d_1}$ is H-very ample for some d_1, in particular it is separated, and by(6.5.4.5) there is some d_2 that $\mathcal{L}^{\otimes d}$ is generated by global sections for all $d \geq d_2$, then by(6.5.4.23), $\mathcal{L}^{\otimes d}$ is H-very ample for $d \geq d_1 + d_2$. □

Prop. (6.5.4.25) [f-Very Ample Implies f-Ample]. If $f : X \to S$ is qc, then f-very ample implies f-ample. ⌟

Proof: Cf.[Sta]01VN.**?** □

Cor. (6.5.4.26) [Serre]. If $S \in \mathcal{A}\mathrm{ff}$, $f : X \to S$ is of f.t. and $\mathcal{L} \in \mathrm{Pic}(X)$, then the following are equivalent:

- $\mathcal{L}$ is ample .
- $\mathcal{L}$ is f-ample.
- $\mathcal{L}^{\otimes n}$ is (H-)f-very ample for some (all large)n.

⌟

Proof: This follows from(6.5.4.22)(6.5.4.24) and(6.5.4.25). □

Cor. (6.5.4.27). If $f : X \to S$ is of f.t. and S is qausi-compact, $\mathcal{L}$ is an invertible sheaf on X, then the following are equivalent:

- $\mathcal{L}$ is f-ample.
- $\mathcal{L}^{\otimes n}$ is (H-)f-very ample for some (all large)n.

⌟

Proof: Cf.[Sta]01VU. □

5 Sheaf of Differentials

Prop. (6.5.5.1) [Differentials on Schemes]. Consider a morphism of schemes $X \to Y$, we define the sheaf of differentials $\Omega_{X/Y}$ together with an S-derivative $\mathcal{O}_X \to \Omega_{X/S}$ as for ringed sites(6.2.4.7). Then $\Omega_{X/S} \in \mathfrak{QCoh}(X)$ by(6.2.4.5). In fact, If $U = \operatorname{Spec} A$ is mapped into $\operatorname{Spec} B \subset S$, then $\Omega_{X/S}(U) \cong \widetilde{\Omega_{A/B}}$.

In particular, the stalk of $\Omega_{X/S}$ at a point $x \in X$ is $\Omega_{\mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)}}$.

Thus when $X \to Y$ is locally of f.t.(or locally of f.p.), then $\Omega_{X/S}$ is an $\mathcal{O}_X$-module of f.t.(or of f.p.). ⌟

Prop. (6.5.5.2) [Base change and Differentials]. Let $\begin{array}{ccc} X' & \xrightarrow{f} & X \\ \downarrow{\scriptstyle g'} & & \downarrow{\scriptstyle g} \\ S' & \longrightarrow & S \end{array}$ be a commutative diagram of schemes, then there is a canonical map

$$f^*\Omega_{X/S} \to \Omega_{X'/S'}$$

which is an isomorphism if the diagram is a fiber product square. ⌟

Proof: Such a diagram gives a diagram $(f^{-1}g^{-1}\mathcal{O}_S \to f^{-1}\mathcal{O}_X) \to ((g')^{-1}(\mathcal{O}_{S'}) \to \mathcal{O}_{X'})$ of sheaves of rings on X'_{Zar}, thus the conclusion follows from(6.2.4.5) and(6.2.7.17). □

Prop. (6.5.5.3). Let X, Y be schemes over another scheme S, then

$$\pi_1^*\Omega_{X/S} \oplus \pi_2^*\Omega_{Y/S} \cong \Omega_{X\times_S Y/S},$$

where the maps are given by(6.5.5.2). ⌟

Proof: It suffices to check on affine subschemes, so we may assume X, Y, S are affine, thus the map is given by

$$\Omega_{A/S} \oplus_S B \oplus_{A\otimes_S B} \Omega_{B/S} \otimes_S A \to \Omega_{A\otimes_S B/S}$$

which is an isomorphism by(5.4.3.6). □

Prop. (6.5.5.4). Let X, Y be schemes over another scheme S, then $\Omega_{X\times_S Y/S} \cong \pi_1^*\Omega_{X/S} \otimes \pi_2^*\Omega_{Y/S}$. ⌟

Prop. (6.5.5.5) [Jacobi-Zariski Sequence]. Let $f : X \to Y$ and $g : Y \to Z$, then there is an exact sequence of sheaves on X:

$$f^*\Omega_{Y/Z} \to \Omega_{X/Z} \to \Omega_{X/Y} \to 0.$$

Where the maps come from(6.5.5.2). ⌟

Proof: Immediate from(5.4.3.8). □

Prop. (6.5.5.6). The stalk of the differential sheaf $\Omega_{X/k}$ at a rational point x of a scheme over a field k is just the Zariski cotangent space $\mathfrak{m}_x/\mathfrak{m}_x^2$(6.6.4.22). ⌟

Proof: Using the Jacobi exact sequence(5.4.3.8) on an affine nbhd $\operatorname{Spec} A$ of x for A and $\mathfrak{m}_x$. Then we verified that there is a right inverse of $A/\mathfrak{m}^2 \to k(x) = x$, then it follows that $\mathfrak{m}_x/\mathfrak{m}_x^2 \cong \Omega_{A/k} \otimes_A k(x) = \Omega_{A_{\mathfrak{m}_x}/k}$ which is the stalk of $\Omega_{X/k}$ by(6.5.5.1). □

Prop. (6.5.5.7) [Euler Exact Sequence]. If $X = \mathbb{P}^n_A = \operatorname{Proj}(A[x_0, \ldots, x_n])$ over $Y = \operatorname{Spec} A$, then there is an exact sequence

$$0 \to \Omega_{X/A} \to (\mathcal{O}_X(-1))^{n+1} \to \mathcal{O}_X \to 0.$$

$\Omega_{X/A}$ is locally free by(6.11.1.16), so by taking dual and exterior powers,

$$0 \to \mathcal{O}_X \to \mathcal{O}_X(1)^{n+1} \to \mathcal{T}_X \to 0, \quad \mathcal{K}_X \cong \mathcal{O}_X(-n-1).$$

⌟

Proof: Let $S = A[x_0, \ldots, x_n], E = S(-1)^{\oplus n+1}$ with a basis $e_0, \ldots, e_n$, then there is a map of S-graded modules $E \to S$ with kernel M. $E \to S$ is surjective in all dimension≥ 1, so we have an exact sequence

$$0 \to \widetilde{M} \to \widetilde{E} \to \mathcal{O}_X \to 0.$$

Notice $E_{(x_i)} \to S_{(x_i)}$ is given by $e_j \mapsto x_j/x_i$, so $\widetilde{M}|_{D(x_i)}$ is a free sheaf generated by sections $(1/x_i)e_j - (x_j/x_i^2)e_i, j \neq i$. So we can define $\varphi_i : \Omega_{X/A}|_{D(x_i)} \to \widetilde{M}|_{D(x_i)} : d(x_j/x_i) \mapsto (1/x_i)e_j - (x_j/x_i^2)e_i, j \neq i$ mapping isomorphically onto the kernel. It suffices to show this map glue to a map $\Omega_{X/A} \to \widetilde{E}$: On $D(x_i x_j)$, $x_k/x_i = (x_k/x_j) \cdot (x_j/x_i)$, so

$$d(\frac{x_k}{x_i}) - \frac{x_k}{x_j} d(\frac{x_j}{x_i}) = \frac{x_j}{x_i} d(\frac{x_k}{x_j}).$$

Applying φ_i to the LHS and φ_j to the RHS gives the same element $(1/x_i)e_k - (x_k/x_i x_j)e_j$, which shows compatibility. □

Conormal Sheaves

Def. (6.5.5.8) [Conormal Sheaf of an Immersion]. Let $i : Z \to X$ be a closed immersion with corresponding sheaf of ideals $\mathcal{I}$. Consider the Qco sheaf $\mathcal{I}/\mathcal{I}^2$, which is annihilated by $\mathcal{I}$, thus corresponds to a sheaf on Z by(6.2.6.18), called the **conormal sheaf** $\mathcal{C}_{Z/X}$ of Z.

More generally, if i is any immersion, we can define the conormal sheaf as the conormal sheaf of the closed immersion $i : Z \to X \backslash \partial Z$. And also the **normal sheaf** $\mathcal{N}_{Z/X}$ is defined to be $\mathcal{N}_{Z/X} = \operatorname{Hom}_{\mathcal{O}_Z}(\mathcal{I}/\mathcal{I}^2, \mathcal{O}_Z)$. ⌟

Prop. (6.5.5.9) [Pullback of Conormal Sheaf]. Let $\begin{array}{ccc} Z' & \xrightarrow{i} & X \\ \downarrow f & & \downarrow g \\ Z' & \xrightarrow{i'} & X' \end{array}$ be a fiber product square where i, i' are immersions, then the canonical map

$$f^* \mathcal{C}_{Z'/X'} \to C_{Z/X}$$

is surjective, and if g is flat, it is an isomorphism. ⌟

Proof: Change X' to $X'\backslash\partial Z'$ and X to $X\backslash(g^{-1}\partial Z'\cup\partial Z)$, we may assume i is a closed immersion. Then we may localize to the case X' and X is affine. Then we notice if $R'\to R$ is a ring map and $I'\subset R'$ is an ideal, with $I=I'R$, then $(I'/(I')^2)\otimes_{R'}R\to I/I^2$ is surjective, and if R/R' is flat, then $I\cong I'\otimes_{R'}R$, and the map is an isomorphism. □

Prop. (6.5.5.10). Let $Z\xrightarrow{i}Y\to X$ be immersions of schemes, then there is a canonical exact sequence

$$i^*\mathcal{C}_{Y/X}\to\mathcal{C}_{Z/X}\to\mathcal{C}_{Z/Y}\to 0$$

⌟

Proof: By changing Y to $Y\backslash\partial Z$ and X to $X\backslash(\partial(Y\backslash Z))$, we can assume the immersions are closed immersion. Now by restricting to affine subsets, it suffices to show that for surjective ring maps $C\to B\to A$, if $I=\ker(B\to A), J=\ker(C\to A), K=\ker(C\to B)$, then there is an exact sequence

$$K/K^2\otimes_B A\to J/J^2\to I/I^2\to 0.$$

But this follows from the observation $K=\ker(J\to I)$. □

Prop. (6.5.5.11) [Conormal Sheaf of the Diagonal]. Let $f:X\to S$ be a morphism, then there is a canonical isomorphism between $\Omega_{X/S}$ and the conormal sheaf of the diagonal $\Delta:X\to X\otimes_S X$. ⌟

Proof: Cf.[Sta]08S2.**?** □

Cor. (6.5.5.12). If $f:X\to S$ is a monomorphism, e.g. an immersion, then $\Omega_{X/S}=0$. ⌟

Prop. (6.5.5.13). If $f:Z\to X$ is an immersion of schemes over S, then there is an exact sequence of sheaves on Z:

$$\mathcal{C}_{Z/X}\to i^*\Omega_{X/S}\to\Omega_{Z/S}\to 0.$$

⌟

Proof: Replace X be $X\backslash\partial Z$, we can assume f is a closed immersion. This follows immediate from(6.2.4.6). □

Prop. (6.5.5.14). If $i:Z\to X$ is an immersion over S that locally has a left inverse, then the canonical sequence

$$0\to\mathcal{C}_{Z/X}\to i^*\Omega_{X/S}\to\Omega_{Z/S}\to 0.$$

is locally split exact. In particular, if $s:S\to X$ is a section of the structure morphism $X\to S$, then the map $\mathcal{C}_{S/X}\to s^*\Omega_{X/S}$ is an isomorphism. ⌟

Proof: Cf.[Sta]0474.**?** □

Prop. (6.5.5.15). Let $\begin{array}{ccc} Z & \xrightarrow{i} & X \\ & \searrow^{j} & \downarrow \\ & & Y\end{array}$ be a commutative diagram where i,j are immersions, then there is a canonical exact sequence

$$\mathcal{C}_{Z/Y}\to\mathcal{C}_{Z/X}\to i^*\Omega_{X/Y}\to 0,$$

where the first arrows comes from(6.5.5.9) and the second map comes from(6.5.5.13). ⌟

Proof: By replacing Y by $Y\backslash\partial Z$ and X by $X\backslash(\partial i(Z)\cup\partial j(Z))$, then we may assume i,j are closed immersion. Then we check locally, the exactness follows from(7.1.1.5). □

6.6 More Properties of Morphisms between Schemes

Main references are [Sta].

Notation (6.6.0.1).

- Use notations defined in Properties of Schemes.

⌟

1 Finitely Presentedness

Def. (6.6.1.1) [Locally of Finite Presentation]. A morphism between schemes $f : Y \to X$ is called **of locally finite presentation** iff for any point $x \in X$, there is an open affine mapped into an open affine that the ring map is of finite presentation. It is called **of finite presentation** iff moreover it is qcqs.

locally of finite presentation is local on the source and target and it is stable under composition and base change but it doesn't satisfies the base change trick by(6.4.1.6)(6.4.1.5) and(5.3.7.9). ⌟

Prop. (6.6.1.2). Open immersion is locally of finite presentation. ⌟

Prop. (6.6.1.3). When the target is locally Noetherian, (locally)finite type and (locally)finite presentation is equivalent. ⌟

Prop. (6.6.1.4). For $f : X \to Y$ over S, if X/S is locally of f.p. and Y/S is locally of f.t., then f is locally of f.p.. If moreover X is of f.t. and Y is qs, then f is of f.t.. ⌟

Proof: The first follows from(5.3.7.11), the second needs to check qcqs. Qc follows from(6.4.4.27). □

Prop. (6.6.1.5) [Chevalley]. A qc morphism locally of f.p. maps locally constructible subset to locally constructible subset. ⌟

Proof: We prove $f(E) \cap U_i$ is constructible for every U_i affine open in X. The inverse image of U_i is qc, hence a locally constructible set is constructible (4.12.3.10). So we reduce to the affine case(5.1.7.3). □

Cor. (6.6.1.6). As in the proposition, if Y is qc, and the image is dense in Y, then it contains an open dense subset of Y, by(4.12.3.17). ⌟

2 Flatness

Def. (6.6.2.1) [Flatness for Schemes]. Flat modules and flat morphisms over schemes are defined in the same way as that of ringed spaces(6.2.2.15). ⌟

Prop. (6.6.2.2). Flatness is stalkwise by(6.2.2.17), it is stable under base change and compositions. $\mathcal{F} \in \mathfrak{Coh}(X)$ is flat over X iff it is locally free, by(5.4.1.10)

Thus for $\mathcal{F} \in \mathfrak{QCoh}(X)$, flatness is equivalent to: For any affine open subsets $\operatorname{Spec} A \subset X$, $\Gamma(\operatorname{Spec} A, \mathcal{F})$ is flat over A, because flatness is also stalkwise for modules(5.1.4.2). Similarly, a morphism of schemes $f : X \to Y$ is flat iff for any affine opens $\operatorname{Spec} B \subset X, \operatorname{Spec} A \subset Y$ that $f(\operatorname{Spec} B) \subset \operatorname{Spec} A$, B is flat over A. ⌟

Prop. (6.6.2.3). For a flat morphism of ringed space, f^* is exact. ⌟

Proof: Because it is f^{-1} followed by tensoring with $\mathcal{O}_X$, check on stalks. □

Prop. (6.6.2.4) [Faithfully Flat Descent for Flat Modules]. Let $f : X \to Y$ be a morphism of schemes over S and $\mathcal{G} \in \mathfrak{QCoh}(Y)$, then $\mathcal{G}$ is flat over S iff $f^*\mathcal{G}$ is flat over S. In particular, Y is flat over S iff X is flat over S. ⌟

Proof: This follows from(5.4.1.6). □

Prop. (6.6.2.5). For a Qco sheaf $\mathcal{F}$ on a scheme X, the following are equivalent, by(5.3.1.7).

1. $\mathcal{F}$ is finite projective.
2. $\mathcal{F}$ is f.p. and flat.
3. $\mathcal{F}$ is f.p. and all its localizations at (maximal)primes are free.
4. $\mathcal{F}$ is finite locally free.
5. $\mathcal{F}$ is finite and locally free.
6. $\mathcal{F}$ is finite and all its localizations at primes are free and the function $p \to \dim_{k(p)} \mathcal{F} \otimes_R k(p)$ is a locally constant function on $\operatorname{Spec} R$.

⌟

Cor. (6.6.2.6). Let $f : X \to Y$ be a finite morphism of locally Noetherian schemes and Y is reduced, the following are equivalent:

- f is flat.
- $f_*\mathcal{O}_X$ is locally free.
- $\dim_{k(x)}(\pi_*\mathcal{O}_X)_x \otimes k(x)$ is a locally constant function for $x \in Y$.

⌟

Proof: 3 follows from(6.5.1.43). □

Prop. (6.6.2.7) [Going-Down]. Generalizations lift along a flat morphism. ⌟

Proof: We can find an affine nbhd, then choose a nbhd of the inverse image, then a generalization in an affine open is a true generalization, so it reduce to the affine case. The rest follows from going-down(5.4.1.19). □

Cor. (6.6.2.8) [Flat Map and Irreducible Components]. A flat morphism maps generic points to generic points. ⌟

Prop. (6.6.2.9) [Flat Map and Associated Points]. Let $f : X \to S$ be a morphism of schemes that S is locally Noetherian, and $\mathcal{F}$ a Qco sheaf on X. If $\mathcal{F}$ is flat over S, then f maps $WeakAss(\mathcal{F})$ to $Ass(S)$. In particular, if X is flat over S, then f maps $WeakAss(X)$ to $Ass(S)$. ⌟

Proof: Let $x \in X, f(x) = s$ that $s \in Ass(S)$, then we get a map $(\mathcal{O}_{S,s}, \mathfrak{m}_s) \to (\mathcal{O}_{X,x}, \mathfrak{m}_x)$. If $\mathfrak{m}_s$ is not associated point, then by prime avoidance(5.1.1.5), there is some $m \in \mathfrak{m}_s$ that is not a non-zero divisor, by(5.2.5.17), so $f^\sharp(m)$ is also a non-zero divisor on $\mathcal{F}_x$, so $\mathfrak{m}_x$ is not a weakly associated point of $\mathcal{F}$. □

Prop. (6.6.2.10) [Flat Map is Open]. A flat morphism locally of f.p. is (universally)open, hence it is qc.

And a qc f.f. morphism of schemes is a quotient map. ⌟

Proof: It suffices to consider the affine case. Then the assertion follows from(5.4.1.32).

For the second, by(6.6.2.7), a subset whose inverse image is closed is stable under specialization(surjectiveness used), then it is closed by(6.4.4.9) □

Prop. (6.6.2.11) [Cartier Divisor and Flat Base Change].

- The flat base change of Cartier divisor is also a Cartier divisor.
- The flat base change of a regular embedding is also a regular embedding.
- The flat base change commutes with blow up, by universal property.

⌟

Prop. (6.6.2.12) [Flat Pullback of Closed Subschemes]. Let $Z \subset X$ be a closed subscheme corresponding to a Qco sheaf of ideals $\mathcal{I}$, and $f : X' \to X$ be a flat morphism, then the pullback $Z' \subset X'$ is a closed subscheme that corresponds to the ideal sheaf $f^*\mathcal{I}$. ⌟

Proof: This is because f^* is exact. □

Prop. (6.6.2.13) [Pullback of Flat Closed Subschemes]. Let X be a scheme over S, $S' \to S$ be a morphism of schemes, and $Z \subset X$ be a closed subscheme corresponding to a Qco sheaf of ideals $\mathcal{I}$ flat over $\mathcal{S}$, then the pullback $Z' \subset X'$ is a closed subscheme that corresponds to the ideal sheaf $f^*\mathcal{I}$. ⌟

Prop. (6.6.2.14) [Flat Loci is Open]. For a morphism $f : X \to S$ locally of f.p., and $\mathcal{F} \in \mathfrak{QCoh}^{\mathrm{pf}}(X)$, then the set of points of X that $\mathcal{F}$ is flat over S is open. In particular, if f is a closed map, then the set of points of Y that $\mathcal{F}$ is flat is open. ⌟

Proof: Cf.[Sta]00RC.**?**

The last assertion follows from the first one. □

Prop. (6.6.2.15) [Generic Flatness]. For a morphism $f : X \to S$ of f.t., if S is reduced and $\mathcal{F}$ is a Qco f.t. $\mathcal{O}_X$-module, then there exists an open dense subset U of S that $X_U \to U$ is flat, of f.p., and $\mathcal{F}_{X_U}$ is flat over U and of f.p. over $\mathcal{O}_U$. ⌟

Proof: As flat and f.p. is local on the base, it suffices to show for S affine. Then this almost immediately reduces to the affine case**??**y choosing an affine cover of X, except that we need X_U to be qs over U. To achieve this, it suffices to do it second time and let $X = \cup_{i\leq n} \operatorname{Spec} B_i = \cup X_i$, and $X_i \cap X_j = D(I_{ij})$, $M_{ij} = B_i/I_{ij}$, then choose f large enough that over S_f, all M_{ij} are f.p. over B_i, then by(5.2.5.9), $X_{i,f} \cap X_{j,f}$ is qc, thus X_f is f.p. over S_f. □

Prop. (6.6.2.16) [Fibral Criterion of flatness]. Let $S \in \mathfrak{Sch}$ and $f : X \to Y$ in $\mathfrak{Sch}/S$, $\mathcal{F} \in \mathfrak{QCoh}^{\mathrm{pf}}(X)$. Let $x \in X, y = f(x)$ and x maps to $s \in S$. Suppose X, Y are both locally Noetherian or X is locally of f.p. over S and Y is locally of f.t. over S, then the following are equivalent:

- $\mathcal{F}$ is flat over S at x and $\mathcal{F}_s$ is flat over Y_s at x.
- Y is flat over S at y and $\mathcal{F}$ is flat over Y at x.

⌟

Proof: Cf.[Sta]039B, 039C. □

Prop. (6.6.2.17) [Hilbert Polynomial Constant in Flat Family]. For <u>X/T projective</u>, where T is an integral Noetherian scheme and $X \subset \mathbb{P}^n_T$. Then for each point T, X_t is a closed subscheme of $\mathbb{P}^n_{k(t)}$, so we can consider its Hilbert Polynomial P_t. Then X/T is flat iff P_t is independent of T.

?Needs huge improvement. ⌟

Proof: $P_t(m) = \dim_{k(t)} H^0(X_t, \mathcal{O}_{X_t}(m))$ for m large by(6.7.3.10). And we may let $X = \mathbb{P}^n_T$ and prove for any coherent sheaf $\mathcal{F}$. Moreover, we may let T be a affine local Noetherian, because flatness is local and we only need to compare Hilbert polynomial with the generic point. Now we prove a stronger assertion: The following are equivalent:

- $\mathcal{F}$ is flat over T.
- $H^0(X, \mathcal{F}(m))$ is a free A-module of finite rank, for m large.
- The Hilbert polynomial P_t of $\mathcal{F}_t$ on $X_t = \mathbb{P}^n_{k(t)}$ is independent of t.

$1 \to 2$: Use the canonical cover and Čech cohomology, then we notice when m is large, $H^0(X, \mathcal{F}(m))$ is a kernel of the Čech resolution, so it is flat. And it is also finite by(6.7.4.12). Then it is free because it is flat by(5.4.1.10).

$2 \to 1$: Let $M = \oplus_{m \geq m_0} H^0(X, \mathcal{F}(m))$, then $\widetilde{M} = \mathcal{F}$(6.5.3.6), notice that the truncation doesn't affect.

$2 \to 3$: It suffice to prove that for any $t \in T$, when m is large,

$$H^0(X_t, \mathcal{F}_t(m)) \cong H^0(X, \mathcal{F}(m)) \otimes_A k(t).$$

For this, we may use(6.7.5.1) to pass to the localization and assume t is the closed pt of T. Then $A \to k(t)$ is surjective and we may let $A^q \to A \to k \to 0$, then by(6.7.4.8), we have $H^0(X_t, \mathcal{F}_t(m))$ is the cokernel of $H^0(X, \mathcal{F}(m))^q \to H^0(X, \mathcal{F}(m))$, but this cokernel is $H^0(X, \mathcal{F}(m)) \otimes_k$ because tensoring is right-adjoint, so we are done.

$3 \to 2$: We have the rank of $H^0(X, \mathcal{F}(m))$ at the generic and closed point of T are the same(still use $H^0(X_t, \mathcal{F}_t(m)) \cong H^0(X, \mathcal{F}(m)) \otimes_A k(t)$.) Now(5.4.8.1) gives $H^0(X, \mathcal{F}(m))$ is free. It is f.g. automatically. □

Cor. (6.6.2.18). For a flat morphism to a connected scheme T, the dimension, degree, and arithmetic genus of the fibers are independent of t. ⌟

Proof: By(6.7.3.6)and (6.7.3.12). □

Def. (6.6.2.19). For a surjective map of varieties $f : X \to T$ over an alg.closed field k, its fiberes over closed points with induced reduced structure $X_{(t)}$ is called a **algebraic family of varieties parametrized by** T if

1. $f^{-1}(t)$ is irreducible of dimension $\dim X - \dim T$ for every closed point t.
2. If ζ is the generic point of $f^{-1}(t)$, then $F^\sharp \mathfrak{m}_t$ generates the maximal ideal $\mathfrak{m}_\zeta \subset \mathcal{O}_{\zeta,X}$.

⌟

Prop. (6.6.2.20). if $X_{(t)}$ is an algebraic family of normal varieties over an alg.closed field k parametrized by a nonsingular curve T, then it is a flat family of schemes. ⌟

Proof: By(6.12.1.20), $X \to T$ is flat. So what we need to do is to prove X_t is reduced so $X_t = X_{(t)}$. Let $A = \mathcal{O}_{x,X}$, let u_t be a uniformizer of $\mathcal{O}_{t,T}$, then A/tA is the local ring of x on X_t. By hypothesis X_t is irreducible so tA has a unique minimal prime p in A, and t generate the maximal ideal of A_p by hypothesis. The local ring of $X_{(t)}$ is A/p, so A/p is normal by hypothesis. Then the result follows from(5.3.5.13). □

Cor. (6.6.2.21) [Igusa]. Let $X_{(t)}$ be an algebraic family of normal varieties in $\mathbb{P}^n_k$ for k alg.closed parametrized a variety T, then the Hilbert polynomials of $X_{(t)}$ are independent of t. ⌟

Proof: ? Why is X/T projective? Cf.[Hartshorne P265]. □

Degenerating Techniques

Finite Locally Free Morphism

Def. (6.6.2.22) [Finite Locally Free]. A morphism $f : X \to Y$ is called **finite locally free of rank** d iff it is affine, and $f_*\mathcal{O}_X$ is a finite locally free $\mathcal{O}_Y$-module of rank d. ⌟

Cor. (6.6.2.23). If f is finite locally free of rank n, then for any locally free sheaf E of rank k on X, f_*E is locally free of rank nk. ⌟

Prop. (6.6.2.24). f is finite locally free iff it is finite, flat and of f.p.. In particular, when Y is locally Noetherian, this is equivalent to f is finite flat. ⌟

Proof: Both notions are local on the target, so we reduce to the ring case, which is(5.3.1.7). □

Cor. (6.6.2.25). Finite locally freeness is stable under composition and base change, and it is local on the target. ⌟

Prop. (6.6.2.26) [Trace and Norm]. Let $f : Y \to X$ be a finite locally free map of constant rank, then there are trace and norm maps $\mathrm{tr} : f_*\mathcal{O}_Y \to \mathcal{O}_X, \mathrm{Nm} : f_*\mathcal{O}_Y \to \mathcal{O}_X$ compatible with arbitrary base change. ⌟

Proof: The proof is the same as that of(5.3.1.11). □

Prop. (6.6.2.27). Let $f : Y \to X$ be a finite locally free map of constant rank, and $b \in \Gamma(Y, \mathcal{O}_Y)$, then $f(Z(b)) = Z(\mathrm{Nm}(b))$. ⌟

Proof: We can assume X is affine, then we need to show that for a prime $\mathfrak{p}$ with inverse images $\mathfrak{p}_i$, $b \in \cup\mathfrak{p}_i$ iff $Nm(b) \in \mathfrak{p}$. We localize at $\mathfrak{p}$, then $\mathrm{Nm}(b) \in \mathfrak{p}$ iff $\mathrm{Nm}(b)$ is non-invertible iff multiplication by b is non-invertible iff b is non-invertible iff $b \notin \cup\mathfrak{p}_i$, because $\mathfrak{p}_i$ are all the maximal ideals of $B_\mathfrak{p}$. □

3 Dimensions

Main references are [Mat80] and [Vak17]Chap11.

Prop. (6.6.3.1) [Locally Algebraic Scheme is Catenary]. If X is a locally algebraic scheme over a field k purely of dimension n, and Y an irreducible subscheme of X, then $\dim Y + \mathrm{codim}(Y, X) = \dim X$. ⌟

Proof: Choose an affine open of the generic point of Y, then we are reduced to the affine case(5.2.4.3)(5.2.4.7). □

Prop. (6.6.3.2). For any scheme, $\dim \mathcal{O}_x = \mathrm{codim}(\overline{\{x\}}, X)$. ⌟

Prop. (6.6.3.3). For an integral scheme algebraic over a field k,

$$\dim X = \dim \mathcal{O}_{p,X} = \dim U = \mathrm{tr.deg}\ K(X)/k$$

for any closed point p and any open subscheme U. ⌟

Proof: Use closed point are dense(6.4.1.26) and k is universal catenary to prove it is true for some U and all the closed point in it, so other U's because X is irreducible. The last equation follows from(5.2.4.23). □

Prop. (6.6.3.4) [Finite Surjection Preserves Dimension]. Let $X \to Y$ be a surjective finite morphism of algebraic integral schemes over a field k, then $\dim X = \dim Y$. ⌟

Proof: The hypothesis implies that for any affine open $\operatorname{Spec} A \subset Y$, the inverse image is $\operatorname{Spec} B$ that $A \to B$ is an injective integral ring extension, so we can use(6.6.3.3) and(5.2.4.14). □

Prop. (6.6.3.5). Let X be a locally Noetherian scheme, if $U \subset X$ is an open subscheme that $U \to X$ is affine, then every irreducible complements of $X - U$ has codimension≤ 1. And if U is dense, then equality must hold. ⌟

Proof: Cf.[Sta]0BCU. □

Prop. (6.6.3.6) [Local Dimensions]. Let Let X be a locally algebraic scheme over a field k and $x \in X$, then the local dimension $\dim_x(X)$ equals the maximal dimension of irreducible components of X passing through x, by(5.2.4.27). ⌟

Prop. (6.6.3.7). If $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, $x \in X$ and $s = f(x)$, then

$$\dim_x(X_s) = \dim \mathcal{O}_{X_s,x} + \operatorname{tr.deg}_{k(s)} k(x).$$

⌟

Proof: This reduces to the case $Y = \operatorname{Spec} k(s)$, and it follows from(5.2.4.28). □

Prop. (6.6.3.8) [Semicontinuity of Dimension]. Let $f : X \to S$ be a morphism of schemes locally of f.t., then the function $x \mapsto \dim_x(X_{f(x)})$ is upper-semicontinuous on X.

Moreover, if f is of f.p., then the open subsets $\{x | \dim_x(X_{f(x)}) \leq n\}$ is retrocompact. ⌟

Proof: This follows directly from(5.2.4.32). □

Prop. (6.6.3.9) [Local Dimension and Base Change]. Let

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} \\ S' & \xrightarrow{g} & S \end{array}$$

be a fiber product diagram of schemes, and f is locally of f.t.. Suppose $x' \in X', x = g'(x'), s = g(s')$. Then

- $\dim_x(X_s) = \dim_{x'}(X_{s'})$.
- $$\dim \mathcal{O}_{F,x'} = \dim \mathcal{O}_{X'_{s'},x'} - \dim \mathcal{O}_{X_s,x} = \operatorname{tr.deg}_{k(s)}(k(x)) - \operatorname{tr.deg}_{k(s')}(k(x'))$$
  where F is the fiber of the morphism $X'_{s'} \to X_s$ over x. In particular, $\dim \mathcal{O}_{X'_{s'},x'} \geq \dim \mathcal{O}_{X_s,x}$ and $\operatorname{tr.deg}_{k(s')}(k(x')) \leq \operatorname{tr.deg}_{k(s)}(k(x))$.
- Given s', s, x that $f(x) = g(s')$, there exists an $x' \in X'$ that $\dim \mathcal{O}_{X'_{s'},x'} = \dim \mathcal{O}_{X_s,x}$ and $\operatorname{tr.deg}_{k(s')}(k(x')) = \operatorname{tr.deg}_{k(s)}(k(x))$.

⌟

Proof: It can be reduced to the case that $S = \operatorname{Spec} k(s), S' = \operatorname{Spec} k(s')$ and X, X' affine. Then 1 follows from(5.2.4.31), and $2, 3$ follows from(5.2.4.26). □

Cor. (6.6.3.10) [Dimension and Field Extension]. Let K/k be a field extension, X a locally algebraic scheme over k purely of dimension n, then X_K is a scheme purely of dimension n. ⌟

Remark (6.6.3.11). This proposition shows in particular local dimension behaves better than the dimension of the stalk. ⌟

Def. (6.6.3.12) [Relative Dimensions]. A morphism of schemes which locally of f.t. is called of **relative dimension** n iff all fibers X_s are equidimensional of dimension n. ⌟

Prop. (6.6.3.13). Being a morphism of relative dimension n is stable under field extension, by(6.6.3.10). ⌟

Dimension and Flatness

Prop. (6.6.3.14) [Faithfully Flat Morphism]. If $f : Y \to X$ is a faithfully flat morphism, then $\dim Y \geq \dim X$. ⌟

Proof: This is easy from(6.6.2.7). □

Prop. (6.6.3.15) [Integral Flat Morphisms]. If $f : X' \to X$ is an integral flat morphism of schemes, and X is pure of dimension n, then so does X'. The converse holds if f is faithfully flat. ⌟

Proof: By(6.6.2.8) and(6.4.4.35), f maps an irreducible component of X' onto an irreducible component of X, Then by(4.12.3.26), the proposition reduces to the affine case(5.2.4.15). If f is faithfully flat, then every irreducible component of X is in the image. □

Cor. (6.6.3.16) [Dimension and Field Extension]. If K/k is an algebraic extension, X a scheme over k purely of dimension n, then X_K is a scheme purely of dimension n. Compare with(6.6.3.10). ⌟

Prop. (6.6.3.17) [Dimension Extension and Flatness]. Let $f : X \to Y, g : Y \to S$ be locally of f.t., $x \in X, y = f(x), s = g(y)$, then

$$\dim_x(X_s) \leq \dim_x(X_y) + \dim_y(Y_s).$$

Moreover, equality holds if $\mathcal{O}_{X,x}/\mathcal{O}_{Y,y}$ is flat.

In particular, if $S = \operatorname{Spec} k$ and X, Y are irreducible and X is flat over Y, then $\dim X_y = \dim X - \dim Y$ for any $y \in Y$. ⌟

Proof: By(6.6.3.7) and the fact transcendental degree is additive, this reduces to

$$\dim \mathcal{O}_{X_s,x} \leq \dim \mathcal{O}_{X_y,x} + \dim \mathcal{O}_{Y_s,y}.$$

We can assume X, Y is affine and $S = \operatorname{Spec} k(s)$, so the rest follows from(5.2.4.13). □

Cor. (6.6.3.18). If $f : X \to Y, g : Y \to Z$ are of relative dimension m and n(6.6.3.12), and f is flat, then $g \circ f$ is of relative dimension $m + n$. ⌟

Cor. (6.6.3.19) [Generic Dimension Equation]. If $f : X \to Y$ is a dominant morphism of irreducible algebraic schemes over K that X is reduced, then there is a dense open subset U of Y that for any $y \in Y$,

$$\dim(X_y) = \dim X - \dim Y.$$

⌟

Proof: This is a combination of the above proposition and generic flatness(6.6.2.15). □

Prop. (6.6.3.20) [Relative Dimension and Base Change]. By(6.6.3.9), the base change of a morphism of locally algebraic schemes over a field k of relative dimension n is still of relative dimension n. In particular, for a variety over K a field, the dimension is invariant under base change of fields. ⌟

Cor. (6.6.3.21). Let Y,Z be irreducible locally algebraic schemes over k, then $Y\times_k Z$ is pure of dimensional $\dim(Y)+\dim(Z)$. ⌟

Proof: Combine(6.6.3.20) and(6.6.3.17). □

Prop. (6.6.3.22). For a morphism $f:X\to Y$ between locally Noetherian schemes which is flat and locally of f.t and of relative dimension n, then if $y=f(x)$, we have $\dim_x(X_y)=\dim_x(X)-\dim_y(Y)$. ⌟

Proof: Shrinking the nbhd, we may assume $\dim_x(X)=\dim X$ and $\dim_y(Y)=\dim Y$ and X,Y are affine. Now f is locally of f.p. and flat, so it is open(6.6.2.10). So we may assume f is surjective. Then $\dim\mathcal{O}_{X,a}=\dim\mathcal{O}_{Y,b}+\dim\mathcal{O}_{X_b,a}=\mathcal{O}_{Y,b}+n$ by(5.2.4.13), then taking supremum**??**, the result follows. □

Cor. (6.6.3.23). For a morphism of schemes that is flat and of f.t., if Y is irreducible, then X is equidimensional of dimension $\dim Y+n$ iff X_y is equidimensional of dimension n for every $y\in Y$. ⌟

Proof: The proof highly relies on(6.6.3.3).

If X is equidimensional of dimension $\dim Y+n$, for $Z\subset X_y$ an irreducible component, choose a closed pt x of Z not contained in any other irreducible component, then

$$\dim_x Z=\dim_x X-\dim_y Y=\dim X-\dim\overline{\{x\}}-\dim Y+\dim\overline{\{y\}}.$$

The two closures are of the same dimension because by(5.2.6.10), their quotient field extension is finite, and use(5.2.4.14).

Conversely, for an irreducible component of X, choose a closed pt x of Z not contained in any other irreducible component, then the image is also closed, by(6.4.1.27), so the result is immediate. □

Prop. (6.6.3.24). If $f:X\to Y$ is a proper flat morphism of schemes of f.p., then the dimension of fibers of f is a locally constant function. ⌟

Proof: Cf.[Sta]04DJ.**?** □

4 Smoothness

Def. (6.6.4.1) [Smooth Morphisms]. A **smooth morphism** $f:X\to Y$ between schemes is a morphism that there is an open affine cover $\{U_i\}$ of S and an open affine cover V_{ij} of $f^{-1}(\{U_i\})$ that the ring map is smooth(5.4.5.12). In particular, it is locally of f.p.. A **standard smooth morphism** is the Spec map of a standard smooth ring map.

Smoothness is local on the source and target(5.4.5.13). Smoothness is stable under base change and composition(5.4.5.13). ⌟

Prop. (6.6.4.2). For a smooth morphism $X\to S$, the morphism of differential $\Omega_{X/S}$ is locally free and $\dim_x\Omega_{X/S}=\dim_x(X_{f(x)})$(local dimension(4.12.3.25)). ⌟

Proof: We can assume that $X \to S$ is standard smooth, so by the proof in(5.4.5.12), $\Omega_{X/S}$ is free of dimension $n-c$, and also standard smooth is relative global complete intersection(5.4.5.11), so $U_{f(x)}$ is equidimensional of dimension $n-c$, thus the result. □

Cor. (6.6.4.3) [Differential Criterion of Smoothness]. If $X \to S$ is a flat of relative dimension n, then X is smooth over S iff it is locally of f.p. and $\Omega_{X/S}$ is locally free of dimension n, by(5.4.5.23). ⌟

Prop. (6.6.4.4) [Smooth Morphism is Open]. Smooth morphism is syntomic hence flat. Smooth morphism is locally of f.p. Hence smooth morphism is universally open(6.6.2.10).

Smooth morphism is locally standard smooth(5.4.5.12). ⌟

Prop. (6.6.4.5) [Fiberwise and Stalkwise]. For a morphism $X \to S$ locally of f.p., the following are equivalent:

- It is smooth at a point $x \in X$ over $s \in S$.
- $\mathcal{O}_{X,x}/\mathcal{O}_{X,f(x)}$ is flat and $X_{f(x)}/k(f(x))$ is smooth at x, by(5.4.5.20).
- $\mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)}$ is flat and $\Omega_{X/S,x}$ can be generated by $\dim_x(X_{f(x)})$ elements, by(6.6.4.2) and(5.4.5.23).
- $\mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)}$ is flat and $\Omega_{X_s/s,x} \otimes_{\mathcal{O}_{X_s,x}} k(x) = \Omega_{X/S,x} \otimes_{\mathcal{O}_{X,x}} k(x)$ can be generated by $\dim_x(X_{f(x)})$ elements, by Nakayama, because $\Omega_{X/S,x}$ is of f.p. by(5.4.3.9).

In particular, A smooth morphism can be seen as a family of smooth schemes. ⌟

Proof: □

Cor. (6.6.4.6) [Smoothness over DVR]. Let $(\mathcal{O}_K, K, k)$ be a DVR, then $X \in \mathcal{S}\mathrm{ch}^{\mathrm{int,ft}}/\mathcal{O}_K$ is smooth over $\mathcal{O}_K$ iff $X_K \neq \varnothing$ and both X_K/K and X_k/k are smooth. ⌟

Proof: Notice that it is flat iff $X_K \neq \varnothing$. □

Prop. (6.6.4.7). If $X \to Y$ is a smooth map of schemes over S, then by(6.5.5.5)(5.4.5.5), there is an exact sequence of sheaves:

$$0 \to f^*\Omega_{Y/S} \xrightarrow{df^*} \Omega_{X/S} \to \Omega_{X/Y} \to 0$$

⌟

Prop. (6.6.4.8). If $Z \to X \to S$, Z/S is smooth and $Z \to X$ is an immersion, then there is an exact sequence of sheaves(6.5.5.13)(5.4.5.6):

$$0 \to \mathcal{C}_{Z/X} \to i^*\Omega_{X/S} \to \Omega_{Z/S} \to 0$$

⌟

Prop. (6.6.4.9). If $X \to Y \to S$, and $X \to Y$ are faithfully flat and locally of f.p., X/S is smooth, then Y/S is smooth. ⌟

Proof: Cf.[Sta]05B5. □

Prop. (6.6.4.10). If $f : X \to S$ is faithfully flat and locally of f.p., then the set of points of S s.t. f is smooth is table under base change. ⌟

Proof: □

Prop. (6.6.4.11). By(6.6.4.5)(6.6.4.2), A morphism is smooth of relative dimension n is equivalent to fppf+fibers equidimensional of dimension n and $\Omega_{X/S}$ is locally free of dimension n. ⌟

Prop. (6.6.4.12) [Jacobian Criterion for Projective Schemes]. Let X be a closed subscheme of $\mathbb{P}^n_R$ defined by r polynomials $F_1(X_0,\ldots,X_n),\ldots,F_r(X_1,\ldots,X_n)$, then for $x\in X$, X is smooth at x iff the Jacobian has rank$\geq n-\dim_{\mathfrak{x}} X$ at x iff the Jacobian has rank$= n-\dim_x X$ at x. ⌟

Proof: Assume that x is in the standard open $X_0\neq 0$, then we can use Euler's identity $\sum X_i\frac{\partial F}{\partial X_i}=\dim(F)F$ to eliminate the first row, then divide by $X_0^{\dim F}$ to get the Jacobian on the affine open $\operatorname{Spec} R[\frac{X_1}{X_0},\ldots,\frac{X_n}{X_0}]$, so we finish by(5.4.5.24). □

Prop. (6.6.4.13) [Generic Smoothness on the Source]. Let $\pi: X\to Y$ be a dominant map of integral schemes of f.t. that $K(Y)\to K(X)$ is separable, then thee is a non-empty open subscheme $U\subset X$ that $\pi|_U$ is smooth of relative dimension $\dim X-\dim Y$. ⌟

Proof: This reduces to the affine case, and follows from(5.4.5.29) and(6.6.3.17). □

Prop. (6.6.4.14)[Generic Smoothness on the Target]. Let $\pi: X\to Y$ be a morphism of k-varieties where $\operatorname{char} k=0$, and X is smooth over k, then there is a dense open subset $U\subset Y$ that $\pi^{-1}(U)\to U$ is smooth. ⌟

Proof: Cf.[Vak17]P681. □

Smooth over Fields

Prop. (6.6.4.15)[Differential Criterion of Smoothness]. Let X be a scheme algebraic over a field k.

- If X is equidimensional of dimension n, then X is smooth over k iff $\Omega_{X/S}$ is locally free of dimension n.
- If $\Omega_{X/k}$ is locally free, and k is of char 0 or k is perfect and X is reduced, then X is smooth over k.

⌟

Proof: 1: This follows from(6.6.4.3).
2: If k is of characteristic 0, then this follows from(5.4.5.28).
perfect case: [Sta]04QP.**?** □

Prop. (6.6.4.16)[Smooth over Field and Geo.Regular]. For a scheme locally algebraic over a field k, X is geometrically regular iff it is smooth over k. In particular, if k is perfect, then smoothness is equivalent to regularity, by(6.4.3.18). ⌟

Proof: The question is local around x, so may assume X is affine. Then this follows from(5.4.5.27). □

Cor. (6.6.4.17) [Hartshorne Definition]. By(6.6.4.5) and(6.6.4.16), a morphism between schemes algebraic over a field k is smooth of relative dimension n iff f is flat and every fiber of f is geometrically regular of dimension n. ⌟

Cor. (6.6.4.18). A smooth scheme over a field k is regular hence normal. ⌟

Prop. (6.6.4.19) [Smoothness and Separable Closed Points]. Let X be smooth over a field k, then the set of closed points of X with finite separable residue field $k(x)/k$ is dense in X. ⌟

Proof: It suffices to show there exists one such points. By(6.6.6.7), we can assume $X \xrightarrow{\pi} \mathbb{A}_k^d \to k$, where π is étale. Thus X is open in A_k^d by(6.6.6.3). Then we can choose a closed point of $\pi(X)$ s.t. the residue field is finite separable, as k^{sep} is infinite. Then choose an inverse image, then the residue if finite étaleover k, by(6.6.6.8). This point is clearly closed. □

Prop. (6.6.4.20) [Smoothness at Rational Points]. Let X be a locally algebraic scheme over a field k. Let $x \in X$ that $k(x)/k$ is finite separable, then X is smooth at x iff it is x is a regular point, by(5.4.5.26). ⌟

Prop. (6.6.4.21) [Geo.Reduced Scheme Generic Smooth]. Let X be a locally algebraic scheme over a field k that is geometrically reduced, then it contains an open dense subset that is smooth over k. ⌟

Proof: The problem is local, so we may assume X is affine, consider its irreducible components, all their intersections can be removed, because they are nowhere dense, so we may assume X is irreducible. So X is integral, let η be the generic pt, then $k(\eta)/k$ is separable, by(6.4.3.2). Then choose an affine subscheme $\operatorname{Spec} A \subset X$, then A is smooth at (0) over k, by(5.4.5.29), then by definition, it is smooth on some dense open subscheme of X. □

Tangent Spaces

Def. (6.6.4.22) [Relative Tangent Spaces]. Let X be a scheme over S and $x \in X$, define $T^*_{X/S,x} = \Omega_{X/S,x} \otimes_{\mathcal{O}_{X,x}} k(x)$, and $T_{X/S,x} = \operatorname{Hom}_{k(x)}(T^*_{X/S,x}, k(x)) = \operatorname{Hom}_{\mathcal{O}_{X,x}}(\Omega_{X/S,x}, k(x))$, called the **relative tangent space** of X over S at x.

When $x \in X$ mapping to $s \in S$, $T_{X/S,x} = \operatorname{Hom}_{k(x)}(\mathfrak{m}_x/\mathfrak{m}_x^2, k(x))$, where $\mathfrak{m}_x$ is the maximal ideal of the stalk of $x \in X_s$.

Then it can be verified that for a k-scheme and a rational point $x \in X$, $T_{X,x}$ is in bijection with $\operatorname{Mor}_k(\operatorname{Spec} k[\varepsilon], X)$ that maps the closed point to x. ⌟

Prop. (6.6.4.23) [Tangent Map]. Let $f : X \to Y$ be a morphism of schemes over S, $x \in X$, $f(x) = y$. Assume $k(x) = k(y)$, then f defines a natural linear map

$$\begin{aligned} df : T_{X/S,x} \to T_{Y/S,y} : &\operatorname{Hom}_{\mathcal{O}_{X,x}}((\Omega_{X/S})_x, k(x)) \to \operatorname{Hom}_{\mathcal{O}_{X,x}}((f^*\Omega_{Y/S})_x, k(x))(6.5.5.5) = \\ &\operatorname{Hom}_{\mathcal{O}_{X,x}}(\Omega_{Y/S,y} \otimes_{\mathcal{O}_{Y,y}} \mathcal{O}_{X,x}, k(y)) = \operatorname{Hom}_{\mathcal{O}_{Y,y}}(\Omega_{Y/S,y}, k(y)) \end{aligned}$$

⌟

Cor. (6.6.4.24). Via similar argument, if $k(x) = k(s) = k(y)$, there is an isomorphism

$$T_{X/S,x} \oplus T_{Y/S,y} \cong T_{X \times_S Y,(x,y)}.$$

⌟

Prop. (6.6.4.25). Let X be a scheme over a field k and $x \in X$ with residue field $k(x)$, then the tangent space is canonical isomorphic to $\operatorname{Mor}(k(x)[\varepsilon], X)$ that maps the closed point to x. And the vector bundle structure is given by the cogroup structure on $\operatorname{Spec} k[\varepsilon] : \mu : k[\varepsilon] \otimes k[\varepsilon] \to k[\varepsilon]$. ⌟

Prop. (6.6.4.26) [Krull's Principal Tangent Theorem]. Let $Z \subset X$ be a closed subscheme with ideal of definition $\mathcal{I}$, $x \in Z$, then $T_{Z,x}$ is the subspace of $T_{X,x}$ cut out by $(\mathcal{I} \mod \mathfrak{m}_x^2)$.

In particular, $\mathcal{T}_{Y \cap Z,p} = T_{Y,p} \cap T_{Z,p} \subset T_{X,p}$. ⌟

Prop. (6.6.4.27) [Tangent Criterion of Smoothness]. By(6.6.4.16)(6.6.4.20) and the definition of regular local ring, if X is a locally algebraic scheme over a field k, then X is smooth at a point x with residue field $k(x)/k$ separable iff $\dim_{k(x)} T_{X,x}$ equals($\leq$) the dimension of $\mathcal{O}_{X,x}$. ⌟

Bertini's Theorem

Prop. (6.6.4.28) [Bertini]. Let k be a field. For any quasi-projective scheme $X \subset \mathbb{P}^n_k$ smooth away from f.m. points, there is an open dense subset U of the dual projective space $\mathbb{P}^{n\vee}_k$ s.t. for any closed point $[H] \subset U$, H doesn't contain any component of X, and the scheme $H \cap X$ is smooth over k.

Moreover, if X is a variety and $\dim X \geq 2$, the smooth cut is even a smooth variety by(6.8.6.25)and(6.4.2.10). ⌟

Proof: Let $\mathbb{P}^n = \mathrm{Proj}\, k[x_0, \ldots, x_n], (\mathbb{P}^n)^\vee = \mathrm{Proj}\, k[a_0, \ldots, a_n]$, Let $\overline{X}$ be cut out by equations $f_1, \ldots, f_r$, we define a projective scheme $Z \subset \mathbb{P}^n \times (\mathbb{P}^n)^\vee$ be cut by the equations

- f_r.
- $f_{r+1} = \sum a_i x_i$.
- determinants of $(r+1) \times (r+1)$-minors of $(\frac{\partial f_i}{\partial x_j})_{(r+1)\times n}$.

Now for any $(x, [H]) \in Z$, $x \in X, x \in H$ that $[H]$ is closed in $(\mathbb{P}^n)^\vee$, the last equation means $X \cap H$ is non-smooth at p or contains the irreducible component passing p, by Jacobian criterion(6.6.4.12). Now consider the projection $Z \to X$, for each closed point $p \in X$ that $\dim_p X = d$, the codimension of the fiber of Z over x is of dimension $r-1 = n - \dim_x X - 1$(To see this, one way is use regularity and tangent space, another way is to use the fact (x_i) is orthogonal to $(\frac{\partial f_i}{\partial x_j})_j$ for all i by Euler identity, so the $r+1$ restrictions of (a_i) are linearly independent), then by(6.6.3.17), $\dim Z = \dim \pi_1^{-1}(Z) \leq n-1$, Thus the image of Z in $\mathbb{P}^{n\vee}_k$ is also a closed subscheme of dimension$\leq n-1$.

If X has f.m. singular points, we also need to cut out the surfaces $N_{k(x)/k}(\sum x_i^k a_i)$, where (x_i^j) are the f.m. closed singular points of x. They are also of dimension $n-1$. □

Cor. (6.6.4.29) [Bertini's Theorem for Surfaces]. Similarly, for any $d \geq 0$, a generic dimension d surface intersect X at a smooth subscheme, by using Veronese embedding. ⌟

Cor. (6.6.4.30). When $X \subset \mathbb{P}^n_k$ is a projective k-variety where k has characteristic 0, the scheme Z in $\mathbb{P}^{n\vee}_k$ is called the **dual variety** of X. When X is irreducible and smooth, it is of dimension $n-1$. ⌟

Proof: □

Prop. (6.6.4.31). The dual variety of the dual variety is X itself. ⌟

Proof: Cf.[Joe Harris, Algebraic Geometry, 15.24]. □

Prop. (6.6.4.32) [Kleinman-Bertini]. Let X be a k-variety that is homogenous space for a k-variety G over a field k, suppose $\alpha : Y \to X, \beta : Z \to X$ are morphisms of varieties, then

- There is a non-zero open subset $V \subset G$ that for any closed point $\sigma \in V$, $\dim \sigma(Y) \times_X Z = \dim Y + \dim Z - \dim X$.
- If Y, Z are smooth over k of characteristic 0, then there is a non-empty open subset $V \subset G$ that $(G \times_k Y) \times_X Z \to G$ is smooth. In particular, for any closed point $\sigma \in V$, $\sigma(Y) \times_X Z$ is smooth over $k(\sigma)$ of dimension $\dim Y + \dim Z - \dim X$.

⌟

Proof: Let $\Gamma = (G \times_k Y) \times_X Z$, then there is a map $\Gamma \to Y \times_k Z$. $Y \times_k Z$ has dimension $\dim Y + \dim Z$ by(6.6.3.21), and there is a base change diagram

$$\begin{array}{ccc} (G \times_k Y) \times_X Z & \longrightarrow & Y \times_k Z \\ \downarrow & & \downarrow \\ G \times_k X & \longrightarrow & X \times_k X \end{array},$$

and $G\times X\to X\times X$ is flat as it is equivariant under $G\times G$-action, by(6.6.2.15), thus $\Gamma\to Y\times_k Z$ is flat of relative dimension $\dim G-\dim X$, thus it has dimension $\dim Y+\dim Z+\dim G-\dim X$.

1: This follows from(6.6.3.19) applied to the map $G\times_k Y\times_X Z\to G$.

2: As $G\times X\to X\times X$ is flat, and its fiber are isomorphic to G_x, which is the fiber of the map $o_x: G\to X$, and this map is smooth by(6.6.4.14), thus $G\times X\to X\times X$ is smooth, and then the assertion follows from(6.6.4.14). □

Cor. (6.6.4.33). Let Z be a smooth k-variety where $\mathrm{char} k=0$. Let V be a f.d. basepoint-free line series on Z, then the section of a general element of V is smooth. ⌟

Proof: Apply Kleinman-Bertini to $\varphi_V: Z\to \mathbb{P}V^\vee$, $Y=V(\sum a_i x_i)\in PV\times PV^\vee\to PV^\vee$, $X=PV^\vee$. □

5 Unramified

More advanced materials to learn at [Sta]Chap40.

Def. (6.6.5.1) [Unramified Morphism]. A morphism is called **(G-)unramified** iff there is an open affine cover U_i and an open affine cover of $f^{-1}(U_i)$ that the induced ring map is (G-)unramified(5.4.6.4). Equivalently, $\Omega_{X/S}=0$ and it is locally of f.t.(f.p.).

(G-)unramifiedness is local on the source and target(6.4.1.5)(6.4.1.6). (G-)unramifiedness is stable under base change and composition(5.4.6.4). Moreover, unramifiedness satisfies the base change trick. ⌟

Prop. (6.6.5.2). An unramified map is locally quasi-finite. ⌟

Proof: Cf.[Sta]02V5. □

Prop. (6.6.5.3) [Fiberwise]. A morphism is (G-)unramified iff it is locally of f.t.(f.p.) and all the fibers X_s are disjoint unions of spectra of finite separable extensions of $k(p)$. ⌟

Proof: By(5.4.6.7), Notice $pS_q=qS_q$ is equivalent to every q is minimal in X_p, which is equivalent to X_p is discrete. □

Cor. (6.6.5.4) [Unramified over Fields]. A scheme over a field k is unramified iff it is a disjoint union of spectra of finite separable extensions of k, because locally of f.p. is trivially satisfied. ⌟

Prop. (6.6.5.5) [Diagonal is Open]. A morphism $X\to S$ is (G-)unramified iff it is of f.t.(f.p.) and the diagonal is a clopen immersion of X, thus all of X. ⌟

Proof: If it is unramified, then the diagonal is an open immersion by(5.4.6.10). Conversely, $\Omega_{X/S}$ is just the conormal sheaf of the diagonal map, so it is zero. □

Cor. (6.6.5.6) [Sections of Unramified Morphism]. Any section of an unramified morphism is an open immersion. In particular, a section of a separable unramified morphism is a clopen immersion. ⌟

Proof: This follows from the proposition and the fact $S\to X$ is a base change of $\Delta_{X/S}$. □

Cor. (6.6.5.7). Let X,Y be schemes over S, if f,g are two maps from X to Y, then if Y/S is unramified and f,g are equal on a pt x of X(both on image and residue field), then there is a nbhd of x that f,g are equal. ⌟

Proof: This follows as $\Delta_{Y/S}$ is open immersion, so the set that f, g are equal is open in X. □

Prop. (6.6.5.8) [Fiberwise]. For a morphism $f : X \to S$ locally of f.t.(f.p.), let $x \in X, s = f(x)$, then the following are equivalent:

- It is (G-)unramified at x,
- The fiber X_s is unramified over $k(s)$ at x, by(6.6.5.3).
- $\Omega_{X_s,x} = 0$.
- $\Omega_{X_s/s,x} \otimes_{\mathcal{O}_{X_s,x}} k(x) = \Omega_{X/S,x} \otimes_{\mathcal{O}_{X,x}} k(x) = 0$ by(5.4.6.6).
- $\mathfrak{m}_s\mathcal{O}_{X,x} = \mathfrak{m}_x$ and $k(x)/k(f(x))$ is separable.

┘

Proof: $1 \to 2 \to 3 \to 4$ is clear. $4 \to 1$: Nakayama implies $\Omega_{X/S,x} = 0$, thus $\Omega_{X/S}$ vanishes on a nbhd of x as it is Qco of f.t..

$4 \iff 5$ follows from(5.4.6.7). □

Cor. (6.6.5.9) [Generic Unramifiedness]. Let $f : X \to Y$ be a finite separable dominant morphism of integral schemes, then there exists an open dense nbhd U of Y s.t. $f : f^{-1}(U) \to U$ is unramified. ┘

Prop. (6.6.5.10). If $X \to Y \to S$ is unramified, then X/Y is also unramified. And if X/S is G-unramified and Y/S is of f.t., then X/Y is G-unramified. ┘

Proof: By(6.6.1.4)and(6.5.5.5). □

Prop. (6.6.5.11) [Unramified Points Base Change]. If f is of f.t.(f.p.), then the set of points of S that f is unramified is stable under base change. ┘

Proof: □

Prop. (6.6.5.12)[Tangent Criterion of unramifiedness]. Let $f : X \to Y$ be a morphism of schemes locally of f.t. over S, $x \in X, y = f(x)$, then the following are equivalent:

- $df : T_{X/S,x} \to T_{Y/S,y}$ is an injection(6.6.4.23).
- f is unramified at x.

┘

Proof: It follows from(6.6.4.23) that df is an isomorphism iff $(f^*\Omega_{Y/S})_x \otimes_{\mathcal{O}_{X,x}} k(x) \to \Omega_{X/S,x} \otimes_{\mathcal{O}_{X,x}} k(x)$ is surjective, which by Jacobi-Zariski(6.5.5.5) is equivalent to $\Omega_{X/Y,x} \otimes_{\mathcal{O}_{X,x}} k(x) = 0$, and this is equivalent to f is unramified at x by(6.6.5.8). □

Prop. (6.6.5.13) [Unramified U.i. Morphisms]. For a morphism f of schemes, the following are equivalent:

- f is unramified and a monomorphism.
- f is unramified and universal injective.
- f is locally of f.t., formally unramified and universal injective.
- f is locally of f.t. and a monomorphism.
- f is locally of f.t. and X_y is either empty or $X_y \to y$ is an isomorphism for all $y \in Y$.

┘

Proof: Cf.[Sta], 05VH. □

Prop. (6.6.5.14) [Unramified and Smoothness]. Let $f : X \to Y$ be a morphism of schemes over S s.t. X/S is smooth(of relative dimension n) and Y/S is unramified, then f is also smooth(of relative dimension n). ⌟

Proof: This follows from differential criterion(6.6.4.3) and(6.6.1.4). Notice to show it is flat, use the fact $\Delta_{Y/S}$ and $X \times Y \to Y$ are both flat(6.6.5.5). □

<u>**Noetherian Case**</u>

Prop. (6.6.5.15). Let S be a Noetherian scheme, $X \to S$ a qc unramified morphism and $Y \to S$ a morphism with Y Noetherian, then $\mathrm{Mor}_S(Y, X)$ is a finite set. ⌟

Proof: Cf.[Sta], 0AKI. □

Prop. (6.6.5.16) [Unramified Morphisms and DVR]. Let R_v be a DVR with fraction field K and $\varphi : X \to X'$ be a morphisms of schemes of f.t. over R_v. Let $Q \in X'(K)$ and $P \in X(\overline{K})$ with $\varphi(P) = Q$. Let $w|v$ be a valuation of $K(P)$ extending v. If P extends to an R_w-valued point $\overline{P}$ of X, then using the fact $R_w \cap K = R_v$, we see Q also extends to a R_v-valued point of X'.

Denote the image of the maximal ideal of R_w under $\overline{P}$ by $P(w)$, then if φ is unramified at $P(w)$, then $K(P)/K$ is unramified in w. ⌟

Proof: Since the unramified point is open, φ is also unramified at P, thus $K(P)/K$ is separable(6.6.5.8). For the rest, Cf.[Diophantine Geometry, P598]**?**. □

6 Étale

More advanced materials to learn at [Sta]Chap40.

Def. (6.6.6.1) [Étale Morphisms]. An **étale morphism** $f : X \to Y$ of schemes is a morphism s.t there is an open affine cover $\{U_i\}$ of S and an open affine cover V_{ij} of $f^{-1}(\{U_i\})$ that the ring map is étale. A **standard étale morphism** is the Spec map of a standard étale ring map.

étale is local on the source and target(5.4.7.5). Étale is stable under base change and composition(5.4.7.5). ⌟

Prop. (6.6.6.2) [Properties of Étale Morphisms].

- Étale at a point x is equivalent to smooth and unramified at a x(5.4.7.4).
- Étale at a point x is equivalent to flat and G-unramified at that point, by(5.4.7.11). So étaleover field is equivalent to G-unramified, because over a field it is obviously flat.
- Étale at a point x is equivalent to locally standard étale at that point(5.4.7.17).
- A morphism is étale iff it is smooth of relative dimension 0, by definition(6.6.4.11).
- Étale is equivalent to flat, locally of f.p. and formally unramified, by(5.4.7.11).

⌟

Cor. (6.6.6.3). Étale map is smooth, hence syntomic, flat.

Étale map is universally open because it is flat and locally of f.p.(6.6.2.10). ⌟

Prop. (6.6.6.4). If X, Y are étaleover S, then any map $X \to Y$ is étale, by(5.4.7.13). ⌟

Prop. (6.6.6.5) [Fiberwise]. A morphism of schemes is étale iff it is flat, locally of f.p., and every fiber X_s is a disjoint union of spectra of finite separable field extensions of $k(s)$. ⌟

Proof: Follows from (6.6.6.2)(6.6.5.3) and (5.4.7.10). □

Cor. (6.6.6.6) [Étale Over Fields]. A scheme is étale over a field k iff it is a disjoint union of spectra of finite separable field extensions. In particular, étaleover fields is equivalent to unramified over fields. ⌟

Prop. (6.6.6.7) [Smoothness and Étale]. If $f: X \to Y$ is smooth at x, then there exist a nbhd U of $x \in X$ and nbhd V of $f(x) \in Y$ that it factors through $U \xrightarrow{\pi} \mathbb{A}^d \to V$, where π is étale. ⌟

Proof: Any standard smooth morphism can be factorized as an étalemap over a polynomial algebra, as easily seen. □

Prop. (6.6.6.8) [Stalkwise and Fiberwise]. For a morphism locally of f.p., by (6.6.5.8) and (6.6.4.5), the following are equivalent:

- It is étale at a point x.
- $\mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)}$ if flat and $X_{f(x)}/k(x)$ is smooth at x.
- $\mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)}$ if flat and $X_{f(x)}/k(x)$ is unramified at x.
- $\mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)}$ is flat and $\Omega_{X_{f(x)},x} = 0$.
- $\mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)}$ is flat and $\Omega_{X_s/s,x} \otimes_{\mathcal{O}_{X_s,x}} k(x) = \Omega_{X/S,x} \otimes_{\mathcal{O}_{X,x}} k(x) = 0$.
- $\mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)}$ is flat and $\mathfrak{m}_{f(x)}\mathcal{O}_{X,x} = \mathfrak{m}_x$ and $k(x)/k(s)$ separable.

In particular, an étalemorphism can be seen as a family of smooth schemes. ⌟

Prop. (6.6.6.9) [Étale Schemes over Field]. Let k be a field and k^s its separable closure. Let $\Gamma = \mathrm{Gal}(k^s/k)$, then the functor $X \mapsto X(k^s)$ is an equivalence between étale schemes over k to the category of discrete Γ-sets. ⌟

Proof: Cf. [Sta]03QR. ? □

Prop. (6.6.6.10). If $X \to Y \to S$, and $X \to Y$ are faithfully flat and locally of f.p., $X \to S$ is étale, then $Y \to S$ is also étale. ⌟

Proof: Cf. [Sta]05B5. □

Cor. (6.6.6.11). If $f: X \to S$ is faithfully flat and locally of f.p., then the set of points of S s.t. f is étale is table under base change. ⌟

Proof: This follows from (6.6.5.11) and (6.6.4.10). □

Def. (6.6.6.12) [Étale Neighborhood]. For a point $s: \mathrm{Spec}\, k \to X$, an étale nbhd of s in X is defined to be an étale map $U \to X$ that s factors through U. ⌟

Prop. (6.6.6.13). For a morphism $f: Y \to X$ of schemes étale over field k, then f is surjective iff $Y(k_s) \to X(k_s)$ is surjective. ⌟

Proof: If $Y \to X$ is surjective, then ? □

Étale Connected Components

Def. (6.6.6.14) [Étale Connected Components]. Let X be a scheme over a field k, let $\pi_0(X) = \mathrm{Spec}(\pi(X))$, where $\pi(X)$ is the largest étale subalgebra of $\Gamma(X)$(5.4.7.23). ⌟

Prop. (6.6.6.15). Let X be an algebraic scheme over a field k, then

- for any field extension k'/k, $\pi_0(X_{k'}) = \pi_0(X)_{k'}$.
- Let Y be a schemes over a field k, then $\pi_0(X \times Y) = \pi_0(X) \times \pi_0(Y)$.

⌟

Proof: 1: Cf.[Mil17b]P15.

2: There is a map $\pi(X) \times_k \pi(Y) \to \pi(X \times Y)$. Because π commutes with base change, we can base change to separable closure. In this case, it suffices to show if X, Y is connected then $X \times Y$ is connected, but this follows from(6.4.3.12). □

Prop. (6.6.6.16). Let X be an algebraic scheme over a field k, then

- The mapping $\varphi : X \to \pi_0(X)$ induces a 1 to 1 correspondence of points of $\pi_0(X)$ and connected components of X.
- For all $x \in \pi_0(X)$, the fiber $\varphi^{-1}(x)$ is geo.connected over $k(x)$.

⌟

Proof: $\pi_0(X)$ is discrete, so the inverse image of each point is a sum of connected components of X. But this must be connected, because $\pi_0(X_{k(x)}) = \pi_0(X)_{k(x)} = k(x)$. Also, this implies for the alg.closure $\overline{k}$ of $k(x)$, $\pi_0(X_{\overline{k}}) = \pi_0(X_{k(x)})_{\overline{k}} = \overline{k}$, thus $X_{\overline{k(x)}}$ is geo.connected. □

Noetherian Case

7 Zariski's Main Theorem

References are [Sta]Chap36.38.

Prop. (6.6.7.1)[Zariski's Main Theorem]. For a morphism $X \to S$ that is quasi-finite and separated, if S is qcqs, Then there is a factorization $X \to T \to S$ that $X \to T$ is a qc open immersion and $T \to S$ is finite. ⌟

Proof: Cf.[[Sta]05K0]. □

8 Complete Intersection

Should be refreshed with intrinsic definition of locally complete intersection, Cf.[Sta].

Def. (6.6.8.1) [Regular Embedding]. A **regular embedding** of codimension r is a locally closed embedding $X \to Y$ that for $p \in X$, the ideal of X in the local ring $\mathcal{O}_{Y,p}$ is generated by a regular sequence of length r. ⌟

Def. (6.6.8.2)[Complete Intersection]. A **complete intersection** of codimension r in Y is a closed subscheme X that is the intersection of r effective Cartier divisors D_i that at each point $p \in X$, the equations defining D_i form a regular sequence. ⌟

Def. (6.6.8.3) [Locally Complete Intersection]. A closed subscheme Y of a nonsingular variety X over a field k is called **locally complete intersection** iff Y is locally generated by $r = \operatorname{codim}(Y, X)$ elements. By(5.3.4.17) Y is C.M.. In particular, by(6.11.1.16), a regular variety is always a locally complete intersection. ⌟

Def. (6.6.8.4) [Syntomic Morphisms]. A **standard syntomic morphism** is the Spec map of a global complete intersection ring map(5.4.4.11). A **syntomic morphism** is a morphism that is locally a standard syntomic morphism. ⌟

Prop. (6.6.8.5). Syntomic is local on the source and target, stable under base change and composition, by(5.4.4.12). ⌟

Prop. (6.6.8.6). Syntomic is equivalent to flat, locally of f.p.+fibers being local complete intersections. ⌟

Proof: This follows from(5.4.4.18). □

Cor. (6.6.8.7). Syntomic morphisms are universally open. ⌟

Prop. (6.6.8.8). An open immersion is syntomic, because localizations are global complete intersections(5.4.4.12). ⌟

Prop. (6.6.8.9). If $f : X \to S$ is a syntomic map, then the function $x \mapsto \dim_x(X_{f(x)})$ is locally constant on X. If it is standard syntomic, then it is constant. ⌟

Proof: It suffices to prove for syntomic maps, Cf.[Sta]02K0. □

Prop. (6.6.8.10). A local complete intersection has its ideal sheaf $\mathcal{I}$, then $\mathcal{I}/\mathcal{I}^2$ locally free by(5.3.4.16). ⌟

Prop. (6.6.8.11). If Y is a complete intersection in $\mathbb{P}^n_k$ of hypersurfaces of degree $d_1, \ldots, d_r$, then $\omega_Y = \mathcal{O}_Y(\sum d_i - n - 1)$. ⌟

Proof: Use the exact sequence $0 \to \mathcal{O}_Z(n-d) \to \mathcal{O}_Z \to i_*\mathcal{O}_Y \to 0$ and(6.11.1.17). □

Prop. (6.6.8.12). For a complete intersection of dimension q, $H^i(Y, \mathcal{O}_Y(n)) = 0$ for $0 < i < q$. And the natural map $\Gamma(P, \mathcal{O}_P(n)) \to H^0(Y, \mathcal{O}_Y(n))$ is a surjection for every n. In particular, Y is connected, and the arithmetic genus $p_a(Y) = \dim H^q(Y, \mathcal{O}_Y)$. ⌟

Proof: We use induction, the case $Y = P$ follows from(6.7.2.1), let $Y = Z \cap H$, where H has degree d, then

$$0 \to \mathcal{O}_Z(n-d) \to \mathcal{O}_Z \to i_*\mathcal{O}_Y \to 0$$

thus use long exact sequence. The rest is easy. □

6.7 Cohomology of Schemes

Main references are [Sta]Chap29.

Notation (6.7.0.1).
- Use notations defined in Cohomology on Ringed Sites.

⌟

1 Zariski Cohomology

Qco Sheaves

Lemma (6.7.1.1) [Zariski-Poincare]. A Qco sheaf on an affine scheme X is Čech-acyclic. ⌟

Proof: Because the principal affine covers are cofinal in the ordering of covers, we only need to consider principal affine covers. Let $R \to A = \prod R_{f_i}$, then it is f.f., so we can use(5.4.2.2), just notice the higher term is $\prod_{i_0,\ldots,i_n} R_{f_{i_0}\cdots f_{i_n}}$. □

Prop. (6.7.1.2)[Čech Cohomology on Separated Schemes]. If X is separated and $\mathcal{F} \in \mathfrak{QCoh}(X)$, $H^p(X,\mathcal{F}) = \check{H}^p(X,\mathcal{F}) = H^p_{\text{alt}}(\{U_i \to X\}, F)$ for any open affine covering $\{U_i \to X\}$. ⌟

Proof: Use(6.3.2.16) and(6.3.2.6), the family of affine open subsets of X satisfies the requirement because X is separated and(6.7.1.1), thus the result It can be calculated by alternating complexes by(6.3.2.7). □

Cor. (6.7.1.3) [Affine Cohomological Vanishing]. If X is affine and $\mathcal{F} \in \mathfrak{QCoh}(X)$, $H^i(X,\mathcal{F}) = 0$ for $i > 0$.

For a qcqs scheme X, choose a finite affine cover $U_1, \ldots, U_t$ of X, then for any $\mathcal{F} \in \mathfrak{QCoh}(X)$, $H^n(X,\mathcal{F}) = 0$ for $n \geq d$, where

$$d = \max_{I \subset \{1,\ldots,t\}} (\#I + t(U_I))$$

and $t(Y)$ is the minimal cardinality of an affine open cover of Y. ⌟

Proof: The last assertion follows form Čech to sheaf2(6.3.2.13) and(6.7.1.2), as U_I is separated for any $I \neq \varnothing$. □

Remark (6.7.1.4). Compare with(7.2.0.4)**?**. ⌟

Prop. (6.7.1.5) [$\mathfrak{QCoh}(X)$ vs. $\mathcal{M}od(\mathcal{O}_X)$]. If X is a Noetherian scheme, then injective objects in $\mathfrak{QCoh}(X)$ are all flabby(6.3.4.8), thus nearly calculating all cohomologies are legitimate in the category $\mathfrak{QCoh}(X)$.

However, in general, this is not true, as there are examples of injective A-module $\mathcal{I}$ s.t. $\widetilde{I}$ is not flask on Spec A, by [Sta]0274. ⌟

Proof: We use the Deligne formula(6.5.1.36) and the definition of injective, by considering the sheaf of ideals of the corresponding induced reduced structure. □

Prop. (6.7.1.6)[Filtered Colimits]. By(6.3.1.16), if X is qcqs, then sheaf cohomology on X commutes with filtered colimits. ⌟

Prop. (6.7.1.7)[$\mathcal{E}xt$ For Coherent Sheaves]. On a locally Noetherian scheme, for $\mathcal{F} \in \mathfrak{QCoh}(X)$ and $\mathcal{G} \in \mathfrak{Coh}(X)$, $\mathcal{E}xt^i(\mathcal{F}, \mathcal{G}) \in \mathfrak{QCoh}(X)$, and affine locally are given by $\mathrm{Ext}^i(\mathcal{F}(U), \mathcal{G}(U))$.

Moreover $\mathcal{G} \in \mathfrak{Coh}(X)$, then $\mathcal{E}xt^i(\mathcal{F}, \mathcal{G}) \in \mathfrak{Coh}(X)$. ⌟

Proof: This follows from(6.8.5.13) and(6.8.5.10). □

Prop. (6.7.1.8). When X is locally Noetherian and $\mathcal{F} \in \mathfrak{Coh}(X)$,

$$\mathcal{E}xt^i(\mathcal{F}, \mathcal{G})_x \cong \mathrm{Ext}^i_{\mathcal{O}_x}(\mathcal{F}_x, \mathcal{G}_x).$$

⌟

Proof: Taking stalk is exact.**?** □

Cor. (6.7.1.9). If X is locally Noetherian, suppose that every coherent sheaf is a quotient of a locally free sheaf, we can define the **homological dimension** $hd(\mathcal{F})$ of a coherent sheaf $\mathcal{F}$ as the minimal length of a flat resolution of $\mathcal{F}$. Then $hd(\mathcal{F}) \leq n \iff \mathcal{E}xt^i(\mathcal{F}, \mathcal{G}) = 0$ for every $\mathcal{G}$ and every $i > n$. And $hd(\mathcal{F}) = \sup pd_{\mathcal{O}_{X,x}} \mathcal{F}_x$, by(6.7.1.8). ⌟

Prop. (6.7.1.10) [Künneth Formula]. If X, Y are qcqs over a field k and $\mathcal{F}, \mathcal{G}$ be Qco $\mathcal{O}_X, \mathcal{O}_Y$-modules, then there is a canonical isomorphism:

$$H^n(X \times_{\mathrm{Spec}\, k} Y, \mathrm{pr}_1^* \mathcal{F} \otimes_{\mathcal{O}_{X \otimes_{\mathrm{Spec}\, k} Y}} \mathrm{pr}_2^* \mathcal{G}) \cong \oplus_{p+q=n} H^p(X, \mathcal{F}) \otimes_k H^q(Y, \mathcal{G}).$$

⌟

Proof: Cf.[Sta]0BEF.**?** □

Prop. (6.7.1.11). On a locally Noetherian scheme X, any Qco sheaf $\mathcal{F}$ admits a resolution of Qco sheaves that are flabby. ⌟

Proof: Because $\mathfrak{QCoh}(X)$ is Serre subcategory,**?** □

Lemma (6.7.1.12) [Gabber]. Let X be a scheme, then there exists a cardinal κ that every Qco sheaf is a colimit of its κ-generated Qco subsheaves. ⌟

Proof: Cf.[Sta]077N. □

Prop. (6.7.1.13) [Qco Cohomology Comparison]. For $X \in \mathfrak{Sch}, \mathcal{F} \in \mathfrak{QCoh}(X), \tau \in$\{fppf, étale, smooth, syntomic, Zariski\}, there are canonical isomorphisms

$$H^p(X, \mathcal{F}) \cong H^p(\mathfrak{Sch}_\tau /X, \mathcal{F}) \cong H^p(X_{\mathrm{Zar}}, \mathcal{F}) \cong H^p(X_{\text{ét}}, \mathcal{F}).$$

⌟

Proof: Let $\mathcal{C} = \mathfrak{Sch}_\tau /X$ or $X_{\text{ét}}, X_{\mathrm{Zar}}$. We use(6.3.2.16) with $\mathfrak{G}$ the set of affine schemes and Cov the subset of $\mathrm{Cov}(\mathcal{C})$ consisting of morphisms between affine schemes. Then Čech vanishing is clear in the affine case by(5.4.2.2). Thus(6.3.2.16) says $H^p(\mathcal{C}, \mathcal{F}_{\mathcal{C}}) = 0$ for $p > 0$.

Next, if $U \subset X$ is an affine open s.t. $U \to X$ is separated. Let $\mathcal{U}$ be an affine open covering of U, then all $U_{i_0,\ldots,i_p}$ are affine, thus

$$H^p(\mathcal{C}, \mathcal{F}_{\mathcal{C}}) = \check{H}(\mathcal{U}, \mathcal{F}_{\mathcal{C}}) = H^p(U, \mathcal{F}|_U)$$

by(6.3.2.15).

Finally, for X, take an injective resolution $\mathcal{F}\to\mathcal{I}^\bullet$, and an injective resolution $\mathcal{F}_\mathcal{C}\to\mathcal{J}^\bullet$. Then the latter restricts to a chain complex $\mathcal{F}\to\mathcal{J}^\bullet|_X$, which is exact because it is exact on any affine open $U\subset X$ as $H^p(\mathcal{C},\mathcal{F}_\mathcal{C})=0$ for $p>0$. Thus by(4.10.2.5), there is a map $\mathcal{J}^\bullet|_X\to\mathcal{I}^\bullet$, inducing a map $H^p(\mathcal{C},\mathcal{F}_\mathcal{C})=H^p(X,\mathcal{J}^\bullet)\to H^p(X,\mathcal{I}^\bullet)\cong H^p(X,\mathcal{F})$.

To show these map are isomorphisms, take an affine open covering $\mathcal{U}$ of X, then there are Čech-to-derived spectral sequences

$$^\tau E_2^{p,q}=\check{H}^p(\mathcal{U},\mathcal{H}^q(\mathcal{F}^a))\Rightarrow H^{p+q}(\mathcal{C},\mathcal{F}_\mathcal{C}),\quad E_2^{p,q}=\check{H}^p(\mathcal{U},\mathcal{H}^q(\mathcal{F}^a))\Rightarrow H^{p+q}(\mathcal{C},\mathcal{F}).$$

The map $\mathcal{J}^\bullet|_X\to\mathcal{I}^\bullet$ induces a map $\check{C}^\bullet(\mathcal{U},\mathcal{J})\to\check{C}^\bullet(\mathcal{U},\mathcal{I})$ which induces a map of the spectral sequences. But as each affine open of X is separated over X, the E^2-page is an isomorphism by what we have proved. Thus $\mathcal{H}^q(\mathcal{F}^a))\to H^{p+q}(\mathcal{C},\mathcal{F})$ is an isomorphism. □

Prop. (6.7.1.14). For $X\in\mathcal{S}\mathrm{ch},\tau\in$\{fppf, étale, smooth, syntomic, Zariski\},

$$H^1_\tau(X,\mathbb{G}_m)\cong\mathrm{Pic}(X)(6.5.3.10).$$

⌟

Proof: As these X_τ are all locally ringed sites, by(6.3.1.17), $H^1_\tau(X,\mathbb{G}_m)\cong\mathrm{Pic}(X_\tau)$. Thus it suffices to prove that

$$\mathrm{Pic}(X_{\mathrm{Zar}})\to\mathrm{Pic}(X_{\text{ét}})\to\ldots\to\mathrm{Pic}(X_{\mathrm{fppf}})$$

are isomorphisms. Then this is because any invertible sheaf is quasi-coherent by(6.2.5.8), so $\mathrm{Pic}(X_\tau)$ are in fact the group of invertible objects in $\mathcal{QC}\mathrm{oh}(X_\tau)$. But $\mathcal{QC}\mathrm{oh}(X_\tau)$ are all equivalent categories, by fpqc descent for Qco sheaves(6.1.5.12). □

2 Proper Schemes

Prop. (6.7.2.1) [Cohomology of Projective Space]. Let $X=\mathbb{P}^r_A$ we have:

(1)

$$H^q(X,\mathcal{O}_X(d))=\begin{cases}(A[T_0,\ldots,T_r])_d & q=0\\ 0 & q\neq 0,r\\ (\frac{1}{T_0\ldots T_r}A[\frac{1}{T_0},\ldots,\frac{1}{T_r}])_d & q=r\end{cases}$$

(2) The cup product defines a perfect pairing

$$H^0(X,\mathcal{O}_X(n))\times H^r(X,\mathcal{O}_X(-n-r-1))\to H^r(X,\mathcal{O}_X(-r-1))\cong A.$$

⌟

Proof: X is separated, we use Cech cohomology. Let $\mathcal{F}=\oplus_{d\in\mathbb{Z}}\mathcal{O}_X(d)$, then $\mathcal{F}$ is a Qco graded ring. Let $U_{i_0,\ldots i_k}$ be the affine open subset $U(x_{i_0})\cap\ldots U(x_{i_k})$ of X, then $\mathcal{F}(U_{i_0,\ldots,i_k})=A[T_0,\ldots,T_r,T_{i_0}^{-1},\ldots,T_{i_k}^{-1}]$ as graded rings, and the cohomology $H^\bullet(\mathcal{F})$ is calculated by the Čech complex(6.3.2.1)

$$\check{C}^\bullet=\prod_i A[T_0,\ldots,T_r,T_i^{-1}]\to\prod_{i,j}A[T_0,\ldots,T_r,T_i^{-1},T_j^{-1}]\to\ldots\to A[T_0,\ldots,T_r,T_1^{-1},\ldots,T_r^{-1}].$$

This complex has a natural $\mathbb{Z}^r$-grading, and the differential is natural inclusion thus preserves the grading, i.e.

$$\check{C}^\bullet = \bigoplus_{v\in\mathbb{Z}^r} \check{C}^\bullet(v)$$

where if we set $NEG(v) = \{i \in \{0, \ldots, r\} | v_i < 0\}$, then

$$\check{C}^\bullet(v) = \prod_{NEG(v)\subset\{i\}} AT_0^{v_0}\ldots T_r^{v_r} \to \prod_{NEG(v)\subset\{i,j\}} AT_0^{v_0}\ldots T_r^{v_r} \to \ldots \to AT_0^{v_0}\ldots T_r^{v_r}$$

is the subcomplex of $\check{C}^\bullet$. So it suffices to calculate the cohomology of $\check{C}^\bullet(v)$ for each v.

If $NEG(v) = \{0, 1, \ldots, n\}$, then there is only one term, so

$$H^\bullet(\check{C}^\bullet(v)) = \begin{cases} AT_0^{v_0}\ldots T_r^{v_r} & q = r \\ 0 & \text{otherwise} \end{cases}.$$

The sum of all such v clearly contribute to $\frac{1}{T_0\ldots T_r}A[\frac{1}{T_0}, \ldots, \frac{1}{T_r}]$ in degree r.

If $NEG(v) = 0$, then the complex is isomorphic to the Čech complex calculating cohomology of $\operatorname{Spec} A$ using the trivial cover $\{V_i \to \operatorname{Spec} A\}, V_i \cong \operatorname{Spec} A$ times $T_0^{v_0}\ldots T_r^{v_r}$. As Spec is separated, it is just to the sheaf cohomology of $\operatorname{Spec} A$, which is A is degree 0 and 0 otherwise by(6.7.1.1). The sum of all such v clearly contribute to $A[T_0, \ldots, T_r]$ in degree 0.

Finally, for other v, choose a $j \in \{0, 1, \ldots, n\}\backslash NEG(v)$, then the maps

$$h : \check{C}^{p+1}(v) \to \check{C}^p(v) : h(s)_{i_0\ldots i_p} = s_{ji_0 i_p}$$

(where we are using the alternating Čech complex) induces a homotopy between 0 and id, so $\check{C}^{p+1}(v)$ have trivial cohomologies.

The pairing given by cup product makes $T_0^{v_0}\ldots T_r^{v_r}$ dual to $T_0^{-1-v_0}\ldots T_r^{-1-v_r}$, thus it is a perfect pairing. □

Cor. (6.7.2.2). when $n > 0$, $H^r(X, \mathcal{O}_X(n-r-1)) = 0$. Notice this an instance of the Kodaira vanishing theorem when k has characteristic 0(12.9.7.3). ⌟

Prop. (6.7.2.3). Let $X = \mathbb{P}_k^n$ and $0 \le p, q \le n$, then $H^q(X, \Omega_X^p) = 0$ for $p \ne q$ and when $p = q$, $H^q(X, \Omega_X^p) = k$. ⌟

Proof: By(6.5.1.26) and(6.5.5.7), there is an exact sequence $0 \to \Omega^q \to \wedge^q\mathcal{O}(-1) \to \Omega^{q-1} \to 0$, and the middle has vanishing q-th cohomology by(6.7.2.1), thus we can induct and (6.7.2.1) gives the result. □

Prop. (6.7.2.4) [Cohomology of Complete Intersections]. Let X be a closed subscheme of $\mathbb{P}_k^n$ defined by a single homogenous equation $f(x_0, x_1, x_2)$ of degree d, then show that $\dim H^0(X, \mathcal{O}_X) = 1$, and if $n \ge 2$, $\dim H^1(X, \mathcal{O}_X) = (d-1)(d-2)/2$. ⌟

Proof: By(6.5.3.15), there is an exact sequence of sheaves on $\mathbb{P}_k^n$:

$$0 \to \mathcal{O}_{\mathbb{P}_k^n}(-d) \cong \mathcal{O}_{\mathbb{P}_k^n}(-X) \to \mathcal{O}_{\mathbb{P}_k^n} \to i_*\mathcal{O}_X \to 0$$

which induces a long exact sequence(6.7.4.2):

$$H^0(\mathbb{P}_k^n, \mathcal{O}_{\mathbb{P}_k^n}(-d)) \to H^0(\mathbb{P}_k^n, \mathcal{O}_{\mathbb{P}_k^n}) \to H^0(X, \mathcal{O}_X) \to H^1(\mathbb{P}_k^n, \mathcal{O}_{\mathbb{P}_k^n}(-d))$$

$$\to H^1(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k}) \to H^1(X, \mathcal{O}_X) \to H^2(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k}(-d)) \to H^2(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k})$$

By(6.7.2.1), this reads:

$$0 \to k \to H^0(X, \mathcal{O}_X) \to 0 \to 0 \to H^1(X, \mathcal{O}_X) \to H^2(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k}(-d)) \to 0,$$

and if $n = 2$, $\dim H^2(\mathbb{P}^2_k, \mathcal{O}_{\mathbb{P}^n_k}(-d)) = (d-1)(d-2)/2$.

? It is faster using Hilbert Polynomial. □

Lemma (6.7.2.5) [Cohomology of Projective Space]. Let R be a Noetherian ring and $n \geq 0$, then for any coherent sheaf $\mathcal{F}$ on $\mathbb{P}^n_R$,

- $H^i(\mathbb{P}^n_R, \mathcal{F}(n)) = 0$ for $i > 0$ and n large enough.
- For any i, $H^i(\mathbb{P}^n_R, \mathcal{F})$ is a finite R-module.
- For any $k \in \mathbb{Z}$, $\bigoplus_{d \geq k} H^0(\mathbb{P}^n_R, \mathcal{F}(d))$ is a finite $R[T_0, \ldots, T_n]$-module.

⌟

Proof: 1: The assertions are true for $\mathcal{O}_X(n)$ by(6.7.2.1), and for general $\mathcal{F}$, we use descending induction on i. This is true for $i > n$ by Čech cohomology(6.7.1.2). For general $i > 0$, choose a surjection $\bigoplus \mathcal{O}_X(n_i) \to \mathcal{F}$ with coherent kernel $\mathcal{R}$(6.5.4.5), then there is an exact sequence

$$H^i(X, \oplus \mathcal{O}_X(n_i + n)) \to H^i(X, \mathcal{F}(n)) \to H^{i+1}(X, \mathcal{R}(n)),$$

and the left term vanish for n large(6.7.2.1), and the right term vanish by induction hypothesis.

2: Notation as above, we use descending induction on i. This is true for $i > n$ by Čech cohomology(6.7.1.2). For general $i > 0$, $H^i(X, \oplus \mathcal{O}_X(n_i))$ is finite by(6.7.2.1), and $H^{i+1}(X, \mathcal{R})$ is finite by induction hypothesis, thus $H^i(X, \mathcal{F}(n))$ is also finite.

3: Notation as above, for n large, $H^i(X, \oplus \mathcal{O}_X(n_i + n)) \to H^i(X, \mathcal{F}(n))$ is surjective. Thus $M_k = \bigoplus_{d \geq k} H^0(\mathbb{P}^n_R, \mathcal{F}(d))$ is a quotient of $N_k = \bigoplus_{d \geq k} H^0(\mathbb{P}^n_R, \mathcal{O}_X(d))$ for k large. Notice for k small enough, $N_k \cong \oplus_i R[T_0, \ldots, T_n][i]$ is a finite graded $R[T_0, \ldots, T_n]$-module, thus N_k is finite for any k as $R[T_0, \ldots, T_n]$ is Noetherian. Then M_k is finite for k large, and each $H^0(\mathbb{P}^n_R, \mathcal{F}(d))$ is itself finite by item 2, thus M_k is a finite $R[T_0, \ldots, T_n]$-module for any k. □

Prop. (6.7.2.6) [Cohomology of Proper Schemes]. Let X be a proper scheme over a Noetherian ring A, $\mathcal{L}$ an ample invertible sheaf on X and $\mathcal{F} \in \mathfrak{Coh}(X)$, then

- $H^i(X, \mathcal{F} \otimes \mathcal{L}^{\otimes d}) = 0$ for $i > 0$ and d large enough.
- The graded ring $A = \bigoplus_{n \geq 0} H^0(X, \mathcal{L}^{\otimes n})$ is a f.g. R-algebra.
- For any $k \in \mathbb{Z}$, $\bigoplus_{d \geq k} H^0(X, \mathcal{F} \otimes \mathcal{L}^{\otimes d})$ is a finite A-module.

⌟

Proof: By(6.5.4.26), there exists a $d > 0$ and some immersion $i : X \to \mathbb{P}^n_A$ that $i^*\mathcal{O}_{\mathbb{P}^n_A}(1) \cong \mathcal{L}^{\otimes d}$, and i is a closed immersion because X is proper. Let $S = R[T_0, \ldots, T_n]$.

1: By projection formula(6.7.4.6),

$$i_*(\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{L}^{\otimes nd+q}) = i_*(\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{L}^{\otimes q})(n).$$

Then by(6.7.4.2) and(6.7.2.5), for n large enough, $H^p(X, \mathcal{F} \otimes \mathcal{L}^{\otimes q}) = 0$ for any $0 \leq q \leq d-1$, $p > 0$.

2: By proof of item1 and(6.7.2.5), we see $\oplus_{n \geq 0} A_{nd+q}$ is a finite graded S-module for any q, thus $A = \oplus_{q=0}^{d-1} \bigoplus_{n \geq 0} A_{nd+q}$ is a f.g. R-module.

3: Similarly, we see $\bigoplus_{d \geq k} H^0(X, \mathcal{F} \otimes \mathcal{L}^{\otimes d})$ is a finite graded S-module, and the S-module structure factors through $S \to A$, thus it is a finite A-module. □

Lemma (6.7.2.7). For an invertible sheaf $\mathcal{L}$ on a qc scheme X, if for each Qco sheaf of ideals $\mathcal{I} \in \mathcal{O}_X$, there exists an n that $H^1(X, \mathcal{I} \otimes \mathcal{L}^n) = 0$, then $\mathcal{L}$ is ample. ⌟

Proof: For any closed pt P, choose an open affine nbhd U that $\mathcal{L}$ is trivial, let $Y = X - U$, by the exact sequence $0 \to \mathcal{I}_{Y \cup \{p\}} \to \mathcal{I}_Y \to k(P) \to 0$, for each n,

$$0 \to \mathcal{I}_{Y \cup \{p\}} \otimes \mathcal{L}^n \to \mathcal{I}_Y \otimes \mathcal{L}^n \to k(P) \otimes \mathcal{L}^n \to 0.$$

Thus by assumption for some n the map $\Gamma(X, \mathcal{I}_Y \otimes \mathcal{L}^n) \to \Gamma(X, k(P) \otimes \mathcal{L}^n)$ is surjective. Now $k(P) \otimes \mathcal{L}^n \cong A/\mathfrak{m}_P$, so we let $s \in \Gamma(X, \mathcal{I}_Y \otimes \mathcal{L}^n)$ maps to a section in $\Gamma(X, k(P) \otimes \mathcal{L}^n)$ that corresponds to $1 \in A/\mathfrak{m}_P$, then $P \in \mathrm{Supp}(s) \subset U$, and $\mathrm{Supp}(s)$ is affine. So we find an affine nbhd X_s for every closed pt of X.

Finally these X_s cover X, because the complement of $\cup X_s$ is closed in X thus qc, then it contains a closed point by(4.4.6.1). □

Prop. (6.7.2.8)[Serre's Cohomological Criterion of Ampleness]. If X is proper over a Noetherian affine scheme, $\mathcal{L}$ is an invertible sheaf, then the following is equivalent.

- $\mathcal{L}$ is ample
- For any $\mathcal{F} \in \mathfrak{Coh}(X)$, for n large enough, $H^p(X, \mathcal{F} \otimes \mathcal{L}^n) = 0$ for $p > 0$.
- For any Qco sheaf of ideals $\mathcal{I} \in \mathcal{O}_X$, there exists an $n \geq 1$ that $H^1(X, \mathcal{I} \otimes \mathcal{L}^{\otimes n}) = 0$

(Notice in this case H-ample $\iff$ ample). ⌟

Proof: $1 \to 2$: This follows from(6.7.2.6). $2 \to 3$ is trivial. $3 \to 1$: (6.7.2.7). □

<u>**Lichtenbaum's theorem**</u>

Lemma (6.7.2.9). Let X is a variety and $\mathcal{F} \in \mathfrak{Coh}(\mathcal{O}_X)$. If $H^d(X, \mathcal{F}) \neq 0$, then $\dim X \geq d$, and if equality holds, X is proper. ⌟

Proof: Cf.[Sta]0G5E. □

Prop. (6.7.2.10) [Lichtenbaum]. Let X be a non-empty separated scheme of f.t. over a field k of dimension d, then the following are equivalent:

- $H^d(X, \mathcal{F}) = 0$ for all $\mathcal{F} \in \mathfrak{Coh}(X)$.
- $H^d(X, \mathcal{F}) = 0$ for all $\mathcal{F} \in \mathfrak{QCoh}(X)$.
- No irreducible component of X of dimension d is proper over k.

⌟

Proof: Cf.[Sta]0G5F. □

3 Euler Characteristics

Def. (6.7.3.1) [Euler Characteristic]. Let X be proper over a field k and $\mathcal{F} \in \mathfrak{Coh}(X)$, then the **Euler characteristic** of $\mathcal{F}$ is defined to be:

$$\chi(\mathcal{F}) = \sum (-1)^i \dim_k H^i(X, \mathcal{F}).$$

It is definable by Grothendieck vanishing(6.3.5.17) and Grothendieck coherence theorem(6.7.4.12), and It is clearly an additive functor on $\mathfrak{Coh}(X)$. ⌟

Prop. (6.7.3.2). For a proper scheme X over a field k and $\mathcal{L}_i$ be invertible sheaves on X. Then for any $\mathcal{F} \in \mathfrak{Coh}(X)$,

$$\chi(X, \mathcal{F} \otimes \mathcal{L}_1^{n_1} \otimes \cdots \otimes \mathcal{L}_r^{n_r})$$

is a polynomial in $(n_1, \ldots, n_r)$ of total degree at most $\dim \operatorname{Supp} \mathcal{F}$. ⌟

Proof: Cf.[Sta]0BEM. □

Prop. (6.7.3.3). Let $f : Y \to X$ be morphism between schemes proper over field k and $\mathcal{F} \in \mathfrak{Coh}(X)$,

$$\chi(Y, \mathcal{F}) = \sum (-1)^i \chi(X, R^i f_* \mathcal{F}).$$

In particular, if f is affine(finite), then $\chi(Y, \mathcal{F}) = \chi(X, f_* \mathcal{F})$. ⌟

Prop. (6.7.3.4). This formula makes sense by(6.7.4.4) and(6.7.4.12), and it is true by Leray spectral sequence(6.3.1.9). ⌟

Prop. (6.7.3.5). If X is a proper scheme and $\mathcal{F} \in \mathfrak{Coh}(X)$ with $\dim \operatorname{Supp}(\mathcal{F}) = 0$, then $\mathcal{F}$ is generated by global sections, $H^i(X, \mathcal{F}) = 0$ for $i > 0$, and

$$\chi(X, \mathcal{F} \otimes \mathcal{E}) = n\chi(X, \mathcal{F})$$

for any $\mathcal{E} \in \mathcal{V}\mathrm{ect}^n(X)$. ⌟

Proof: The first two are clear as $\mathcal{F} = i_* \mathcal{G}$ where $i : \operatorname{Supp}(\mathcal{F}) \to X$. The last assertion follows from the projection formula(6.7.4.6) $i_*(\mathcal{G} \otimes i^* \mathcal{E}) \cong \mathcal{F} \otimes \mathcal{E}$. □

Def. (6.7.3.6)[Arithmetic Genus]. The **arithmetic genus** of a proper scheme of dimension r over a field is defined to be $p_a(X) = (-1)^r(\chi(\mathcal{O}_X) - 1)$(6.7.3.1). In particular, when X is a complete curve over a field k, then $p_a(X) = \dim_k H^1(X, \mathcal{O}_X)$(6.11.1.12).

The arithmetic genus is stable under base change of fields, by flat base change theorem. ⌟

Prop. (6.7.3.7)[Arithmetic Genus of Product]. By Künneth formula, if X, Y are proper schemes of dimension r, s over a field k, then

$$H^n(X \otimes_k Y, \mathcal{O}_{X \otimes_k Y}) \cong \bigoplus_{0 \le k \le n} H^k(X, \mathcal{O}_X) \otimes H^{n-k}(Y, \mathcal{O}_Y).$$

Thus $\chi(X \times_k Y) = \chi(X)\chi(Y)$. In particular, we have

$$p_a(X \times Y) = p_a(X)p_a(Y) + (-1)^s p_a(X) + (-1)^r p_a(Y).$$

⌟

Prop. (6.7.3.8) [Arithmetic Genus of Complete Intersections]. Let C be a smooth complete intersection of a degree m surface S_1 and a degree n surface S_2 in $\mathbb{P}^3_k$, then $p_a(C) = \frac{1}{2}(mn(m+n-4)+2)$. ⌟

Proof: There are exact sequences $0 \to \mathcal{O}_{\mathbb{P}^3_k}(-S_i) \to \mathcal{O}_{\mathbb{P}^3_k} \to \mathcal{O}_{S_i} \to 0$, which gives

$$0 \to \mathcal{O}_{\mathbb{P}^3_k}(-S_2)|_{S_1} \to \mathcal{O}_{S_1} \to \mathcal{O}_{S_1 \cap S_2} \to 0.$$

So by adjunction formula,

$$\mathcal{K}_C = \mathcal{K}_{S_1}(S_1 \cap S_2)|_C = \mathcal{K}_{\mathbb{P}^3_k}(S_1)(S_2)|_C = \mathcal{O}_C(m+n-4).$$

So $2g - 2 = mn(m+n-4)$. □

Prop. (6.7.3.9) [Asymptotic Riemann-Roch]. If X is a proper scheme over a field k of dimension d and $\mathcal{L}$ is an ample invertible sheaf, then $\dim \Gamma(X, \mathcal{L}^n) \sim cn^d$. ⌟

Proof: Cf.[Sta]0BJ8. □

Hilbert Polynomials

References are [Hartshorne I.7] and [Vak17].

Prop. (6.7.3.10) [Hilbert Polynomial]. For a projective scheme over a field k and a coherent sheaf $\mathcal{F}$, there is a polynomial **Hilbert polynomial** $P \in \mathbb{Q}[\lambda]$ that $\chi(\mathcal{F}(n)) = P(n)$, and $\deg P \leq \dim \operatorname{Supp}(\mathcal{F})$.

This Hilbert polynomial is compatible with the definition in(6.7.3.12), because by(6.7.4.7), the higher cohomology group vanishes for n large, so $\chi(\mathcal{F}(n)) = \Gamma(\mathcal{F}(n)) = \Gamma_*(\mathcal{F})_n$. ⌟

Proof: □

Prop. (6.7.3.11). Let $X \hookrightarrow Y \hookrightarrow \mathbb{P}^n_k$ be a sequence of closed embeddings, then $P_X(m) \leq P_Y(m)$ for m large, and if equality holds for m large, then $X = Y$. ⌟

Proof: Cf.[Vak17]P490. □

Def. (6.7.3.12) [Hilbert Polynomial]. For a scheme projective over a field k of dimension r, we define the **Hilbert polynomial** P_Y as the Hilbert polynomial of its homogenous coordinate ring $\Gamma_*(Y)$. It has dimension r by(5.2.2.17).

The **degree** of Y is defined as the $r!$ times the leading coefficients of P_Y. ⌟

Prop. (6.7.3.13).

- The degree is a positive integer.
- If $Y = Y_1 \cup Y_2$ and $\dim Y_1 \cap Y_2 < r$, then $\deg Y = \deg Y_1 + \deg Y_2$.
- If H is a hypersurface whose ideal is generated by a homogeneous polynomial of degree d, then $\deg H = d$.

⌟

Proof: Cf.[Hartshorne P52]. □

Prop. (6.7.3.14). For a variety of degree k and a general linear space, the intersection has k points. ⌟

Proof: □

4 Relative Cohomology

Prop. (6.7.4.1) [Filtered Colimits]. If $f : X \to Y$ is qcqs, then $R^i f_*$ commutes with filtered colimits, by(6.3.1.6) and(6.7.1.6). ⌟

Prop. (6.7.4.2) [Sheaf Cohomology Commutes with Affine Map]. For $f : X \to Y$ affine and $\mathcal{F} \in \mathfrak{QCoh}(X)$, $H^n(Y, \mathcal{F}) = H^n(X, f_*\mathcal{F})$. ⌟

Proof: Because $R^i f_*\mathcal{F}(U) = 0$ by(6.7.1.3) and(6.3.1.7), we can then use(6.3.1.8) to conclude. □

Prop. (6.7.4.3) [Higher Direct Image Preserves Qco Sheaves]. If $f : X \to S$ is qcqs then $R^n f_*$ maps $\mathfrak{QCoh}(X)$ to $\mathfrak{QCoh}(S)$, and for $U \subset S$ affine open, $\underline{(R^p f_*\mathcal{F})|_U = (H^p(f^{-1}(U), \mathcal{F}))^\sim}$. ⌟

Proof: Firstly by(6.3.3.18), $(R^p f_*\mathcal{F})|_U = R^p f_{U*}(\mathcal{F}|_U)$, so it suffices to prove for S affine. Then $R^p f_*\mathcal{F}$ is the sheafification of the presheaf $G : U \mapsto H^p(f^{-1}(U), \mathcal{F})$ by(6.3.1.7).

If f is separated, then we can use Čech cohomology(6.7.1.2) to see that $H^p(f^{-1}(D(f)), \mathcal{F}) = H^p(X, \mathcal{F})_f$ thus G is itself a sheaf and the conclusion follows.

In general we can choose a finite affine cover U_i of X, then every intersection of U_i is quasi-compact and separated, and there is a spectral sequence convergence $H^p(\{U_i \to X\}, \mathcal{H}^q(F)) \Longrightarrow H^{p+q}(X, F)$, where the left can be calculated using Čech cohomology. Taking localization w.r.t. f, we get the desired isomorphism $H^p(f^{-1}(D(f)), \mathcal{F}) = H^p(X, \mathcal{F})_f$ also by comparison(4.10.7.5). □

Prop. (6.7.4.4) [Cohomological Boundedness of Rf_*]. For a qcqs morphism $f : X \to S$, if S is qc, there is an N that for every base change f' of f, we have $R^n f'_* \mathcal{F} = 0$ for every $\mathcal{F} \in \mathfrak{QCoh}(X)$ and $n \geq N$.

In particular, if f is affine, then $R^n f'_* \mathcal{F} = 0$ for $n > 0$. And if f is projective, then $R^n f'_* \mathcal{F} = 0$ for n bigger than the maximal dimension of the fiber of f. ⌟

Proof: Check affine locally on S and use(6.7.4.3), choose a finite affine cover $\mathcal{U}$ of X. Then when n is large, $(R^n f'_* \mathcal{F})|_{U_i} = 0$ by(6.7.4.3) and(6.7.1.3) for any i, thus $R^n f'_* \mathcal{F} = 0$. For base changes, notice the cardinality of the affine cover are the same. □

Cor. (6.7.4.5). For a qc separated scheme X, the cohomology vanish for n large. And when X is separated and can be covered by r affine opens, then N can chosen to be r. ⌟

Cor. (6.7.4.6) [Projection Formula].

- Let $f : X \to Y$ be a morphism of schemes, and $\mathcal{E}$ a locally free $\mathcal{O}_Y$-module, then for any $\mathcal{F} \in \mathfrak{Mod}(\mathcal{O}_X)$ and any i, there are natural isomorphisms.
$$R^i f_*(\mathcal{F} \otimes f^* \mathcal{E}) \cong R^i f_*(\mathcal{F}) \otimes \mathcal{E}.$$
- If $f : X \to Y$ is a qcqs morphism of schemes, then for any $\mathcal{F} \in \mathfrak{Coh}(\mathcal{O}_X), \mathcal{E} \in \mathfrak{Coh}(\mathcal{O}_Y)$, there is a natural isomorphism
$$Rf_*(\mathcal{F} \otimes^{\mathrm{L}} Lf^* \mathcal{E}) \cong Rf_*(\mathcal{F}) \otimes^{\mathrm{L}} \mathcal{E}.$$

⌟

Proof: 1 follows from(6.3.3.20) and 2 follows from(6.8.5.8). □

Proper Morphism and $\mathfrak{Coh}(X)$

Prop. (6.7.4.7)[Relative Serre Vanishing]. If $f : X \to Y$ is a proper morphism of locally Noetherian schemes, $\mathcal{I}$ an invertible sheaf on X, then the following are equivalent:

- $\mathcal{L}$ is f-ample.
- For any $\mathcal{F} \in \mathfrak{Coh}(X)$, for n sufficiently large, $R^i f_*(\mathcal{F} \otimes \mathcal{I}^{\otimes n}) = 0$ and $i > 0$.
- For any Qco sheaf of ideals $\mathcal{I} \subset \mathcal{O}_X$, there exists an $n \geq 1$ that $R^1 f_*(\mathcal{I} \otimes \mathcal{L}^{\otimes n}) = 0$.

⌟

Proof: $1 \to 2$: By(6.7.4.3), this follows from(6.7.2.8). $2 \to 3$ is trivial as X is Noetherian. $3 \to 1$: Notice for any affine open subset U of Y, $U \to Y$ is qc, thus $f^{-1}(U) \to X$ is quasi-compact, thus by(6.5.1.8), a Qco sheaf of ideals $\mathcal{I}$ on $f^{-1}(U)$ can be extended to a Qco sheaf of ideals on X. Then we can use(6.7.4.3) and Leray spectral sequence to reduce to(6.7.2.8). □

Cor. (6.7.4.8). Let X be proper over a Noetherian affine scheme with an ample invertible sheaf $\mathcal{I}$, then for any finite exact sequence in $\mathfrak{Coh}(X)$, if tensoring it with $\mathcal{I}^{\oplus n}$ for large n, the resulting global section is exact. ⌟

Cor. (6.7.4.9). Let X be proper over a Noetherian affine scheme with an ample invertible sheaf $\mathcal{I}$, and $\mathcal{F},\mathcal{G}\in\mathfrak{Coh}(X)$, $i\geq 0$, then for n large(depending on $\mathcal{F},\mathcal{G},i$),

$$\mathrm{Ext}^i(\mathcal{F},\mathcal{G}(n))\cong\Gamma(X,\mathcal{E}xt^i(\mathcal{F},\mathcal{G}(n))).$$

⌟

Proof: By(6.3.3.34)(6.7.1.7), there is a spectral sequence s.t. for n large, all the small terms vanish. □

Lemma (6.7.4.10). If $f:X\to Y$ is projective and Y locally Noetherian, then for any $n\in\mathbb{N}$, R^nf_* maps coherent sheaves to coherent sheaves. ⌟

Proof: By(6.7.4.3), this problem is local on the target, so we may assume that $Y=\operatorname{Spec}R$ and $X=\mathbb{P}^n_R$, in which case this follows from(6.7.2.5). □

Prop. (6.7.4.11) [Grothendieck's Coherence Theorem]. If $f:X\to Y$ is proper and Y locally Noetherian, then for any $n\in\mathbb{N}$, R^nf_* maps coherent sheaves to coherent sheaves. ⌟

Proof: By(6.7.4.3), this problem is local on the target, so we may assume Y is Noetherian, and then X is also Noetherian. We prove by devissage(6.5.1.55): 1 is trivial, for 2, for any closed subscheme $i:Z\subset X$, denote $g=f|_Z$, then it suffices to find a coherent sheaf $\mathcal{G}$ on Z s.t.

1. $\mathcal{G}_\xi\cong k(\xi)$.
2. $R^pg_*\mathcal{G}$ are coherent for any $p\geq 0$.

Because then $i_*\mathcal{G}$ is a coherent sheaf on X(6.5.1.32) that $R^pf_*(i_*\mathcal{G})=R^pg_*\mathcal{G}$ for any p by relative Leray spectral sequence(6.3.1.8) and(6.7.4.4), and also $(i_*\mathcal{G})_\xi=\mathcal{G}_\xi$.

As $g:Z\to Y$ is proper, by Chow's lemma(6.4.5.23), there is a birational, H-projective map $\pi:Z'\to Z$ over Y that Z' is projective over Y. Then there is a closed immersion $j:Z'\to\mathbb{P}^n_Y$ and an induced closed immersion $j':Z'\to\mathbb{P}^n_Z$. Then $\mathcal{L}=j^*\mathcal{O}_{\mathbb{P}^n_Y}(1)=(j')^*\mathcal{O}_{\mathbb{P}^n_Z}(1)$ is both $g\circ\pi$-relatively ample and π-relatively ample.

Hence by relative Serre vanishing(6.7.4.7) there exists an n that $R^p\pi_*\mathcal{L}^{\otimes n}=0$ for any $p>0$. Let $\mathcal{G}=\pi_*\mathcal{L}^{\otimes n}$, then this $\mathcal{G}$ satisfies the conditions: $\mathcal{G}_\xi=\kappa(\xi)$ as $\pi^{-1}(U)\to U$ is an isomorphism, and from relative Leray spectral sequence

$$R^pg_*R^q\pi_*\mathcal{L}^{\otimes n}\Longrightarrow R^n(g\circ\pi)_*\mathcal{L}^{\otimes n},$$

we see $R^pg_*\mathcal{G}\cong R^pg'_*\mathcal{L}^{\otimes n}$, which are coherent by(6.7.4.10). □

Cor. (6.7.4.12) [Coherent Cohomology Finite]. If $\pi:X\to\operatorname{Spec}A$ is proper over a Noetherian affine scheme A and $\mathcal{F}$ is a coherent sheaf on X, $H^i(X,\mathcal{F})$ are finite A-modules. ⌟

Proof: By(6.7.4.3), $R^p\pi_*\mathcal{F}$ is the Qco sheaf $\widetilde{H^p(X,\mathcal{F})}$, which is coherent iff $H^p(X,\mathcal{F})$ is a finite A-module. □

Prop. (6.7.4.13). Given a proper morphism between locally Noetherian schemes $f:X\to Y$, a coherent sheaf $\mathcal{F}$ on X and a coherent sheaf of ideals $\mathcal{I}$ of $\mathcal{O}_Y$. Then $\mathcal{M}=\bigoplus_{n\geq 0}R^pf_*(\mathcal{I}^n\mathcal{F})$ is a Qco graded $\mathcal{A}=\bigoplus_{n\geq 0}\mathcal{I}^n$-module of f.t.. ⌟

Proof: By(6.7.4.3), this is local on Y, so we may assume Y is affine, Cf.[Sta]02O8. □

Prop. (6.7.4.14). Let $f: X \to Y$ be a proper morphism between locally Noetherian schemes and $\mathcal{F}$ a coherent sheaf on X, $y \in Y$. Consider the infinitesimal nbhds $X_n = \mathrm{Spec}(\mathcal{O}_{Y,y}/\mathfrak{m}_y^n) \times_Y X \xrightarrow{i_n} X$ of the fiber $X_1 = X_y$, and set $\mathcal{F}_n = i_{n*}\mathcal{F}$, then

$$(R^n f_*\mathcal{F})_y^\wedge \cong \varprojlim_n H^n(X_n, \mathcal{F}_n)$$

as $\mathcal{O}_{Y,y}^\wedge$-modules. ⌟

Proof: Cf.[Sta]02OD. □

Cor. (6.7.4.15)[Support of Higher Direct Images]. Let $f: X \to Y$ be a proper morphism between locally Noetherian schemes and $y \in Y$ s.t. $\dim(X_y) = d$, then for any coherent sheaf $\mathcal{F}$ on X, $(R^p f_*\mathcal{F})_y = 0$ for $p > d$. ⌟

Proof: Cf.[Sta]02V7. □

5 Base Change

Prop. (6.7.5.1)[Flat Base Change]. For a Cartesian diagram of schemes

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ \downarrow{f'} & & \downarrow{f} \\ S' & \xrightarrow{g} & S \end{array}$$

If g is flat and f is qcqs, then for every Qco sheaf $\mathcal{F}$ on X with base change $\mathcal{F}'$ on X', there is a canonical isomorphism

$$g^* Rf_*\mathcal{F} \cong Rf'_*\mathcal{F}'.$$

By(6.3.3.18), when S, S' is affine, this reads:

$$H^i(X, \mathcal{F}) \otimes_A B \cong H^i(X \otimes_A B, (g')^*\mathcal{F}).$$

⌟

Proof: Firstly by(6.3.3.18)(6.7.4.3), it suffices to show for S, S' affine. If X is separated, then the then we can use Čech cohomology(6.7.1.2), and the Čech complex of K' is just the cohomology of the Čech complex tensored with B, so it commutes with taking cohomology because B is A-flat.

Now if X is only qs, then we choose a finite affine open cover $\{U_i\}$, then every intersection of U_i is quasi-compact and separated. and there is a spectral sequence convergence $H^p(\{U_i \to X\}, \mathcal{H}^q(F)) \Longrightarrow H^{p+q}(X, F)$. Tensoring with B, we also get the desired isomorphism $H^i(X, \mathcal{F}) \otimes_A B \cong H^i(X \otimes_A B, (g')^*\mathcal{F})$ by comparison(4.10.7.5). □

Prop. (6.7.5.2)[Finite Locally Free Base Change]. For a Cartesian diagram of schemes

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ \downarrow{f'} & & \downarrow{f} \\ S' & \xrightarrow{g} & S \end{array}$$

If $S = \mathrm{Spec}\, A, S' = \mathrm{Spec}\, B$ and B is finite locally free over A, for every Qco sheaf $\mathcal{F}$ on X with base change $\mathcal{F}'$ on X', there is a canonical isomorphism

$$H^i(X, \mathcal{F}) \otimes_A B \cong H^i(X \otimes_A B, (g')^*\mathcal{F}).$$

⌟

Proof: If X is separated, then the then we can use Čech cohomology(6.7.1.2), and the Čech complex of K' is just the cohomology of the Čech complex tensored with B, so it commutes with taking cohomology because B is A-flat and tensoring a f.p. ring map commutes with colimits of rings.

In general we choose an affine open cover $\{U_i\}$, then every intersection of U_i is separated. and there is a spectral sequence convergence $H^p(\{U_i\to X\},\mathcal{H}^q(F))\Longrightarrow H^{p+q}(X,F)$. Tensoring with B, we also get the desired isomorphism $H^i(X,\mathcal{F})\otimes_A B\cong H^i(X\otimes_A B,(g')^*\mathcal{F})$ by comparison(4.10.7.5). □

Prop. (6.7.5.3) [Representing Higher Direct Image]. Let $f: X\to S$ be a qcqs morphism of schemes. If S is qc and separated and $\mathcal{F}$ is a Qco sheaf on X, there exists a $\mathcal{K}^\bullet\in K^+(\mathfrak{QCoh}(\mathcal{O}_S))$ s.t. for any morphism $g:S'\to S$, the complex $g^*\mathcal{K}^\bullet$ is a representative for $Rf'_*\mathcal{F}'$, where the notation is as in(6.7.5.1). ⌟

Proof: We only prove the case X is separated, the general case in [Sta]01XN.

Choose a finite affine open covering $\mathcal{U}$ of X, consider the complex of sheaves $\mathfrak{C}^\bullet(\mathcal{U},\mathcal{F})=\mathcal{H}om^\bullet((\mathbb{Z}^\sharp_{\mathcal{U},\bullet}),\mathcal{F})$(6.3.2.1), then $\mathfrak{C}^p(\mathcal{U},\mathcal{F})=\bigoplus_{i_0\ldots i_p}j_{i_0\ldots i_p*}\mathcal{F}_{i_0\ldots i_p}$. Then let $\check{\mathcal{C}}^\bullet(\mathcal{U},f,\mathcal{F})=f_*\mathfrak{C}^\bullet(\mathcal{U},\mathcal{F})$. There is a natural map $\mathcal{F}\to\mathfrak{C}^\bullet(\mathcal{U},\mathcal{F})$. Now $j_{i_0\ldots i_p}$ and $f_{i_0\ldots i_p}$ are both affine by(6.4.4.88), so are their base changes, thus the higher direct image vanish. So by relative Leray spectral sequence, we see each term $j_{i_0\ldots i_p*}\mathcal{F}'_{i_0\ldots i_p}$ is f'_*-acyclic. Then by Leray's acyclicity theorem,

$$Rf'_*(\mathcal{F}')=Rf'_*(\mathfrak{C}^\bullet(\mathcal{U},\mathcal{F}))\cong\mathcal{C}^\bullet(\mathcal{U}',f',\mathcal{F}')=g^*\mathcal{C}^\bullet(\mathcal{U},f,\mathcal{F}).$$

The last equation follows from the fact $f_{i_0\ldots i_p}$ are all affine thus the base change are isomorphisms. □

Prop. (6.7.5.4) [Proper Flat Base Change]. If $f:X\to S$ is a proper morphism of f.p., then

- If E a perfect object in $D(\mathcal{O}_X)$, $\mathcal{G}\in D(\mathcal{O}_X)$ is representable by a bounded complex of f.p. $\mathcal{O}_X$-modules flat over S, then
$$Rf_*(E\otimes^{\mathrm{L}}_{\mathcal{O}_X}\mathcal{G}^\bullet),\quad Rf_*R\mathcal{H}om(E,\mathcal{G}^\bullet)$$
are perfect complexes in $D(\mathcal{O}_S)$, and its formation commutes with base change.
- If E a pseudo-coherent object in $D(\mathcal{O}_X)$, $\mathcal{G}\in D(\mathcal{O}_X)$ is representable by a bounded above complex of f.p. $\mathcal{O}_X$-modules flat over S, then $Rf_*(E\otimes^{\mathrm{L}}_{\mathcal{O}_X}\mathcal{G}^\bullet)$ is a pseudo-coherent complex in $D(\mathcal{O}_S)$, and its formation commutes with base change.

⌟

Proof: Cf.[Sta]0A1H, 0A1J, 0CSC.**?** □

Cor. (6.7.5.5). Let $f:X\to S$ be a proper morphism of f.p., then

- If $E\in D(\mathcal{O}_X)$ is perfect(pseudo-coherent) and f is flat, then Rf_*E is a perfect(pseudo-coherent) object in $D(\mathcal{O}_S)$, and its formation commutes with base change.
- If $\mathcal{G}\in\mathfrak{QCoh}^{\mathrm{pf}}(\mathcal{O}_X)$ and is flat over S, then $Rf_*\mathcal{G}$ is a perfect object of $D(\mathcal{O}_S)$ and its formation commutes with base change.

⌟

Cor. (6.7.5.6). If $A\in\mathcal{CA}\mathrm{lg}$, X be a proper scheme of f.p. over A, then if $\mathcal{G}\in\mathfrak{QCoh}^{\mathrm{pf}}(\mathcal{O}_X)$ and is flat over A, there exists a finite complex of finite projective A-modules $L^\bullet$ that for any $A'\in\mathcal{CA}\mathrm{lg}_A$, $M\in\mathfrak{Mod}_A$, by(6.7.5.5) and projection formula(6.7.4.6),

$$H^i(X_{A'},\mathcal{F}_{A'})=H^i(L^\bullet\otimes_A A'),\quad H^i(X,\mathcal{F}\otimes_A M)=H^i(L^\bullet\otimes_A M)$$

⌟

6 Semicontinuity

Prop. (6.7.6.1). T^i is left exact iff Coker d^{i-1} is a projective A-module, iff it is representable by a finite A-module. ⌟

Proof: Denote $W^i = \operatorname{Coker} d^{i-1}$, then $\operatorname{Coker} d^{i-1} \otimes_A M = W^i \otimes M$, because tensoring is right exact. Thus $T^i(M) = \ker(W^i \otimes M \to L^{i+1} \otimes M)$. Then for $M' \subset M$, there is a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & T^i(M) & \longrightarrow & W^i \otimes M' & \longrightarrow & L^{i+1} \otimes M' \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ 0 & \longrightarrow & T^i(M) & \longrightarrow & W^i \otimes M & \longrightarrow & L^{i+1} \otimes M \end{array}$$

γ is injective, so using spectral sequence, its clear α is injective iff β is injective, i.e. W^i is flat, which is equivalent to finite projective(5.3.1.7).

To prove T^i is representable, let $Q = \operatorname{Coker}(L^{i+1,*} \to W^{i,*})$, then Q is finite because W^i is finite(5.3.1.18), and $0 \to \operatorname{Hom}(Q, M) \to \operatorname{Hom}(W^{i,*}, M) \to \operatorname{Hom}(L^{i+1,*}, M)$, but by(5.3.1.19), the last two are just $W^i \otimes M$ and $L^{i+1} \otimes M$, $\operatorname{Hom}(Q, M) = T^i(M)$ by what has already be proved. □

Prop. (6.7.6.2). T^i is right exact iff the cup product $H^i(X, \mathcal{F}) \otimes_A M \to H^i(X, \mathcal{F} \otimes_A M)$ is an isomorphism for any A-module M. ⌟

Proof: Because T^i and $\otimes$ commutes with direct limit, it suffices to prove for M finite. In this case, choose a finite presentation $A^r \to A^s \to M \to 0$, then there is a diagram

$$\begin{array}{ccccccc} T^i(A) \otimes A^r & \longrightarrow & T^i(A) \otimes A^s & \longrightarrow & T^i(A) \otimes M & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ T^i(A^r) & \longrightarrow & T^i(A^s) & \longrightarrow & T^i(M) & & \end{array}$$

The first two vertical arrows are isomorphisms, so if T^i is right exact, so does the third vertical arrow. Conversely, if $T^i(A) \otimes_A M \to T^i(M)$ are all isomorphisms, then by a similar diagram, we can show $T^i(M) \to T^i(M')$ are surjective for $M \to M'$ surjective. □

Cor. (6.7.6.3). T^i is exact iff it is right exact and $T^i(A) = H^i(X, \mathcal{F})$ is a finite projective A-modules. ⌟

Proof: When T^i is right exact, $H^i(X, \mathcal{F} \otimes_A M) \cong H^i(X, \mathcal{F}) \otimes_A M$ by(6.7.6.2), so it is exact iff $H^i(X, \mathcal{F})$ is flat. Because it is in priori finite, this is equivalent to finite projective(5.3.1.7). □

Def. (6.7.6.4). For a point $y \in \operatorname{Spec} A$, define $T^i_y(N) = H^i(L^\bullet_y \otimes N)$, then T^i is (left/right)exact at y iff T^i_y are all (left/right)exact(exact sequence is stalkwise(5.1.4.2)). ⌟

Prop. (6.7.6.5). If T^i is (left/right)exact at a point y, then the same is true on a nbhd of y. ⌟

Proof: From(6.7.6.1), $(\operatorname{Coker} d^{i-1})_y$ is a finite projective $A_\mathfrak{p}$ module, so it is free, and it is a coherent sheaf, so it is free at a nbhd of y by(6.5.1.38), so the same is true on a nbhd of y. Now right exactness of T^i is equivalent to left exactness of T^{i+1}, and exact is left exact+right exact, so we are done. □

Prop. (6.7.6.6). T^i is right exact at y iff $H^i(X, \mathcal{F}) \otimes k(y) \to H^i(X, \mathcal{F} \otimes_A k(y))$ is surjective. ⌟

Proof: Cf.[Hartshorne P289].? □

Prop. (6.7.6.7) [Cohomology and Stalks]. Let $f : X \to Y$ be a proper morphism of locally Noetherian schemes and $\mathcal{F}$ is a coherent sheaf on X flat over Y, $y \in Y$, then

- If the natural map
$$\varphi^i(y) : R^i f_*(\mathcal{F}) \otimes k(y) \to H^i(X_y, \mathcal{F}_y)$$
is surjective, then it is an isomorphism, and and the same is true for y' in an open nbhd of y.
- Assume $\varphi^i(y)$ is surjective, then $\varphi^{i-1}(y)$ is also surjective iff $R^i f_*(\mathcal{F})$ is finite projective in a nbhd of y.

⌟

Proof: 1: This follows from(6.7.6.2)(6.7.6.6) and(6.7.6.5).

2: $\varphi^{i-1}(y), \varphi^i(y)$ are both surjective iff T^i and T^{i-1} are both right exact at y(6.7.6.6), which is equivalent to T^i exact at y. Then we finish by(6.7.6.3) □

Remark (6.7.6.8). How's this related to(6.7.5.5)**?** ⌟

Prop. (6.7.6.9) [Semicontinuity of Cohomology]. Let $X \to Y$ be a projective morphism of locally Noetherian schemes and $\mathcal{F}$ is a coherent sheaf on X, flat over Y, then for each i, $h^i(y, \mathcal{F}) = \dim_{k(y)} H^i(X_y, \mathcal{F}_y)$ is an upper semicontinuous function on Y. ⌟

Proof: The question is local on Y, so we may assume Y is affine Noetherian. By(6.7.5.1), $H^i(y, \mathcal{F}) = \dim_{k(y)} T^i(k(y))$. And as in the proof of(6.7.6.1), $T^i(M) = \ker(W^i \otimes M \to L^{i+1} \otimes M)$, and $W^i \to L^{i+1} \to W^{i+1} \to 0$ is exact, so $0 \to T^i(k(y)) \to W^i \otimes k(y) \to L^{i+1} \otimes k(y) \to W^{i+1} \otimes k(y) \to 0$, and counting dimension, $h^i(y, \mathcal{F}) = \dim W^i \otimes k(y) + \dim W^{i+1} \otimes k(y) - \dim L^{i+1} \otimes k(y)$. Notice the last term is constant as L^{i+1} is free A-module and the first two terms are upper semi-continuous by(6.5.1.41), thus $h^i(y, \mathcal{F})$ is upper-semicontinuous. □

Cor. (6.7.6.10) [Grauert]. If Y is integral and $h^i(y, \mathcal{F})$ is constant on Y, then $R^i f_*(\mathcal{F})$ is locally free on Y and $R^i f_*(\mathcal{F}) \otimes k(y) \cong H^i(X_y, \mathcal{F}_y)$. ⌟

Proof: Cf.[Hartshorne P288]. □

6.8 Topics in Schemes

Main references are [Sta]and [Har77].

1 Cartier Divisors

Def. (6.8.1.1) [Cartier Divisor]. A **Cartier divisor** on a scheme X is an element in $\Gamma(X, \mathcal{K}_X^*/\mathcal{O}_X^*)$.

An **effective Cartier divisor** is a Cartier divisor that is locally defined as $\{(U_i, f_i)\}$ where $f_i \in \Gamma(U_i, \mathcal{O}_{U_i})$ are nonzero-divisors, equivalently, it is a closed subscheme whose ideal sheaf is an invertible sheaf.(Notice by definition, $\mathcal{K}$ is the localization w.r.t. nonzero-divisors, and f_i is invertible in $\mathcal{K}^*$ so f_i must be nonzero-divisors.)

The group of effective Cartier divisors is denoted by $\mathrm{Cart}^{\mathrm{eff}}(X)$.

The **Cartier divisor group** CaCl is the quotient of $\Gamma(X, \mathcal{K}^*) \to \Gamma(X, \mathcal{K}^*/\mathcal{O}_X^*)$. ⌟

Prop. (6.8.1.2) [Cartier Divisor is Nowhere Dense]. Let $D \subset X$ be an effective Cartier divisor, then it is nowhere dense in X, i.e $X \backslash D \to X$ is scheme-theoretically dense. ⌟

Proof: It suffices to check affine-locally, it is qc so the scheme-theoretic closure of $\mathrm{Spec}\, A_f \to \mathrm{Spec}\, A$ is $V(\ker(A \to A_f)) = V(0)$ as f is a nonzero-divisor. □

Prop. (6.8.1.3) [Closed Subschemes and Effective Cartier Divisors]. Let X be a locally Noetherian scheme and $D \subset X$ is a closed subscheme corresponding to a Qco sheaf of ideals $\mathcal{I} \subset \mathcal{O}_X$. If for any $x \in D$, the ideal $\mathcal{I}_x \subset \mathcal{O}_{X,x}$ is generated by a single nonzero-divisor, then D is an effective Cartier divisor. ⌟

Proof: Cf.[Sta]0AG8. □

Cor. (6.8.1.4) [Prime Divisor and Effective Cartier Divisor]. Let X be a locally Noetherian scheme and D is a prime Weil divisor on X and $\mathcal{O}_{X,x}$ are UFDs for any $x \in D$, then D is an effective Cartier divisor. ⌟

Proof: For any $x \in D$, let $A = \mathcal{O}_{X,x}$, and $\mathfrak{p}$ be the prime corresponding to the generic point of D, then $\dim A_{\mathfrak{p}} = 1$, so $\mathfrak{p}$ is principle as A is a UFD, so D is an effective Cartier divisor by(6.8.1.3). □

Prop. (6.8.1.5) [Cartier-Pic]. For an integral scheme X, the homomorphism $\mathrm{CaCl}(X) \to \mathrm{Pic}(X)$(6.8.1.1)(6.5.3.10) induced from long exact sequence of $0 \to \mathcal{O}_X^* \to \mathcal{K}_X^* \to \mathcal{K}_X^*/\mathcal{O}_X^* \to 0$ is an isomorphism.

Explicitly, for a Cartier divisor $D = \{(U_i, f_i)\}$, the image is the invertible sheaf $\mathcal{O}_X(D)$(6.5.3.12). ⌟

Proof: It is clearly injective by definition, so it suffices to show any invertible sheaf can embed into the constant sheaf: for any invertible sheaf $\mathcal{L}$, tensor with $\mathcal{K}$ and restrict to the stalk of the generic point, i.e. there is a compatible choice of homomorphisms into $K(X)$. □

Prop. (6.8.1.6). If $X \in \mathrm{N}\mathcal{S}\mathrm{ch}$ and the diagonal map is affine, for a dense affine open U, if all the stalk of $X \backslash U$ are UFD, then U is the complement of an effective Cartier divisor. ⌟

Proof: The irreducible complements of $X \backslash U$ is finite and has codimension 1 by(6.6.3.5) because $U \to X$ is affine, and it is an effective Cartier divisor by(8.1.5.1)., so their sum will suffice. □

Prop. (6.8.1.7)[Pullback of Effective Cartier Divisors]. Let $f : X \to Y \in \mathcal{S}\mathrm{ch}$ and $D \in \mathrm{Cart}^{\mathrm{eff}}(Y)$, then the pullback of D via f is an effective Cartier divisor on X in the following cases:

- $f(x)\notin D$ for any $x\in \mathrm{WeakAsso}(X)$.
- $X,Y\in \mathcal{S}\mathrm{ch}^{\mathrm{int}}$ and f is dominant.
- f is flat.

⌟

Proof: 2 is a special case of 1 as a reduced scheme has no embedded points.
1 follows from(5.2.5.17).
3 is easy. □

Prop. (6.8.1.8) [Effective Cartier Divisors]. If X is a Noetherian scheme with an ample invertible sheaf $\mathcal{L}$, then any line bundle in $\mathrm{Pic}(X)$ is isomorphism to $\mathcal{O}_X(D-D')$ for some effective Cartier divisors D,D' on X. ⌟

Proof: Cf.[Sta]0AYM. □

Relative Effective Cartier Divisors

Def. (6.8.1.9) [Relative (Effective) Cartier Divisors]. Let X be a scheme over S, then a **relative effective (Cartier)divisor** on X/S is an effective Cartier divisor D on X that is flat over S. ⌟

Prop. (6.8.1.10) [Fibral Criterion of Relative Effective Divisor]. Let $f:X\to S$ be a morphism of locally Noetherian schemes locally of f.t., $D\subset X$ be a closed subscheme and $x\in D$, $s=f(x)$, then the following are equivalent:

- D is a relative effective divisor at a nbhd of x.
- X and D are flat over S at x, and the fiber D_s is a Cartier divisor on X_s at x.
- X is flat over S at x, and D is cut out by an element that is regular on the fiber X_s.

In particular, a relative Cartier divisor pair can be regarded as a family of Cartier divisors pairs. ⌟

Proof: $1\to 2$: Let $\mathcal{O}_{D,x}=b\mathcal{O}_{X,x}$, then there is an exact sequence $0\to\mathcal{O}_{X,x}\xrightarrow{b}\mathcal{O}_{X,x}\to\mathcal{O}_{D,x}\to 0$, which induces a long exact sequence

$$\mathrm{Tor}_1^{\mathcal{O}_{S,s}}(\mathcal{O}_{X,x},k(s))\to\mathrm{Tor}_1^{\mathcal{O}_{S,s}}(\mathcal{O}_{X,x},k(s))\to\mathrm{Tor}_1^{\mathcal{O}_{S,s}}(\mathcal{O}_{D,x},k(s))\to\mathcal{O}_{X_s,x}\otimes k(s)\xrightarrow{b}\mathcal{O}_{X_s,x}\otimes k(s).$$

Because D is flat over S, $\mathrm{Tor}_1^{\mathcal{O}_{S,s}}(\mathcal{O}_{D,x},k(s))=0$, thus b is regular in $\mathcal{O}_{X_s,x}$ and D_s is en effective divisor on X_s at x. Also the map $\mathrm{Tor}_1^{\mathcal{O}_{S,s}}(\mathcal{O}_{X,x},k(s))\to\mathrm{Tor}_1^{\mathcal{O}_{S,s}}(\mathcal{O}_{X,x},k(s))$ is surjective, which is multiplication by b, and b is in the maximal ideal, thus by Nakayama lemma, $\mathrm{Tor}_1^{\mathcal{O}_{S,s}}(\mathcal{O}_{X,x},k(s))=0$. Then $\mathcal{O}_{X,x}$ is $\mathcal{O}_{S,s}$-flat by local criterion(5.4.1.16).

$2\to 3$: Let D corresponds to an ideal I in $\mathcal{O}_{X,x}$, and because D_s is effective divisor on X_s, there exists $b\in I$ s.t. the image of b in $\mathcal{O}_{X,x}\otimes k(s)$ generate the ideal of D_s. Then it suffices to show that b generates I. Notice there is an exact sequence $0\to I\to\mathcal{O}_{X,x}\to\mathcal{O}_{D,x}\to 0$, and $\mathcal{O}_{D,x}$ is flat over $\mathcal{O}_{S,s}$, thus $I\otimes k(s)\to\mathcal{O}_{X,x}\otimes k(s)$ is injective, and the image is just the ideal of D_s, thus b generates $I\otimes k(s)$. Thus by Nakayama, it also generates I.

$3\to 1$: The exact sequence $0\to I\to\mathcal{O}_{X,x}\to\mathcal{O}_{D,x}\to 0$ induces the long exact sequence

$$\mathrm{Tor}_1^{\mathcal{O}_{S,s}}(\mathcal{O}_{X,x},k(s))\to\mathrm{Tor}_1^{\mathcal{O}_{S,s}}(\mathcal{O}_{D,x},k(s))\to I\otimes k(s)\to\mathcal{O}_{X_s,x}\otimes k(s).$$

$I\otimes k(s)\to\mathcal{O}_{X_s,x}\otimes k(s)$ is injective because its composition with $\mathcal{O}_{X_s,x}\otimes k(s)\to I\otimes k(s)\to\mathcal{O}_{X_s,x}\otimes k(s)$ is multiplication by b, thus injective as b is regular on the fiber X_s. Thus $\mathrm{Tor}_1^{\mathcal{O}_{S,s}}(\mathcal{O}_{D,x},k(s))=0$, thus D is flat at x by local criterion(5.4.1.16). And also I is flat over $\mathcal{O}_{S,s}$. Notice $b:\mathcal{O}_{X,x}\to I$ is isomorphism after tensoring $k(x)$ and I is flat, so $\ker(b)=0$ by Nakayama, and b is regular. □

Cor. (6.8.1.11). If D, E are relative effective Cartier divisors on X/S, then $D+E$ is also a relative Cartier divisor on X/S. ⌟

Proof: This follows from item3 of(6.8.1.10). □

Prop. (6.8.1.12) [Pullback of Divisors]. For $S \in \mathcal{S}\mathrm{ch}$, $X \in \mathcal{S}\mathrm{ch}/S$ and Z an relative Cartier divisor on X/S, then for any $T \in \mathcal{S}\mathrm{ch}/S$, Z_T is a relative Cartier divisor on X_T/T.

And if $f : X\prime \to X$ is a flat morphism over S, then f^*Z is also a relative Cartier divisor on X'/S. ⌟

Proof: If $0 \to \mathcal{O}_X \xrightarrow{\mathcal{I}} \mathcal{O}_X \to i_*\mathcal{O}_Z \to 0$, then $0 \to \mathcal{O}_{X_T} \xrightarrow{\mathcal{I}_T} \mathcal{O}_{X_T} \to i_*\mathcal{O}_{Z_T} \to 0$ because $\mathcal{O}_Z$ is flat over $\mathcal{O}_S$, so $\mathcal{I}_T$ is also an effective divisor on X_T/T.

The second case is similar. □

2 Blowing Up

Blowing-up

Blowing-up serves as a way to magnify local properties to global ones.

Def. (6.8.2.1) [Blowing-Up]. Let X be a scheme and a closed subscheme $Z \subset X$ defined by $\mathcal{I}$, the **blowing up** of X along Z $\mathbf{Bl}_Z X$ is defined as the map $\beta : \mathbf{Proj}_X(\oplus_{d\geq 0}\mathcal{I}^d) \to X$.

The map $\beta : \mathbf{Bl}_Z X \to X$ pulls back Z to an effective Cartier divisor $E_Z X$, called the **exceptional divisor**, and it has the universal property that any morphism $Y \to X$ that pulls back Z to an effective Cartier divisor uniquely factors through $\mathbf{Bl}_Z X$. ⌟

Proof: Notice first an effective devisor is equivalent to an invertible sheaf of ideal. And any morphism $Z \to X$ pulls back I to the image of $f^{-1}I \otimes_{\mathcal{O}_X} \mathcal{O}_Z \to f^{-1}I \cdot \mathcal{O}_Z$. This is just $\mathcal{O}(1)$ on $\mathbf{Bl}\, X_{\mathcal{I}}$ so invertible.

For the construction, the local uniqueness will implies the existence. Notice locally $\widetilde{X}_I$ is projective over X. Now because the $Z \to X$ pulls back I to an invertible sheaf and it is generated by $f^{-1}(a_i)$, we use**??** to get another $Z \to \mathrm{Proj}_X^n$ and it factors through the closed subscheme $\widetilde{X}_I$. If there is another morphism g, then $f^{-1}I \cdot \mathcal{O}_Z = g^{-1}(\pi^{-1}I \cdot \mathcal{O}_{\widetilde{X}_I}) \cdot \mathcal{O}_Z = g^{-1}(\mathcal{O}_{\widetilde{X}_I}) \cdot \mathcal{O}_Z$ surjective, and a surjective morphism between two invertible sheave is an isomorphism, and they are both ideal sheaves, thus is the same, so this morphism is unique as it is determined by the map on $\mathcal{O}_X$**??**. □

Cor. (6.8.2.2). Let X be a scheme and $Z \subset X$.

- If Z is itself an effective Cartier divisor, then the $\mathbf{Bl}_Z X = X$.
- If $U \subset X$ is an open subscheme, then $\mathbf{Bl}_Z(U) = \beta^{-1}(U) \subset \mathbf{Bl}_Z(X)$. In particular, Blowing-up is a local construction.
- If $Z = X$, then $\mathbf{Bl}_X X = \varnothing$.
- β is an isomorphism $\beta^{-1}(X\backslash Z) \to X\backslash Z$ away from Z.
- If X is reduced, then $\mathbf{Bl}_Z X$ is also reduced.
- If X is irreducible and Z doesn't contain the generic point of X, then $\mathbf{Bl}_Z X$ is irreducible.

⌟

Proof: 1: By universal property.

2: This follows from universal property and the fact the restriction of an effective Cartier divisor is an effective Cartier divisor.

3: By universal property.
4: By item2 and 3.
5: ?
6: ? □

Cor. (6.8.2.3). $\pi : \widetilde{X}_I \to X$ is birational, proper thus surjective. If X is a (complete)variety, then so does $\widetilde{X}_I$. ⌟

Def. (6.8.2.4) [Strict Transform]. Let $Z \subset X$ is a closed subscheme and $f : Y \to X$ be a morphism, then $Y \times_X \mathbf{Bl}_Z X$ is called the **total transform** of Y, and the **strict transform** of Y is the scheme-theoretic closure of $Y \times_X \mathbf{Bl}_Z X \backslash Y \times_X E_Z X$ in $Y \times_X \mathbf{Bl}_Z X$, or equivalently the closed subscheme of $Y \times_X \mathbf{Bl}_Z X$ cut out by the Qco ideal of sections supported on $Y \times_X E_Z Y$. ⌟

Prop. (6.8.2.5) [Strict Transformation]. Let $Z \subset X$ is a closed subscheme and $f : Y \to X$ be a morphism, then the strict transform of Y is the blowing-up of Y at the closed subscheme $f^{-1}Z$. ⌟

Proof: Cf.[Sta]080E.? (Recall the definition of fiber product, we only need to check for Z,X affine and glue. For this, check $B \otimes_A (\oplus I^d) \to \oplus (IB)^d$ defines the fiber map). □

Prop. (6.8.2.6). If X is H-(quasi-)projective, then so does $\widetilde{X}_I$ and π is H-projective(6.5.2.19). And any birational projective morphism from another variety Z to X comes from a blowing-up. ⌟

Proof: Cf.[Hartshorne P166]. □

Prop. (6.8.2.7) [Exceptional Divisor]. Let E be $\pi^{-1}(x)$ for a blowing-up, called the **exceptional divisor**. Often the line bundle $\mathcal{O}_{\widetilde{X}}(E)$ associated with it is called denoted by E.

There are canonical coordinates near E: let $\widetilde{U}_i$ be $\widetilde{U} - \{(l_i = 0)\}$, then endow $\widetilde{U}_i$ with the coordinate $z(i) = (l_j/l_i, \ldots, z_i, \ldots, l_n/l_i)$, it is holomorphic to $\mathbb{C}^n$. π in this coordinate is written as $(z(1), \ldots, z(n)) \mapsto (z(i)z(1), \ldots, z(i), \ldots, z(n)z(i))$.

The transition function can be written, it is

$$\varphi_j \circ \varphi_i^{-1}((z(i)_1, \ldots, z(i)_n)) = (\frac{z(i)_1}{z(i)_j}, \ldots, \frac{1}{z(i)_j}, \ldots, z(i)_i z(i)_j, \ldots, \frac{z(i)_n}{z(i)_j}).$$

Notice it is somewhat tricky because it has two different coordinates.

The defining function of E in this coordinate is $(z(i)) = (z_i)$. So the line bundle $\mathcal{O}_{\widetilde{X}}(E)$ has transition function $g_{ij} = z(i)/z(j)$, and it can be thought of as the line bundle that has line $[l]$ at the point $(z, [l]) \in \widetilde{U}$. So it is kindof tautological, in fact its restriction on $E \cong \mathbb{CP}^{n-1}$ is just the tautological line bundle. ⌟

Prop. (6.8.2.8). The canonical line bundle $\mathcal{K}_{\widetilde{X}} = \pi^*\mathcal{K}_X + (n-1)E$, where n is the dimension of X. ⌟

Proof: Away from E, the π is a holomorphism, so It suffices to compare the two transition function of the two canonical maps near E using the coordinates in(6.8.2.7), with the local section given by $dz_1 \wedge \ldots \wedge dz_n$ and $dz(i)_1 \wedge dz(i)_n$ respectively. On $\widetilde{U}_i$, locally $dz_1 \wedge \ldots \wedge dz_n$ is pulled by π^* to the trivial bundle on U', and by calculation, $dz(j)_1 \wedge dz(j)_n = z(i)_j^{n-1} dz(i)_1 \wedge dz(i)_n$, so $\mathcal{K}_{\widetilde{X}} - (n-2)E$ has a global section $z(i)_i^{n-1} dz(i)_1 \wedge dz(i)_n$, so it is also trivial on $\widetilde{U}$, so $\mathcal{K}_{\widetilde{X}} = \pi^*\mathcal{K}_X + (n-1)E$ is true. □

Blowing up along a regular variety

Prop. (6.8.2.9). If X is a regular variety over k and Y is a regular closed subvariety defined by $\mathcal{I}$, then the blowing up along $\mathcal{I}$ is also regular, and the inverse image Y' of Y is locally principal in it. In fact, $Y' \to Y$ is isomorphic to $\mathbb{P}(\mathcal{I}/\mathcal{I}^2)$, the projective space associated to the locally free bundle $\mathcal{I}/\mathcal{I}^2$ on Y, and the normal sheaf $\mathcal{N}_{Y'/X'} \cong \mathcal{O}_{\mathbb{P}(\mathcal{I}/\mathcal{I}^2)}(-1)$. ⌟

Proof: (Imagine the blowing up of $\mathbb{A}^2$ along $\{0\}$). $X' \cong \operatorname{Proj} \oplus \mathcal{I}^d$ and $Y' \cong \operatorname{Proj} \oplus \mathcal{I}^d/\mathcal{I}^{d+1}$. Then since Y is regular, (5.3.4.17) tells us $\mathcal{I}$ is locally generated by a regular sequence and(5.3.4.16) tells $Y' = \mathbb{P}(\mathcal{I}/\mathcal{I}^2)$. Y' is regular by(5.3.5.18), and then(5.3.5.24) shows that X' is regular also. For the normal sheaf, the defining sheaf $\mathcal{I}' = \mathcal{O}_{X'}$ and then $\mathcal{I}'/\mathcal{I}'^2 = \mathcal{O}_Y(1)$, thus $\mathcal{N}_{Y'/X'} \cong \mathcal{O}_{\mathbb{P}(\mathcal{I}/\mathcal{I}^2)}(-1)$. □

Prop. (6.8.2.10). In a blowing up along a regular variety of codimension $r \geq 2$, There is an isomorphism $\operatorname{Pic} X' \cong \operatorname{Pic} X \oplus \mathbb{Z}$ induced by the Weil divisor exact sequence of $Y' \subset X'$. This is because $r \geq 2$ and (6.8.2.2).

We also have $\omega_{X'} = f^*\omega_X \otimes \mathcal{L}((r-1)Y')$ because $\mathcal{L}(Y') = \mathcal{O}(-1)$ and $\omega_Y \cong \omega_X \otimes \mathcal{L}(D) \otimes \mathcal{O}_Y$ by(6.11.1.17), so it suffice to prove $\omega_{Y'} \cong f^*\omega_X \otimes \mathcal{O}_{Y'}(-r)$. For this, notice for a closed pt of Y, the fiber is a $\mathbb{P}^{r-1}$ because $\mathcal{I}/\mathcal{I}^2$ is locally free of rank r by(6.11.1.16) and the functoriality of $\mathcal{O}(1)$. ⌟

3 Compatifications

Def. (6.8.3.1) [Compatifications]. Let $S \in \mathcal{S}\mathrm{ch}_{\mathrm{qcqs}}, X \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,ft}}/S$, then the category of **compatifications of** X/S is the category of pairs $(i, \overline{X})$, where $i : X \to \overline{X}$ is an immersion and $\overline{X} \to S$ is proper. ⌟

Thm. (6.8.3.2)[Nagata Compatification]. Situation as in(6.8.3.1), then X/S has a compactification. ⌟

Proof: Cf.[Sta]0F41. □

4 Limits of Schemes

Prop. (6.8.4.1) [Noetherian Reduction]. For any $S \in \mathcal{S}\mathrm{ch}_{\mathrm{qcqs}}$, there exists a direct system $(S_i, f_{ii'})$ indexed over a set I that

- $f_{ii'}$ are affine.
- S_i are of f.t. over $\mathbb{Z}$.
- $S = \varprojlim_i S_i$.

⌟

Proof: Cf.[Sta]01ZA. □

Prop. (6.8.4.2) [Characterizing Morphisms of F.P.]. Let $f : X \to S$ be a morphism of schemes, then the following are equivalent:

- f is locally of finite presentation.
- For any directed inverse system $(T_i, f_{ii'})$ in $\mathcal{A}\mathrm{ff}_S$, we have

$$\mathrm{Mor}_S(\varprojlim_i T_i, X) = \varinjlim_i \mathrm{Mor}_S(T_i, X)$$

- For any directed inverse system $(T_i, f_{ii'})$ in $\mathcal{S}\mathrm{ch}_S$ with T_i qcqs and $f_{ii'}$ affine, we have

$$\mathrm{Mor}_S(\varprojlim_i T_i, X) = \varinjlim_i \mathrm{Mor}_S(T_i, X)$$

⌟

Proof: Cf.[Sta]01ZC. □

Prop. (6.8.4.3) [Reduction to Finite Presented Morphisms]. Let $f : X \to S$ be a morphism of schemes, if X is qcqs and S is qs, then $X = \varprojlim_i X_i$ is a limit of a directed system of schemes X_i of f.p. over S with affine morphisms over S. ⌟

Proof: Cf.[Sta]09MV. □

Prop. (6.8.4.4) [Integral and Finite]. Let $f : X \to S$ be an integral morphism of schemes with S qcqs, then $X = \varprojlim_i X_i$ is a limit of a directed system of schemes X_i finite of f.p. over S with affine morphisms over S. ⌟

Proof: Consider $\mathcal{A} = f_*\mathcal{O}_X$, which is a Qco sheaf of $\mathcal{O}_S$-modules. Then $\mathcal{A} = \varinjlim \mathcal{A}_i$ is a filtered colimit of finite and f.p. $\mathcal{O}_S$-modules by(6.5.1.13). Then $X_i = \mathbf{Spec}_S(\mathcal{A}_i)$ satisfies the requirement by(6.2.7.12). □

Descending Properties

Prop. (6.8.4.5) [Descending l.p. Schemes]. ⌟

Descending Properties of Morphisms

Prop. (6.8.4.6) [Descending Properness]. Cf.[Sta]0CNV. ⌟

Prop. (6.8.4.7) [Descending Morphisms between l.p. schemes]. ⌟

Sheaves

5 $D_{\mathcal{QC}oh}(X)$

Def. (6.8.5.1) [Notations]. For $X \in \mathcal{S}\mathrm{ch}$,

Denote $D^*_{\mathcal{QC}oh}(X) = D^*_{\mathcal{QC}oh(X)}(\mathcal{M}od(\mathcal{O}_X))$(4.10.1.8). There is a natural functor $D^*(\mathcal{QC}oh(X)) \to D^*_{\mathcal{QC}oh}(X)$.

Denote $D^*_{\mathcal{C}oh}(X) = D^*_{\mathcal{C}oh(X)}(\mathcal{M}od(\mathcal{O}_X))$(4.10.1.8). There is a natural functor $D^*(\mathcal{C}oh(X)) \to D^*_{\mathcal{C}oh}(X)$.

By(6.3.1.5), these notions are affine local. ⌟

Prop. (6.8.5.2) [Direct Sum]. Direct sum exists in $D_{\mathcal{QC}oh}(X)$, and equals that in $D(X)$. ⌟

Proof: By(4.10.1.15), direct sum exists in $D(X)$ and are given by term-wise direct sums. Notice the direct sum of elements in $D_{\mathcal{QC}oh}(X)$ is also in $D_{\mathcal{QC}oh}(X)$ as direct sums are exact functor and $\mathcal{QC}oh(X)$ is stable under direct sums. □

Prop. (6.8.5.3) [Affine Case]. Let $X = \mathrm{Spec}\, A$, there is a natural equivalence$\tilde{}: D(A) \to D(\mathcal{QC}oh(X))$. Then the functors $R\Gamma(X, -) : D_{\mathcal{QC}oh}(X) \to D(A)$ is quasi-inverse to the inclusion functor $D^*(\mathcal{QC}oh(X)) \to D^*_{\mathcal{QC}oh}(X)$(6.8.5.1), and they are both isomorphism of triangulated categories. ⌟

Proof: Cf.[Sta]06Z0. □

Prop. (6.8.5.4) [Derived Pullbacks]. Let $f : X \to S$ be a qcqs morphism of schemes, then Lf^* maps $D_{\mathfrak{QCoh}}(X)$ into $D_{\mathfrak{QCoh}}(S)$, and affine locally it is just the derived tensor functor $-\otimes^{\mathrm{L}}_A B : D(A) \to D(B)$ via identifications in(6.8.5.3), by(6.3.3.14)(6.3.3.15). ⌟

Prop. (6.8.5.5) [Derived Products]. For $X \in \mathcal{S}\mathrm{ch}$, $D_{\mathfrak{QCoh}}(X)$ is stable under derived tensor products, and affine locally it is just the derived tensor product $- \otimes^{\mathrm{L}} -$ via identifications in(6.8.5.3), by(6.3.3.6)(6.3.3.15). ⌟

Prop. (6.8.5.6) [Higher Direct Images]. Let $f : X \to S$ be a qcqs morphism of schemes, then Rf_* maps $D_{\mathfrak{QCoh}}(X)$ into $D_{\mathfrak{QCoh}}(S)$. And if f is affine, affine locally it is just the restriction $D(B) \to D(A)$ via identifications in(6.8.5.3), by(6.3.1.9).

Moreover, if S is qc, then there exists a $N \in \mathbb{Z}$ s.t. $Rf_*(D^{\leq m}_{\mathfrak{QCoh}}(X)) \subset D^{\leq m+N}_{\mathfrak{QCoh}}(S)$, and this N is invariant under base change. ⌟

Proof: Cf.[Sta]08D5.? □

Prop. (6.8.5.7). For $f : X \to Y$ qcqs, $Rf_* : D_{\mathfrak{QCoh}}(X) \to D_{\mathfrak{QCoh}}(Y)$ preserves direct sums. ⌟

Proof: Cf.[Sta]08DZ. □

Prop. (6.8.5.8) [Projection Formula]. Let $f : X \to Y$ be a qcqs morphism of schemes and $E \in D_{\mathfrak{QCoh}}(X), K \in D_{\mathfrak{QCoh}}(Y)$, then the projection map(6.3.3.19)

$$Rf_*(E) \otimes^{\mathrm{L}}_{\mathcal{O}_Y} K \to Rf_*(E \otimes^{\mathrm{L}}_{\mathcal{O}_Y} Lf^* K)$$

is an isomorphism. ⌟

Proof: Cf.[Sta]08EU. □

Pseudo-Coherent and Perfect Complexes

Prop. (6.8.5.9) [Affine Case]. If $X = \operatorname{Spec} A$, $M \in D(A)$ and E is the corresponding element in $D(X)$, then

- E is an (m-)pseudo-coherent object in $D(X)$ iff M is an (m-)pseudo-coherent object in $D(A)$(5.9.5.9).
- E has Tor-amplitude in $[a, b]$ iff M has Tor amplitude in $[a, b]$.
- E is a perfect object in $D(X)$ iff M is a perfect object in $D(A)$(5.9.5.3).

⌟

Proof: Cf.[Sta]08E7, 08EB, 08E9,. □

Prop. (6.8.5.10) [Noetherian Case]. Let X be a Noetherian scheme and $\mathcal{E} \in D_{\mathfrak{QCoh}}(X)$, then the following are equivalent:

- $\mathcal{E}$ is m-pseudo-coherent.
- $\mathcal{E} \in D^-_{\mathfrak{QCoh}}(X)$ and $H^i(\mathcal{E}) \in \mathfrak{Coh}(X)$ for $i \geq m$.

In particular, E is pseudo-coherent iff $E \in D^-_{\mathfrak{Coh}}(X)$. ⌟

Proof: Cf.[Sta]08E8. □

Prop. (6.8.5.11) [$\mathcal{E}xt$]. Let $X \in \mathcal{S}\mathrm{ch}$.

1. If $X = \operatorname{Spec} A$ and $K, L \in D(A)$, then $\mathcal{E}xt^n(\widetilde{K}, \widetilde{L})$ is the sheaf extending the sheaf on the basis $D(f) \mapsto \operatorname{Ext}^n_{A_f}(K_f, L_f)$.
2. If $X = \operatorname{Spec} A$ and $K, L \in D(A)$, then $R\mathcal{H}om(\widetilde{K}, \widetilde{L}) = (R\operatorname{Hom}_A(K, L))^\sim$ iff K is pseudo-coherent and $L \in D^+(A)$, or K is perfect.
3. If $\mathcal{L} \in D_{\mathcal{QC}oh}(X)$ and $\mathcal{K} \in D(X)$ perfect, then $R\mathcal{H}om(\mathcal{K}, \mathcal{L}) \in D_{\mathcal{QC}oh}(X)$.
4. If $\mathcal{L} \in D^+_{\mathcal{QC}oh}(X)$ and $\mathcal{K} \in D(X)$ pseudo-coherent, $R\mathcal{H}om(\mathcal{K}, \mathcal{L}) \in D_{\mathcal{QC}oh}(X)$ and are locally bounded below.

⌟

Proof: 1: This follows from(6.3.3.27) as

$$H^n(R\mathcal{H}om(X_f, \widetilde{K}, \widetilde{L})) = \operatorname{Hom}_{D(\mathcal{O}_{X_f})}(\widetilde{K}_f, \widetilde{L}_f[n]) = \operatorname{Hom}_{D(A_f)}(K_f, L_f[n]) = \operatorname{Ext}^n(K_f, L_f).$$

2: This follows from(6.3.4.22).
3, 4 follows from item2,(6.3.4.22) and locality of cohomology. □

Prop. (6.8.5.12) [Criterion for Relative Perfectness over Affine Base]. Let $A \in \mathcal{CA}\mathrm{lg}$ and X be a separated, flat of f.p. scheme over A, $K \in D_{\mathcal{QC}oh}(X)$. If $R\Gamma(X, E \otimes^{\mathrm{L}} K)$ is perfect in $D(A)$ for any perfect object $E \in D(X)$, then K is perfect over A. ⌟

Proof: Cf.[Sta]0GET. □

<u>$D_{\mathcal{C}oh}(X)$</u>

Prop. (6.8.5.13) [$R\mathcal{H}om$ Preserves $D_{\mathcal{C}oh}(X)$]. If X is a locally Noetherian scheme and $L \in D^+_{\mathcal{C}oh}(X)$ and $K \in D^-_{\mathcal{C}oh}(X)$, then $R\mathcal{H}om(K, L) \in D^+_{\mathcal{C}oh}(X)$. ⌟

Proof: Cf.[Sta]0D0C. □

Prop. (6.8.5.14). Let X be a Noetherian scheme, then there are natural equivalences

$$D^-(\mathcal{C}oh(X)) \cong D^-_{\mathcal{C}oh(X)}(\mathcal{QC}oh(X)) \cong D^-_{\mathcal{C}oh}(X), \quad D^b(\mathcal{C}oh(X)) \cong D^b_{\mathcal{C}oh}(X).$$

⌟

Proof: Cf.[Sta]0FDA, 0FDB. □

Prop. (6.8.5.15). Let S be Noetherian and $f : X \to S$ be a proper morphism, then Rf_* maps $D^b_{\mathcal{C}oh}(X)$ to $D^b_{\mathcal{C}oh}(S)$. ⌟

Proof: Cf.[Sta]08E2. □

Prop. (6.8.5.16) [Perfect Complexes for Regular Schemes]. If X is a Noetherian regular scheme of finite dimension, then $D^b_{\mathcal{C}oh}(X)$ consists exactly of the perfect objects in $D(X)$, by(5.9.5.5) and(6.8.5.9). ⌟

Def. (6.8.5.17) [K-Groups of Schemes]. Let $X \in \mathcal{S}\mathrm{ch}$, the **Grothendieck group** of X is defined to be $K_0(X) = K_0(D_{\mathrm{perf}}(X))$. If X is locally Noetherian, also define the **Grothendieck group of coherent sheaves** on X to be $K_0'(X) = K_0(\mathcal{C}oh(X))$. ⌟

Prop. (6.8.5.18). If X is Noetherian, then

$$K_0'(X) = K_0(\mathcal{C}\mathrm{oh}(X)) = K_0(D^b(\mathcal{C}\mathrm{oh}(X))) = K_0(D^b_{\mathcal{C}\mathrm{oh}}(X)).$$

In particular, there is a map $K_0(X) \to K_0'(X)$. ⌟

Proof: This follows from(4.10.1.13) and(6.8.5.14). □

Prop. (6.8.5.19) [$K_0 \cong K_0'$]. If X is a Noetherian regular scheme of finite dimension, then the map $K_0(X) \to K_0'(X)$(6.8.5.18) is an isomorphism, by(6.8.5.16). ⌟

Prop. (6.8.5.20). For $X \in \mathcal{S}\mathrm{ch}$, $- \otimes^{\mathrm{L}} -$ defines a ring structure on $K_0(X)$, by(10.1.2.2) and(4.10.3.12). ⌟

Prop. (6.8.5.21). If $X = \operatorname{Spec} R$, then $K_0(X) = K_0(R)$. And if R is Noetherian, then $K_0'(X) = K_0'(R)$. ⌟

Proof: Cf.[Sta]0FDH. □

Prop. (6.8.5.22) [Push and Pull]. Let $f : X \to Y$ be a proper morphism of locally Noetherian schemes, then there is a map

$$f_* : K_0'(X) \to K_0'(Y) : [\mathcal{F}] \mapsto \oplus_{i\geq 0}[R^{2i} f_*\mathcal{F}] - \oplus_{i\geq 0}[R^{2i+1} f_*\mathcal{F}],$$

which is definable by(6.8.5.15). And there is an obvious map $f^* : K_0'(Y) \to K_0'(X)$. They satisfy

$$f_*(\alpha \cdot f^*\beta) = f_*\alpha \cdot \beta, \alpha \in K_0'(X), \beta \in K_0'(Y).$$

⌟

Proof: The first assertion follows from long exact sequence for Rf_*. The last assertion follows from projection formula(6.8.5.8). □

Prop. (6.8.5.23) [Lambda Operators]. Let $X \in \mathcal{S}\mathrm{ch}$, there are functor $\lambda^r : K_0(\mathcal{C}\mathrm{oh}^{\mathrm{free}}(X)) \to K_0(\mathcal{C}\mathrm{oh}^{\mathrm{free}}(X))$ that sends $[\mathcal{E}]$ to $[\wedge^r\mathcal{E}]$. ⌟

Proof: Consider a map $c : \mathcal{C}\mathrm{oh}^{\mathrm{free}}(X) \to K_0(\mathcal{Q}\mathcal{C}\mathrm{oh}^{\mathrm{free}}(X))[t] : \mathcal{E} \mapsto \sum_{i=0}^{\infty}[\wedge^i\mathcal{E}]t^i$. It suffices to prove that for any exact sequence $0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0$, $c(\mathcal{E}) = c(\mathcal{E}')c(\mathcal{E}'')$, and then take λ^r as

$$c(M) = \sum_{r>0} \lambda^r(M)t^r.$$

To show this, notice that there is a filtration of $\wedge^r\mathcal{E}$ with quotients

$$\wedge^r\mathcal{E}', \wedge^{r-1}(\mathcal{E}') \otimes \mathcal{E}'', \ldots, \wedge^r(\mathcal{E}''),$$

by(6.5.1.26). □

Prop. (6.8.5.24) [Adam Operators]. Let $X \in \mathcal{S}\mathrm{ch}$, then there is are **Adam operators**

$$\psi^{-1}, \psi^1, \psi^2, : K_0(X) \to K_0(X)$$

s.t. for $\mathcal{L} \in \mathrm{Pic}(X)$,

$$\psi^{-1}[\mathcal{L}] = [\mathcal{L}^{-1}], \quad \psi^1[\mathcal{L}] = [\mathcal{L}], \quad \psi^2[\mathcal{L}] = [\mathcal{L}^{\otimes 2}].$$

⌟

Proof: For any $L \in K_0(X)$, there is an action of $\{\pm 1\}$ on $L \otimes^{\mathrm{L}} L$ by switching factors. Denote $(L \otimes^{\mathrm{L}} L)^+, (L \otimes^{\mathrm{L}} L)^-$ the fixed and anti-fixed parts**?** of $L \otimes^{\mathrm{L}} L$, and define $\psi^2[L] = [(L \otimes^{\mathrm{L}} L)^+] - [(L \otimes^{\mathrm{L}} L)^-]$. **?** □

Coherator

Prop. (6.8.5.25) $[R\mathcal{Q}_X]$. ⌟

Prop. (6.8.5.26) $[D\mathcal{Q}_X]$. Let X be a qcqs scheme, then the inclusion functor $D_{\mathcal{QC}oh}(X) \to D(X)$ has a right adjoint, called the **coherator**, denoted by $D\mathcal{Q}_X$. ⌟

Proof: Use(4.8.4.32). The conditions are satisfied as $D_{\mathcal{QC}oh}(X)$ is compactly generated and has direct sums that is preserved by inclusion by(6.8.5.30)(6.8.5.2). □

Prop. (6.8.5.27). Let $f : X \to Y$ be a morphism of qcqs schemes, then

$$Rf_* \circ D\mathcal{Q}_X = D\mathcal{Q}_Y \circ Rf_* : D(X) \to D_{\mathcal{QC}oh}(Y).$$

⌟

Proof: They are both right adjoint to $Lf^* : D_{\mathcal{QC}oh}(Y) \to D(X)$, as Lf^* maps $D_{\mathcal{QC}oh}(Y)$ into $D_{\mathcal{QC}oh}(X)$(6.8.5.4). □

Prop. (6.8.5.28) [Cohomological Boundedness of $D\mathcal{Q}_X$]. Let X be a qcqs scheme, then there exists $N \in \mathbb{Z}$ s.t. if $K \in D(X)$ satisfies $K|_U \in D^{[a,b]}(\mathcal{O}_U)$ for any affine open $U \subset X$, then $D\mathcal{Q}_X(K) \in D^{[a,b+N]}_{\mathcal{QC}oh}(X)$. ⌟

Proof: Cf.[Sta]0CSA. □

Compact Generators

Prop. (6.8.5.29) [Perfect and Compact Objects]. Let X be a qcqs scheme, then $K \in D(X)$ is perfect iff it is a compact object in $D_{\mathcal{QC}oh}(X)$. ⌟

Proof: Cf.[Sta]09M1. □

Prop. (6.8.5.30) [$D_{\mathcal{QC}oh}(X)$ is Compactly Generated]. There is a perfect object $P \subset D_{\mathcal{QC}oh}(X)$ that is a generator of $D_{\mathcal{QC}oh}(X)$(4.8.4.28). ⌟

Proof: Cf.[Sta]09IS. □

Resolution Property

Def. (6.8.5.31) [Resolution Properties]. A scheme X is said to have **resolution property** iff every $\mathcal{F} \in \mathcal{QC}oh^{\mathrm{ft}}(X)$ is a quotient of a locally free sheaf. ⌟

Prop. (6.8.5.32). If X has an ample invertible sheaf, then X has the resolution property by(6.5.4.5). In fact, every coherent sheaf is a quotient of a finite direct sum of $\mathcal{O}_X(-n)$. ⌟

Prop. (6.8.5.33) [Regular Scheme has Resolution property]. If X is qc regular scheme with an affine diagonal, then X has the resolution property, Cf.[Sta]0F8A**?**. Conversely, if X is qcqs with the resolution property, then X has affine diagonal. Cf.[Sta]0F8C. ⌟

Prop. (6.8.5.34) [Kleiman]. If X is a qc irreducible and locally factorial scheme with affine diagonal map, then X has the resolution property. ⌟

Proof: By(6.8.1.6), we have an basis of the form X_s for $s \in \Gamma(X, \mathcal{L})$ for various invertible sheaves, then for any coherent sheaf, it is generated by f.m. sections in $\Gamma(U_i, \mathcal{F})$ and $U_i = X_s$ for $s \in \Gamma(X, \mathcal{L})$, and for each of them, we can use(6.5.3.5), we can extend these to global sections on $\Gamma(\mathcal{F} \otimes \mathcal{L}_i^{n_i})$ for n_i large. Then tensoring $\mathcal{L}_i^{-n}$, we find a $\oplus L_i^{-n_i} \to \mathcal{F}$ surjective. □

Prop. (6.8.5.35). When X has the resolution property, $\mathcal{E}xt^\bullet(-, \mathcal{G})$ is an universal δ-functor for every $\mathcal{G} \in \mathfrak{QCoh}(X)$, because locally free sheaf is adapted to $\mathcal{E}xt^\bullet(-, \mathcal{G})$ by(6.3.3.25), so we can calculate $\mathcal{E}xt(\mathcal{F}, \mathcal{G})$ using a finite locally free resolution of $\mathcal{F}$. ⌟

Prop. (6.8.5.36). If X is a qcqs scheme with the resolution property, then the map $K_0(\mathcal{V}\mathrm{ect}(X)) \to K_0(X)$ is an isomorphism. ⌟

Proof: Cf.[Sta]0FDJ. □

6 Duality for Schemes

Main references are [Hartshorne Residues and Duality, Hartshorne], [Sta]Chap48 and [Grothendieck Duality and Base Change, Conrad]

Right Adjoints of Pushforwards

Prop. (6.8.6.1) [Right Adjoints of Pushforwards Exist]. Let $f : X \to Y$ be a morphism between qcqs schemes, then the functor $Rf_* : D_{\mathfrak{QCoh}}(X) \to D_{\mathfrak{QCoh}}(Y)$ has a right adjoint, denoted by $f^\times$. ⌟

Proof: Use(4.8.4.32). The conditions are satisfied as $D_{\mathfrak{QCoh}}(X)$ is compactly generated and has direct sums by(6.8.5.30)(6.8.5.2), and Rf_* preserves direct limits(6.8.5.7). □

Prop. (6.8.6.2). Let $f : X \to Y$ be a morphism between qcqs schemes, then $f^\times$ maps $D^+_{\mathfrak{QCoh}}(Y)$ into $D^+_{\mathfrak{QCoh}}(X)$. ⌟

Proof: This follows from the fact Rf_* has finite cohomological dimension N(6.8.5.6) and(4.10.1.18). □

Prop. (6.8.6.3). Let $f : X \to Y$ be a morphism of qcqs schemes, then for $K \in D_{\mathfrak{QCoh}}(X), L \in D_{\mathfrak{QCoh}}(Y)$, there is a canonical map

$$Rf_* R\mathcal{H}om_{\mathcal{O}_X}(L, f^\times K) \to R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* L, Rf_* f^\times K) \to R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* L, K),$$

by(6.3.3.31) and adjunction.

Then this map becomes isomorphism after applying the coherator $D\mathfrak{Q}_X$(6.8.5.26). ⌟

Proof: By Yoneda lemma, it suffices to show that for any $M \in D_{\mathfrak{QCoh}}(Y)$,

$$\mathrm{Hom}_Y(M, Rf_* R\mathcal{H}om_{\mathcal{O}_X}(L, f^\times K)) \cong \mathrm{Hom}_Y(M, R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* L, K)):$$

$$\begin{aligned}
\mathrm{Hom}_Y(M, Rf_* R\mathcal{H}om_{\mathcal{O}_X}(L, f^\times K)) &= \mathrm{Hom}_X(Lf^* M, R\mathcal{H}om_{\mathcal{O}_X}(L, f^\times K)) \\
&= \mathrm{Hom}_X(Lf^* M \otimes^{\mathrm{L}} L, f^\times K) \\
(\text{ as } Lf^* M \otimes^{\mathrm{L}} L \in D_{\mathfrak{QCoh}}(X) \text{ by (6.8.5.4)(6.8.5.5)}) &= \mathrm{Hom}_Y(Rf_*(Lf^* M \otimes^{\mathrm{L}} L), K) \\
&= \mathrm{Hom}_Y(M \otimes Rf_* L, K) \\
&= \mathrm{Hom}_Y(M, R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* L, K))
\end{aligned}$$

□

Cor. (6.8.6.4). By(6.8.5.6), this adjointness is true without coheration if both $R\mathcal{H}om_{\mathcal{O}_X}(L, f^\times K)$ and $R\mathcal{H}om_{\mathcal{O}_Y}(Rf_*L, K)$ are in $D_{\mathfrak{QCoh}}(Y)$. This is the case if L, Rf_*L are perfect or $K \in D^+_{\mathfrak{QCoh}}(Y)$ and and L, Rf_*L are pseudo-coherent, by(6.8.5.11).

In particular, this holds if $f : X \to Y$ is a proper morphism of Noetherian schemes and $L \in D^-_{\mathfrak{Coh}}(X)$ and $S \in D^+_{\mathfrak{QCoh}}(S)$, by(6.8.5.15) and(6.8.5.10). ⌟

Cor. (6.8.6.5) [Global Sections]. Let $f : X \to Y$ be a morphism of qcqs schemes, then for $K \in D_{\mathfrak{QCoh}}(X), L \in D_{\mathfrak{QCoh}}(Y)$, there is a canonical isomorphism

$$R\operatorname{Hom}_{\mathcal{O}_X}(L, f^\times K) \to R\operatorname{Hom}_{\mathcal{O}_Y}(Rf_*L, Rf_*f^\times K) \to R\mathcal{H}om_{\mathcal{O}_Y}(Rf_*L, K)$$

⌟

Proof: This is because for any $E \in D(X)$, $H^i(X, E) = \operatorname{Ext}^i_X(\mathcal{O}_X, E) = \operatorname{Hom}(\mathcal{O}_X[-i], E) = \operatorname{Hom}(\mathcal{O}_X[-i], D\mathfrak{Q}(E))$ only depends on $D\mathfrak{Q}(E)$. □

Prop. (6.8.6.6) [Proper Flat $f^\times$]. Let $f : X \to Y$ be a proper flat morphism of f.p. between qcqs schemes, then $f^\times$ is compatible with base change between qcqs schemes. ⌟

Proof: Cf.[Sta]0AAB. □

Upper Shriek

Def. (6.8.6.7) [$\mathcal{S}\mathrm{ch}^{\mathrm{ft,sep}}_S$]. For a locally Noetherian scheme S, let $\mathcal{S}\mathrm{ch}^{\mathrm{ft,sep}}_S$ be the full subcategory of $\mathcal{S}\mathrm{ch}/S$ consisting of schemes separated of f.t. over S. ⌟

Prop. (6.8.6.8) [Lower Shriek]. Let $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{ft,sep}}_S$, take a compactification $\overline{f} : \overline{X} \to Y$ of X/Y, then we can define the functor

$$f^! : D^+_{\mathfrak{QCoh}}(Y) \to D^+_{\mathfrak{QCoh}}(X) : f^!K = \overline{f}^\times(K)|_X.$$

and this functor is independent of the compactification chosen. ⌟

Proof: Cf.[Sta]0AA0. □

Prop. (6.8.6.9). If $f : X \to Y, g : Y \to Z \in \mathcal{S}\mathrm{ch}^{\mathrm{ft,sep}}_S$, then there is a canonical isomorphism of functors $(g \circ f)^! \cong f^! \circ g^!$. ⌟

Proof: Cf.[Sta]0ATX. □

Prop. (6.8.6.10) [Properties of $f^!$]. Let $S \in \mathcal{S}\mathrm{ch}$ be Noetherian, then for $X, Y \in \mathcal{S}\mathrm{ch}^{\mathrm{ft,sep}}_S$,

- If $j : X \to Y$ is an open immersion, then $j^! = j^*$.
- If $i : X \to Y$ is a closed immersion, then $i^! = R\mathcal{H}om(\mathcal{O}_X, -)$.
- $f^!$ maps $D^+_{\mathfrak{QCoh}}(Y)$ into $D^+_{\mathfrak{QCoh}}(X)$.
- If $f : X \to Y$ is a local complete intersection morphism, then $f^!\mathcal{O}_Y$ is an invertible object of $D(X)$, and $f^!$ preserves perfect complexes.
- If $f : X \to Y$ is finite, then $f_*f^!(-) = R\mathcal{H}om_{\mathcal{O}_Y}(f_*\mathcal{O}_X, -)$.
- If $f : X \to Y$ is an effective Cartier divisor, then $f^!(-) = Lf^*(-) \otimes^{\mathrm{L}}_{\mathcal{O}_X} \mathcal{O}_Y(-X)[-1]$.
- If $f : X \to Y$ is a Koszul regular immersion of codimension c, then $f^!(-) = Lf^*(-) \otimes^{\mathrm{L}} \wedge^c \mathcal{N}[-c]$.
- If $f : X \to Y$ is smooth proper of relative dimension d, then $f^!(-) = Lf^*(-) \otimes^{\mathrm{L}} \Omega^d_{X/Y}[d]$.

⌟

Proof: Cf.[Sta]0AU0, 0AA2, 0AU1, 0B6V, 0AU3.? □

Dualizing Complexes

Def. (6.8.6.11) [Dualizing Complex]. Let X be a locally Noetherian scheme, then a complex $K \in D_{\mathfrak{QCoh}}(X)$ is called a **dualizing complex** if it satisfies the following equivalent conditions:

- For any affine open $U = \operatorname{Spec} A \subset X$, $K|_U$ is a dualizing complex in $D(A)$.
- There exists an affine open covering $U_i = \operatorname{Spec} A_i$ of X s.t. $K|U_i$ is a dualizing complex in $D(A_i)$ for any i.

⌟

Proof: This follows from(5.9.8.2). □

Prop. (6.8.6.12) [Dualizing]. Let X be a locally Noetherian scheme and ω_X be a dualizing complex, then $D = R\mathcal{H}om_{\mathcal{O}_X}(-, \omega_X)$ is an anti-equivalence of $D_{\mathfrak{QCoh}}(X)$ with itself, and there is a canonical isomorphism $\mathrm{id} \cong D^{\circ 2}$.

Moreover, if X is qc, then D exchanges $D^+_{\mathfrak{QCoh}}(X)$ and $D^-_{\mathfrak{QCoh}}(X)$, and induces an equivalence $D : D^b_{\mathfrak{QCoh}}(X) \to D^b_{\mathfrak{QCoh}}(X)$. ⌟

Proof: Cf.[Sta]0A89. □

Thm. (6.8.6.13) [Grothendieck Duality]. Let S be a Noetherian scheme, then

- $f^!$ makes $D^+_{\mathfrak{QCoh}}$ a pseudo-functor on $\mathcal{S}\mathrm{ch}_S^{\mathrm{ft,sep}}$.
- If $f : X \to Y \in \mathcal{S}\mathrm{ch}_S^{\mathrm{ft,sep}}$ is proper, then $f^!$ is the right adjoint of Rf_*, and there is a canonical isomorphism
$$Rf_* R\mathcal{H}om_{\mathcal{O}_X}(K, f^! M) \cong R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* K, M)$$
for any $K \in D^-_{\mathfrak{Coh}}(X)$ and $M \in D^+_{\mathfrak{QCoh}}(Y)$, by**??**
- If $X \in \mathcal{S}\mathrm{ch}_S^{\mathrm{ft,sep}}$ has a dualizing complex ω_X, then $D_X = R\mathcal{H}om(-, \omega_X)$ defines an involution of $D_{\mathfrak{Coh}}(X)$ switching $D^+_{\mathfrak{Coh}}(X)$ and $D^-_{\mathfrak{Coh}}(X)$ and fixing $D^b_{\mathfrak{Coh}}(X)$.
- If Y has a dualizing complex ω_Y, then
  - $\omega_X = f^! \omega_Y$ is a dualizing complex for X,
  - for $M \in D^+_{\mathfrak{Coh}}(Y)$, there is a canonical isomorphism $D_X(f^! M) \cong Lf^* D_Y(M)$.
  - If moreover f is proper, then $Rf_* R\mathcal{H}om_{\mathcal{O}_X}(K, \omega_X) = R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* K, \omega_Y)$ for $K \in D^-_{\mathfrak{Coh}}(X)$.

⌟

Proof: Cf.[Sta]0AU3. □

Thm. (6.8.6.14) [Over a Dualizing Basis]. ⌟

Proof: Cf.[Sta]0AUE. □

Dualizing Modules

Prop. (6.8.6.15) [Relative Dualizing Modules]. Let $f : X \to Y$ be a locally quasi-finite morphism of locally Noetherian schemes, then there exists a unique coherent $\mathcal{O}_Y$-module $\omega_{X/Y} \in \mathfrak{Coh}(Y)$ that affine locally is given by the dualizing sheaf $\omega_{B/A}$(5.9.8.4). ⌟

Proof: Cf.[Sta]0BVG. □

Relative Dualizing Complex

Def. (6.8.6.16) [Relative Dualizing Complexes]. For a separable f.t. morphism of Noetherian schemes $f : X \to S$, the **relative dualizing complex** is defined to be $\omega_{X/S} = f^!\mathcal{O}_S$. ⌟

Prop. (6.8.6.17). Let Y be a qcqs scheme and $f : X \to Y$ be a proper flat morphism of f.p., then

- $\omega_{X/Y}$ is perfect over Y.
- $R^i f_*\omega_{X/Y} = 0$ for $i > 0$.
- $\mathcal{O}_X \to \mathcal{H}om_{\mathcal{O}_X}(\omega_{X/S}, \omega_{X/S})$ is an isomorphism.

⌟

Proof: As $f^\times$ commutes with base change(6.8.6.6), it suffices to assume that $Y = \operatorname{Spec} A$.

1: By(6.8.6.4)(6.3.4.23) and(6.7.5.5), for any perfect object $E \in D(X)$, there are canonical isomorphisms:

$$Rf_*(E \otimes^{\mathrm{L}} \omega_{X/Y}) = Rf_*R\mathcal{H}om_{\mathcal{O}_X}(E^\vee, \omega_{X/Y}) = R\mathcal{H}om_{\mathcal{O}_Y}(Rf_*E^\vee, \mathcal{O}_Y) = (Rf_*E^\vee)^\vee,$$

which is perfect. So $\omega_{X/Y}$ is perfect over S by(6.8.5.12).

2: By(6.8.5.8),

$$\mathcal{H}om_Y(\mathcal{O}_Y[-i], Rf_*\omega_{X/Y}) = \operatorname{Hom}_Y(Rf_*Lf^*\mathcal{O}_Y[-i], \mathcal{O}_Y) = \operatorname{Hom}_Y((Rf_*\mathcal{O}_X)[-i], \mathcal{O}_Y).$$

By proper flat base change(6.7.5.5), $Rf_*\mathcal{O}_X$ is perfect in Y, so it can be represented by a finite complex of finite projective A-modules, so by(6.3.4.22), $R^i f_*\omega_{X/Y} = 0$ for $i > 0$.

3: For any perfect object $E \in D(X)$, by(6.8.6.4)(6.3.4.23)(6.7.5.5)(6.3.4.23) and(6.3.1.9), there are canonical isomorphisms

$$\begin{aligned}\operatorname{Hom}_X(E, R\mathcal{H}om_{\mathcal{O}_X}(\omega_{X/Y}, \omega_{X/Y})) &= \operatorname{Hom}_Y(Rf_*(E \otimes^{\mathrm{L}} \omega_{X/Y}), \mathcal{O}_Y)\\ &= \operatorname{Hom}_Y(Rf_*\mathcal{H}om(E^\vee, \omega_{X/Y}), \mathcal{O}_Y)\\ &= \operatorname{Hom}_Y(\mathcal{H}om(Rf_*E^\vee, \mathcal{O}_Y), \mathcal{O}_Y)\\ &= R\Gamma(Y, Rf_*E^\vee)\\ &= \operatorname{Hom}_X(E, \mathcal{O}_X)\end{aligned}$$

So by(6.8.5.30), perfect objects generate $D_{\mathfrak{QCoh}}(X)$, so $R\mathcal{H}om_{\mathcal{O}_X}(\omega_{X/Y}, \omega_{X/Y}) \cong \mathcal{O}_X$. □

Proper over Field case

Prop. (6.8.6.18)[Serre Duality(Proper over Fields case)]. Let X be a proper scheme over a field k of dimension d, then there exists a unique dualizing complex ω_X with the following properties:

- $H^i(\omega_X) \neq 0$ only for $i \in [-\dim(X), 0]$.
- $[\omega_X] = H^{-d}(\omega_X)$ is a coherent (S_2)-module whose support is the irreducible components of X of dimension d.
- $\dim \operatorname{Supp}(H^i(\omega_X)) \leq -i$.
- For $x \in X$ closed, $H^i(\omega_{X,x}) \oplus \ldots \oplus H^0(\omega_{X,x}) \neq 0$ iff $\operatorname{depth}(\mathcal{O}_{X,x}) \leq -i$.
- For $K \in D_{\mathfrak{QCoh}}(X)$, there is a functorial isomorphisms

$$\operatorname{Ext}_X^{-i}(K, \omega_X) \cong \operatorname{Hom}_k(H^i(X, K), k)$$

compatible with shifts and distinguished triangles, which characterizes ω_X uniquely.

- There are functorial isomorphisms $\mathrm{Hom}(\mathcal{F},[\omega_X])=\mathrm{Hom}_k(H^d(X,\mathcal{F}),k)$ for $\mathcal{F}\in\mathfrak{Coh}(X)$.
- If X is C.M., equidimensional, then $\omega_X=[\omega_X][d]$.
- If X is smooth over k, then $\omega_X=\mathcal{K}_{X/k}[d]$.

⌟

Proof: Cf.[Sta]0FVV, 0AWT.**?** □

Cor. (6.8.6.19) [Serre Duality(Smooth over Fields case)]. If $k\in\mathtt{Field}$, $X\in\mathcal{S}\mathrm{ch}/k$ is a smooth proper scheme over k of dimension d, then for any locally free sheaf $\mathcal{F}$, there is a functorial isomorphism:

$$H^i(X,\mathcal{F})\cong(H^{n-i}(X,\mathcal{F}^\vee\otimes\mathcal{K}_{X/k}))^\vee.$$

⌟

Cor. (6.8.6.20). For a smooth proper variety X over a field k of dimension n, $H^n(X,\mathcal{K}_X)=k$, by(6.11.1.12). ⌟

Cor. (6.8.6.21). For a smooth proper variety X over a field k of dimension n, $\Omega_{X/k}$ is locally free by(6.6.4.15), thus by(6.5.1.25), $\Omega^{n-p}_{X/k}\cong(\Omega^p_{X/k})^\vee\otimes\mathcal{K}_X$. So by(6.8.6.19):

$$H^q(X,\Omega^p_{X/k})\cong(H^{n-q}(X,\Omega^{n-p}_{X/k}))^\vee.$$

⌟

Cor. (6.8.6.22). If X is a closed subscheme of $\mathbb{P}^n_k$ of codimension r, then X has a dualizing sheaf $[\omega_X]=\mathcal{E}xt^r_P(i_*\mathcal{O}_X,\mathcal{K}_{\mathbb{P}^n_k/k})$, and $\mathcal{E}xt^i(i_*\mathcal{O}_X,\mathcal{K}_{\mathbb{P}^n/k})=0$ for $i<r$ ⌟

Proof: This follows from(6.8.6.18) and(6.8.6.13). □

Prop. (6.8.6.23) [Characterizing Cohen-Macauley Schemes]. Let X be projective of dimension n over a field k and $[\omega_X]$ be the dualizing sheaf, then for $\mathcal{F}\in\mathfrak{Coh}(X)$, there is a natural map

$$\mathrm{Ext}^i(\mathcal{F},[\omega_X])\to(H^{n-i}(X,\mathcal{F}))^\vee$$

And the following are equivalent:

- For any $\mathcal{F}$ locally free on X, $H^i(X,\mathcal{F}(-q))=0$ for $i<n$ and q large.
- $H^i(X,\mathcal{O}_X(-q))=0$ for $i<n$ and q large.
- This is an isomorphism of δ-functors.
- X is C.M. and equidimensional.

⌟

Proof: Notice the left side is an universal δ-functor in $\mathcal{F}$ by(6.8.5.35), so the map exist, and
$2\to3$: This implies that the right is also universal by(6.8.5.32).
$3\to1$: For $\mathcal{F}$ locally free, by(6.3.3.33),

$$H^i(X,\mathcal{F}(-q))=(\mathrm{Ext}^{n-i}(\mathcal{F}(-q),\omega_X))^\vee=(H^{n-i}(X,\mathcal{F}^\vee\otimes\omega_X(q)))^\vee$$

which is 0 for q large.

$4 \to 1$: Embed X in $P = \mathbb{P}_k^N$, for $\mathcal{F}$ locally free, since X is catenary, equidimensional is equivalent to $\dim \mathcal{F}_x = n$ for all closed pt x, and C.M. says depth $\mathcal{F}_x = n$. Thus by(5.3.5.26), $pd_{\mathcal{O}_{P,x}} \mathcal{F}_x = N - n$. Thus $\mathcal{E}xt_P^k(\mathcal{F}, -)$ vanish for $k > N - n$ checked on stalks.

Now $H^i(X, \mathcal{F}(-q))$ is dual to $\mathrm{Ext}_P^{N-i}(\mathcal{F}, \omega_P(q))$ by the proof of(6.8.6.22), which is isomorphic to $\Gamma(P, \mathcal{E}xt_P^{N-i}(\mathcal{F}, \omega_P(q)))$ for q large by(6.7.4.9), so it vanish when $i < n$ by what we proved.

$1 \to 4$: The same as the proof of $4 \to 1$, then for $i < n$,

$$\Gamma(P, \mathcal{E}xt_P^{N-i}(\mathcal{F}, \omega_P(q))) = 0 = \Gamma(P, \mathcal{E}xt_P^{N-i}(\mathcal{F}, \omega_P)(q))$$

for q large, so $\mathcal{E}xt_P^{N-i}(\mathcal{F}, \omega_P) = 0$ as it is coherent. Then the stalk is $\mathrm{Ext}_{\mathcal{O}_{P,x}}^{N-i}(\mathcal{O}_{X,x}, \mathcal{O}_{P,x})$, so $pd_{\mathcal{O}_{P,x}} \mathcal{F}_x \leq N - n$ by(5.3.5.27), so depth $\mathcal{O}_{X,x} \geq n$, we must have equality, thus X is C.M. and equidimensional, as it suffice to check at closed pts. □

Cor. (6.8.6.24) [Enriques-Severi-Zariski]. Let X be a normal projective scheme that every irreducible component has dimension≥ 2, then for any $\mathcal{F} \in \mathcal{V}\mathrm{ect}(X)$, $H^1(X, \mathcal{F}(-q)) = 0$ for q large. ⌟

Proof: Just notice that $\dim \mathcal{F}_x \geq 2$, and Serre criterion shows depth $\mathcal{F}_x \geq 2$, the rest is the same as $4 \to 1$ in the proof of(6.8.6.23). □

Prop. (6.8.6.25) [Ample Effective Divisor Connected]. Let X be a proper connected CM. equidimensional scheme over k of dimension at least 2 and D is an ample effective Cartier divisor, then D is connected.

In particular, if X is a smooth complete variety of dimension≥ 2, D is also a complete variety. ⌟

Proof: Let $D = V(s)$, where s is a section of an ample invertible sheaf, then there is an exact sequence

$$0 \to \mathcal{O}_X(-nD) \to \mathcal{O}_X \to i_* \mathcal{O}_{V(s^n)} \to 0,$$

which gives a long exact sequence

$$0 \to H^0(X, \mathcal{O}_X(-nD)) \to H^0(X, \mathcal{O}_X) \to H^0(V(s^n), \mathcal{O}_{V(s^n)}) \to H^1(X, \mathcal{O}_X(-nD)).$$

But by Serre duality(6.8.6.19) and(6.7.2.6), $H^0(X, \mathcal{O}_X(-nD)) = H^{\dim X}(X, [\omega_X] \otimes \mathcal{O}_X(nD)) = 0$ for n sufficiently large, and $H^1(X, \mathcal{O}_X(-nD)) = H^{\dim X - 1}(X, [\omega_X] \otimes \mathcal{O}_X(nD)) = 0$ for n sufficiently large, so $H^0(V(s^n), \mathcal{O}_{V(s^n)}) \cong H^0(X, \mathcal{O}_X)$ has no idempotents for n sufficiently large, so $V(s^n)$ is connected, and D is also connected. □

Cor. (6.8.6.26). Any global complete intersection in $\mathbb{P}^n$ is connected. ⌟

Topological Sheaves

Prop. (6.8.6.27) [Global Verdier Duality]. If $f : X \to Y$ is a map between locally compact spaces with finite dimension, then there exists a functor $f^! : D^+(SAb_Y) \to D^+(SAb_X)$ that

$$R\,\mathrm{Hom}(Rf_! \mathcal{F}^\bullet, \mathcal{G}^\bullet) \cong R\,\mathrm{Hom}(\mathcal{F}, f^! \mathcal{G}^\bullet).$$

In particular, $f^!$ is right adjoint to $Rf_!$. Cf.[Gelfand P228].

There is also a local form of Verdier duality, which implies the global version by taking global section, Cf.[Cohomology of Sheaves Iversen P330]. ⌟

Prop. (6.8.6.28). When $X \to Y$ is an inclusion of open subset, $f_!$ is just $j_!$ defined in(6.2.6.2) and $f^!$ is the restriction. When it is an inclusion of closed subset of locally compact spaces, it is the direct image f_* and $f^!$ is the $j^!$ previously defined in(6.2.6.2). They are not barely defined on $D^+(SAb)$ but on SAb. ⌟

Prop. (6.8.6.29). We consider the case where $f : X \to \mathrm{pt}$, and let $G = \mathbb{Z}$, denote $f^!(\mathbb{Z})$ by $\mathcal{D}_X^\bullet$, called the **dualizing complex**, then there is a duality:

$$R\,\mathrm{Hom}(R\Gamma_c(X, \mathcal{F}^\bullet), \mathbb{Z}) \cong R\,\mathrm{Hom}(\mathcal{F}^\bullet, \mathcal{D}_X^\bullet).$$

for $\mathcal{F}^\bullet \in D^+(\mathcal{S}\mathrm{h}(X))$. ⌟

Prop. (6.8.6.30). When X is a n dimensional topological manifold with boundary, then $\mathcal{D}_X^\bullet = \omega_X[n]$, where the sheaf ω_X is defined by

$$\Gamma(U, \omega_X) = \mathrm{Hom}_{\mathcal{A}\mathrm{b}}(H_c^n(U, \mathbb{Z}), \mathbb{Z}).$$

Cf.[Gelfand P234]. If we replace $\mathbb{Z}$ by a field k, then w_X is the sheaf of k-orientations of $\mathrm{int}(X)$, thus the constant sheaf when X is oriented or char $k = 2$**?**.

In particular, place k in dimension i then we get an isomorphism

$$\mathrm{Hom}_k(H_c^i(X, \mathcal{F}), k) = \mathrm{Ext}^{n-i}(\mathcal{F}, \omega_X)$$

(because k is a field thus injective). Gelfand even gives an interpretation of this pair in [Gelfand P236].

And if $\mathcal{F} = \omega_X$ and X oriented or char$k = 2$, we have $\mathrm{Ext}^{n-i}(k_X, k_X[n]) = H^{n-i}(X, k_X)$ using the adjointness of constant sheaf, so we get the Poincare duality:

$$H_c^i(X, k_X)^\vee \cong H^{n-i}(X, k_X).$$

⌟

Prop. (6.8.6.31). Compact cohomology commute with colimits, Cf.[Cohomology of Sheaves Iversen P173]. ⌟

7 Discriminant and Different

Trace Elements

Def. (6.8.7.1) [Traces]. Let $f : X \to Y$ be a finite locally free morphism, the **trace of** f is defined to be

$$\mathrm{tr}_f : f_*\mathcal{O}_X \to \mathcal{O}_Y.$$

Then $\mathrm{tr}_f \circ f^\# = [\deg(f)] : \mathcal{O}_Y \to \mathcal{O}_Y$. Let the **trace pairing** be

$$Q_f : f_*\mathcal{O}_X \otimes f_*\mathcal{O}_X \to \mathcal{O}_Y : (s, t) \mapsto \mathrm{tr}_f(st)$$

which is equivalent to a map $Q_f : f_*\mathcal{O}_X \to f_*\mathcal{O}_X^\vee$, so the determinant of which is

$$\det(Q_f) : \wedge(f_*\mathcal{O}_X) \to \wedge(f_*\mathcal{O}_X)^{-1},$$

a section of the line bundle $\wedge(f_*\mathcal{O}_X)^{-2}$. Then the **discriminant of** f is defined to be the closed subscheme D_f of Y cut out by this section $\det(Q_f)$. ⌟

Def. (6.8.7.2) [Trace Element of Rings]. Let $A \to B$ be a flat quasi-finite map of Noetherian rings, $[\omega_{B/A}]$ the dualizing module(5.9.8.4), then there exists a unique element $\tau_{A/B} \in \omega_{B/A}$ s.t. for any Noetherian A-algebra A_1 s.t. $B \otimes_A A_1 = C \times D$ with C finite over A_1, the image of $\tau_{B/A}$ in $[\omega_{C/A_1}]$ is $\mathrm{tr}_{C/A}$, called the **trace element**. ⌟

Def. (6.8.7.3) [Trace Element of Morphisms]. Let $f : X \to Y$ be a flat quasi-finite morphism of locally Noetherian schemes, then denote $\tau_{X/Y} \in \Gamma(X, [\omega_{X/Y}])$ the **trace element of** f affine locally given by the trace element $\tau_{B/A}$(6.8.7.2). ⌟

Prop. (6.8.7.4) [Discriminant and ÉtaleLocus]. If $f : X \to Y$ is finite locally free, then f is étaleiff $D_f = \varnothing$. ⌟

Proof: f is flat, so it suffices to check fiberwise. Then this follows from(5.4.7.21). □

Differents

Def. (6.8.7.5) [Kähler Different]. Let $f : X \to Y$ be a morphism of schemes locally of f.t., the **Kähler different** of f is the 0-th fitting ideal $\mathrm{Fit}_0(\Omega_{X/Y}) \in \mathfrak{QCoh}(X)$(6.5.1.21). ⌟

Prop. (6.8.7.6). Let $f : X \to Y$ be a morphism of schemes locally of f.t., then the closed subscheme cut out by the Kähler different is stable under base change. ⌟

Proof: Cf.[Sta]0BVX. □

Prop. (6.8.7.7). If $X = \mathrm{Spec}\, A[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$, then the Kähler different of $X \to \mathrm{Spec}\, A$ is just the ideal generated by the Jacobians $\det(\frac{\partial f_{i(j)}}{\partial X_j})_{0 \le j \le n}$. ⌟

Proof: Because $\Omega_{X/A}$ has a presentation

$$0 \to \bigoplus_{0 \le i \le m} f_i \xrightarrow{d} \bigoplus_{0 \le j \le n} dX_j \to \Omega_{X/A} \to 0.$$

□

Prop. (6.8.7.8) [Kähler Different and Unramified Locus]. Let $f : X \to Y$ be a morphism of schemes locally of f.t., then the closed subscheme cut out by the Kähler different contains exactly the points that f is not unramified. ⌟

Proof: Cf.[Sta]0C3J. □

Def. (6.8.7.9) [Differents]. Let $f : X \to Y$ be a flat quasi-finite morphism between locally Noetherian schemes, define the **different of** f to be the annihilator of $[\omega_{X/Y}]/\tau_{X/Y}$, which is a coherent ideal $\mathfrak{D}_f \subset \mathcal{O}_X$. ⌟

Prop. (6.8.7.10) [Differents and Étale(Unramified) Locus]. Let $f : X \to Y$ be a flat quasi-finite morphism between locally Noetherian schemes, then the closed subscheme of X cut out by the different $\mathfrak{D}_f$ contains exactly the set of points that f is not étale(unramified). ⌟

Proof: Cf.[Sta]0BW9. □

Prop. (6.8.7.11). If $f : X \to Y$ is a quasi-finite syntomic morphism between locally Noetherian schemes, then the different $\mathfrak{D}_f$ equals the Kähler different of f(6.8.7.5). ⌟

Proof: Cf.[Sta]0BWG. □

Prop. (6.8.7.12) [Differents for Smooth Schemes]. Let S be a locally Noetherian scheme and X, Y be smooth scheme of relative dimension n over S, and $f : X \to Y$ is a quasi-finite morphism, then f is syntomic, and the closed subscheme R cut out by the different $\mathfrak{D}_f$ of f is the locally principal vanishing locus of

$$\wedge^n(df^*) \in \mathrm{Hom}(f^*\Omega^n_{Y/S}, \Omega^n_{X/S}) = \Gamma(Y, (f^*\Omega^n_{Y/S})^{-1} \otimes \Omega^n_{X/S}).$$

And if f is étaleat the associated points of X, then R is an effective Cartier divisor, and

$$f^*\Omega^n_{Y/S} \otimes \mathcal{O}(R) \cong \Omega^n_{X/S}.$$

⌟

Proof: Cf.[Sta]0BWJ. □

8 Fourier-Mukai Transform

Cf.[Sta]Chap56.

9 Deformation Theory

Basic references are [Sta]Chap36.

Def. (6.8.9.1) [Thickenings]. For $X, X' \in \mathcal{S}\mathrm{ch}$, X' a called a **thickening** of X iff X is a closed subscheme of X' that their underlying topological space are the same. Morphisms of thickenings are defined routinely.

A thickening is said to **have order** n iff the ideal sheaf $\mathcal{I}$ satisfies $\mathcal{I}^{n+1} = 0$.

Base change and composition of a (order n)thickening is also a (order n)thickening, because closed immersion and surjective do. ⌟

Prop. (6.8.9.2). Any thickening of an affine scheme is also affine. ⌟

Proof: This is a special case of(6.4.4.36). □

Prop. (6.8.9.3) [Picard Group of Thickenings]. Let $X \subset X'$ be a first order thickening with ideal sheaf $\mathcal{I}$, then there is a canonical long exact sequence of Abelian groups:

$$0 \to H^0(X, \mathcal{I}) \to H^0(X', \mathcal{O}^*_{X'}) \to H^0(X, \mathcal{O}^*_X) \to H^1(X, \mathcal{I}) \to \mathrm{Pic}(X') \to \mathrm{Pic}(X) \to H^2(X, \mathcal{I}) \to \ldots$$

⌟

Proof: This follows from taking cohomology of the exact sequence $0 \to \mathcal{I} \to \mathcal{O}_{X'} \to i_*\mathcal{O}_X \to 0$, where $\mathcal{I} \to \mathcal{O}_{X'}$ is given by $a \mapsto 1 + a$. □

Prop. (6.8.9.4). Let $X \subset X'$ be a thickening with ideal sheaf $\mathcal{I}$ and n is invertible in $\mathcal{O}_X$, then $\mathrm{Pic}(X)[n] \to \mathrm{Pic}(X')[n]$ is an isomorphism. ⌟

Proof: By taking cohomology of the exact sequence $0 \to (1 + \mathcal{I})^* \to \mathcal{O}_{X'} \to i_*\mathcal{O}_X \to 0$, it suffices to show that $n : (1 + \mathcal{I})^* \to (1 + \mathcal{I})^*$ is an isomorphism, which is true by(5.1.1.18). □

Def. (6.8.9.5) [Infinitesimal Neighbourhood]. Let $Z \subset U \subset X$ be a closed immersion of the open subscheme U that Z corresponds to the ideal $\mathcal{I}$ on U, then a **n-th infinitesimal neighbourhood** of Z in X is the closed subscheme of U corresponding to $\mathcal{I}^n$.

The infinitesimal neighbourhood of Z in X has the universal property s.t. for any infinitesimal thickening $T \subset T'$ of order n over X and a map $T \to Z \in \mathcal{S}\mathrm{ch}_X$ extension to a morphism of infinitesimal thickenings $(T \subset T') \to (Z \to Z')$ over X. ⌟

Def. (6.8.9.6) [Infinitesimal Extension]. Let X be a scheme algebraic over a field k and $\mathcal{F}$ is a coherent sheaf on X, then a **infinitesimal extension** of X by the sheaf $\mathcal{F}$ is a scheme X' over k that has a sheaf of ideals $\mathcal{I}$ that $\mathcal{I}^2 = 0$ and $(X', \mathcal{O}_{X'}/\mathcal{I}) \cong (X, \mathcal{O}_X)$, and moreover, $\mathcal{I}$ with the $\mathcal{O}_X$-structure is isomorphic to $\mathcal{F}$.

There is a trivial extension, that is $(X', \mathcal{O}_{X'}) \cong (X, \mathcal{O}_X \oplus \mathcal{F})$, where the multiplication is $(a, f)(a', f') = (aa', af' + a'f)$. ⌟

Def. (6.8.9.7) [Deformation]. Let X be a scheme algebraic over a field k, an **infinitesimal deformation** of X is a scheme X' flat over $D = k[t]/(t^2)$ that $X' \otimes_D k = X$. A infinitesimal deformation is a first order thickening, by(6.8.9.1).

If Y is a closed subscheme of X, then we define the **infinitesimal deformation of Y in X** to be a closed subscheme $Y' \subset X \otimes_k D$ which is flat over D and $Y' \otimes_D k = Y$.

A scheme algebraic over a field k is called **rigid** if it has no infinitesimal deformations. ⌟

Prop. (6.8.9.8) [Affine Case]. Any thickening of an affine scheme is affine. (Immediate from(6.4.4.36)). ⌟

Prop. (6.8.9.9). Let X be a nonsingular variety over an alg.closed field k, infinitesimal deformation of X is the same as an infinitesimal extension of X by the sheaf $\mathcal{O}_X$. Thus we get the set of infinitesimal deformations of X is parametrized by $H^1(X, \mathcal{T}_X)$, by(6.8.9.11)below. ⌟

Proof: For an infinitesimal deformation, tensoring $\mathcal{O}_{X'}$ with the exact sequence $0 \to k \xrightarrow{t} D \to k \to 0$, we get(by flatness)

$$0 \to \mathcal{O}_X \xrightarrow{t} \mathcal{O}_{X'} \to \mathcal{O}_X \to 0,$$

, and conversely, an extension is locally free(because it is f.g. so flat over D is equivalent to free). □

Prop. (6.8.9.10). If X is an affine regular scheme algebraic over an alg.closed field k, then any extension by coherent sheave is trivial. ⌟

Proof: For any infinitesimal extension, the morphism $X \to X'$ is a closed immersion and surjection, so X' is also affine by(6.8.9.8), $= \operatorname{Spec} A'$. Now the rest follows from**??**. □

Cor. (6.8.9.11) [Infinitesimal Extension and Cohomology]. Let X be a nonsingular variety over an alg.closed field k, then the set of infinitesimal extensions by a coherent sheaf $\mathcal{F}$ is parametrized by $H^1(X, \mathcal{F} \otimes \mathcal{T}_X)$.

If Y is a closed subscheme of X, then the set of infinitesimal deformation of Y in X is parametrized by $H^0(Y, \mathcal{N}_{Y/X})$. ⌟

Proof: By the proposition, we know that an infinitesimal extension s locally isomorphic to $(U, \mathcal{O}_X(U) \otimes \mathcal{F}(U))$, by a section $\mathcal{F}(U) \to \mathcal{O}_{X'}(U)$.

But there is a twist, because there can because different sections. But the different sections different at a $\mathrm{Hom}_{\mathcal{O}_X(U)}(\Omega_{\mathcal{O}_X(U)/k}, \mathcal{F}(U)) = (\mathcal{T} \otimes \mathcal{F})(U)$. These forms a Čech cocycle for $\mathcal{F} \otimes \mathcal{T}_X$, and the converse is also true. Finally, use the fact that X is separated so Čech and sheaf cohomology coincide.

For the subscheme,**?** □

Formal Properties

Def. (6.8.9.12) [Formal Properties]. Let $f : X \to S$ be a morphism of schemes, then f is called a **formally unramified/smooth/étale** if for any first order thickening of affine schemes $T \to T'$ and a morphism $(T \to T') \to (X \to S)$, there exists at most one/exists one/exists exactly one lifting $T' \to X$.

Formally unramified/smooth/etale morphisms are stable under base change and compositions. ⌟

Prop. (6.8.9.13).

- A morphism is (G-)unramified iff it is formally unramified and locally of f.t.(f.p.).
- A morphism is étaleiff it is formally étaleand locally of f.p.
- A morphism is smooth it is formally smooth and locally of f.p.

⌟

Proof: [Sta] □

6.9 Logarithmic Geometry

Main references are [DLLZ19], [LOG p-DIVISIBLE GROUPS], [Kato],

6.10 Resolution of Singularities

References are[K-M85].

Def. (6.10.0.1) [Desingularizations]. Let $X \in \mathcal{S}\mathrm{ch}$ be reduced and locally Noetherian, then a **desingularization** of X is a modification(6.4.5.10) $Z \to X$ s.t. Z is regular. A **strong desingularization** is a desingularization $\pi : Z \to X$ that π is an isomorphism over any regular point $x \in X$. ⌟

Thm. (6.10.0.2) [Hironaka]. Let X be a reduced scheme locally of f.t. over an excellent, reduced, locally Noetherian scheme S of characteristic 0(i.e. $\mathrm{char}\,\kappa(x) = 0$ for any $x \in X$), then X admits a strong desingularization over S. ⌟

Proof: [Hironaka, Resolution of singularities of an algebraic variety over a field of characteristic zero. I, II, Ann. Math. 79 (1964), 109 – 203; 205 – 326.] or [Resolution of Singularities, Hauser, Lipman, Oort, Quiros]. □

Thm. (6.10.0.3) [de Jong]. Let R be a CDVR or a field, $X \in \mathcal{S}\mathrm{ch}^{\mathrm{ft,sep}}_{\mathrm{int}}/R$, then X admits an alteration(6.4.5.10) $Y \to X$ over R s.t. Y is regular. ⌟

Proof: [de Jong, Smoothness, Semi-stability and Alterations, Publ. Math. IHES 83 (1996), 51–93.] □

6.11 Varieties

References are [Sta]and [Har77].

The materials distinguishes here in the fact that most schemes considered have geo.reduced, geo.connected or geo.integral properties in nature.

1 Varieties

Classical varieties

Prop. (6.11.1.1) [Soberization Functor]. For a sep.closed field k, the soberization functor t induce a fully faithful functor from classical varieties over k to quasi-projective integral schemes over k. It maps projective varieties to projective integral schemes and preserves fiber products **?**. ⌟

Proof: We assign the irreducible closed subsets space $t(X)$ and show that this embeds X in $t(X)$, and for an affine variety $(V, \mathcal{O}_V)$, the regular function sheaf is isomorphic to the pullback sheaf on $t(V) = \mathrm{Spec}(A)$.

By definition $t(X)$ is quasi-projective, which is separated, the set of geometric pts of any closed variety is dense so $t(V)$ is homeomorphic to X. And because they are both reduced, they are isomorphic. So it is essentially surjective.

It is fully faithful by(6.11.1.11). □

Prop. (6.11.1.2). The soberization of a classical variety X is regular at a closed point iff the local defining functions has rank $n - \dim X$. ⌟

Proof: Consider the space of closed point of X, they correspond to classical points because k is alg.closed. Let $a_p = (x_1 - a_1, \ldots, x_n - a_n)$ and b be the locally defining ideal. Then the differential defines an isomorphism of vector space $a_p/a_p^2 \cong k^n$, and the local ring at p is $m/m^2 \cong (a_p/b)/(a_p/b)^2 \cong a_p/(b + a_p^2)$. The rank of the defining functions is $b + a_p^2/a_p^2$. Counting dimension gives us the result. (Use (6.6.3.3) also). □

Varieties

Def. (6.11.1.3) [Varieties]. Given $k \in \mathtt{Field}$,

- A **variety** over k is a geo.integral separated scheme algebraic over k.
- An **prevariety** over k is an integral separated scheme algebraic over k.
- A **complete variety** over k is a variety over k that is also proper(i.e. universally closed) over k.
- A classical variety over k is an abstract variety over k because quasi-projective is f.t. and separated(6.4.5.19).
- A **non-singular variety** over k is a regular variety over k.
- A **curve** over k is a variety of dimension 1 over k.

The category of varieties over k is denoted by $\mathcal{V}\mathrm{ar}_k$.

If X/k is a (complete)variety and K/k is a field extension, then X_K is a (complete)variety over K, by(6.4.3.17). ⌟

Remark (6.11.1.4). Notice the prevariety is the same as the variety defined in [Sta]. ⌟

Cor. (6.11.1.5). Any variety is birational to an integral H-quasi-projective scheme. A complete variety is birational to an integral projective scheme by Chow's lemma(6.4.5.23)(6.4.5.3). ⌟

Prop. (6.11.1.6). By valuation criterion, for a complete variety, every valuation of the function fields of K/k dominate a unique point of X. So the points of X correspond to valuations of K containing k ⌟

Prop. (6.11.1.7) [Generically Smoothness]. A variety is generically smooth, by(6.6.4.21). ⌟

Prop. (6.11.1.8) [Nagata]. By Nagata compactification(6.8.3.2), any variety can be embedded as an open subset of a complete variety. ⌟

Proof: □

Prop. (6.11.1.9) [Product of Varieties]. The product of two (complete)varieties over k is also a (complete)variety. ⌟

Proof: It is geometrically integral by(6.4.3.17), it is separated because separatedness is stable under composition and base change(6.4.4.2). So does properness. □

Def. (6.11.1.10) [Arithmetic Points]. An **arithmetic point** of a scheme X over a field k is an element of $X(k^s)$. When X is a variety, the arithmetic points of X is dense in X, by(6.4.3.3).

An **geometric point** of a scheme X is an element of $X(\overline{k})$. ⌟

Prop. (6.11.1.11). To verify two morphisms f, g between two varieties X and Y are equal, it suffices to prove that they are equal on the set of arithmetic points of an open subscheme U(6.11.1.10). ⌟

Proof: Because the equalizer is a closed subscheme of X(6.2.7.18), and it contains all geometric pts of an open subset of X, so it must by X, as the geometric-points are dense in U(6.11.1.10), and X is reduced and irreducible. □

Prop. (6.11.1.12) [Global Sections]. Let $k \in \texttt{Field}$ and $X \in \mathcal{S}\mathrm{ch}^{proper}/k$, then

- $A = \Gamma(X, \mathcal{O}_X)$ is a finite k-algebra hence is a finite product of Artinian local k-algebras, one for each connected component of X.
- If X is reduced, then $A = \prod k_i$ is a finite product of finite field extensions of k.
- If X is geo.reduced, then k_i are all separable over k.
- If X is geo.connected, then A is geo.irreducible over k(5.3.6.1).
- If X is geo.integral(i.e. a complete variety), then $\Gamma(X, \mathcal{O}_X) = k$.

⌟

Proof: 1: $H^0(X, \mathcal{O}_X)$ is finite k-algebra by(6.7.4.11), thus it is Artinian(5.1.3.4). The connected components of X clearly corresponds to idempotents of A, which corresponds to Artinian local k-algebras, as a local ring is connected.

2: This follows from(5.1.3.5).

3: $A \otimes_k \overline{k} = H^0(X_{\overline{k}}, \mathcal{O}_{X_{\overline{k}}})$ is also reduced by flat base change(6.7.5.1), so each k'/k is geo.reduced(5.3.6.2), thus separable by(5.3.9.4).

4: By hypothesis $A \otimes_k \overline{k} = H^0(X_{\overline{k}}, \mathcal{O}_{X_{\overline{k}}})$ is an Artinian local ring, thus it has only one point, so irreducible, so it is geo.irreducible(5.3.6.3).

5: By item3, 4, $A = k'$ is a finite separable field extension of k that $\mathrm{Spec}(k' \otimes_k \overline{k})$ is irreducible, but $k' \otimes_k \overline{k}$ is a finite product of $\overline{k}$, thus $k' = k$. □

Prop. (6.11.1.13)[Check Properties on Geometric/Closed Points]. A nice property of varieties is that identity of two morphisms of products of varieties can be checked at the geometric pts(6.11.1.10), by(6.11.1.11) and(6.11.1.9).

Surjectiveness of a map between varieties can be checked on closed points, by(6.4.1.29).

Also surjective and injective of Qco sheaves need only be checked at closed pts by(6.5.1.38)(6.4.1.26). ⌟

Canonical Sheaves

Prop. (6.11.1.14)[Canonical Sheaves]. For a smooth variety X over a field k and Y a local complete intersection of X of codimension r, by(6.6.4.2) and(6.6.4.16) and(6.6.8.10), $\mathcal{K}_{X/k}$ and $\mathcal{I}/\mathcal{I}^2$ is locally free, so we can define the following locally free sheaves:

- The **canonical sheaf** $\mathcal{K}_{X/k}=\wedge^n\Omega_{X/k}$ on X.
- The **tangent sheaf** $\mathcal{T}_X=(\mathcal{K}_{X/k})^{-1}$ on X.
- The conormal sheaf $\mathcal{C}_{Y/X}=\mathcal{I}/\mathcal{I}^2$ on Y.
- The normal sheaf $\mathcal{N}_{Y/X}=\mathcal{C}_{Y/X}^{-1}$ on Y.

⌟

Prop. (6.11.1.15)[Kodaira-Spencer map]. There is another characterization of tangent vector fields. (Note: this should be a special case of Prop8.5.9 in [FGA]).

Let X be a variety over k and $S=k[\varepsilon]$ the dual numbers. Then $H^0(X,\mathcal{T}_X)\cong \mathrm{Aut}^{(1)}(X_S/S)$, where $\mathrm{Aut}^{(1)}(X_S/S)$ means that the automorphisms of X_S over S that is identity on X(inclusion to X_S induced by $\mathrm{Spec}\, k\subset \mathrm{Spec}\, S$). ⌟

Proof: First the case $X=\mathrm{Spec}\, A$ is affine, then because $H^0(X,\mathcal{T}_X)=\mathrm{Hom}_k(\mathcal{K}_{A/k},A)=\mathrm{Der}(A,A)$, so this is equivalent to $\mathrm{Der}(A,A)\cong$ automorphisms of $A[\varepsilon]$ that is identity under pass to quotients to A. For this, a $d\in \mathrm{Der}(A,A)$ is mapped to $a+b\varepsilon\mapsto a+b\varepsilon+d(a)\varepsilon$. This is checked to be a ring morphism, and any desired morphism are like these.

The above construction is natural and functorial in A, so it glue together to give the global case. □

Prop. (6.11.1.16)[Smoothness and Conormal Sheaves]. ? Let X be a smooth variety over a field k, then an irreducible closed subscheme Y of codimension r in X is smooth iff $\mathcal{K}_{Y/k}$ is locally free and(6.5.5.13) is exact on the left.

In this case, $\mathcal{I}$ is locally generated by r elements and $\mathcal{C}_{Y/X}$ is a locally free sheaf of rank r on Y by(6.6.8.10). ⌟

Proof: Cf.[Hartshorne P178]. Should has something to do with(6.6.4.2),(6.6.4.16) and(6.6.4.15). □

Prop. (6.11.1.17) [Adjunction Formulas]. For a smooth variety X over a field k and Y a smooth subvariety of codimension r. There is an exact sequence

$$0\to \mathcal{I}/\mathcal{I}^2\to \mathcal{K}_{X/k}\otimes \mathcal{O}_Y\to \mathcal{K}_{Y/k}\to 0$$

by(6.5.5.14). Taking the highest exterior power(6.5.1.25), we get:

$$\mathcal{K}_Y=\mathcal{K}_X\otimes\wedge^r\mathcal{N}_{Y/X}=\mathcal{K}_X\otimes(\wedge\mathcal{I}/\mathcal{I}^2)^{-1}$$

In particular, if $r=1$ then Y is a divisor D in X, the canonical sheaf

$$\mathcal{K}_Y \cong (\mathcal{K}_X \otimes \mathcal{L}(D))_Y, \quad \mathcal{K}_{\mathbb{P}^n_k/k} = \mathcal{O}(-n-1)(6.5.5.7).$$

because $\mathcal{I}_Y \cong \mathcal{L}(-Y)$ in this case so $\mathcal{I}_Y/\mathcal{I}_Y^2 = L(-Y)\otimes\mathcal{O}_Y$.

Taking dual, we get:

$$0 \to \mathcal{T}_Y \to \mathcal{T}_X \otimes \mathcal{O}_Y \to \mathcal{N}_{Y/X} \to 0$$

⌟

Prop. (6.11.1.18) [Geometric Genus]. For a smooth proper variety over a field k, the **geometric genus** p_g is defined as the rank of the global section of the invertible canonical sheaf $\mathcal{K}_X = \wedge^n \mathcal{K}_{X/k}$. It is a birational invariance. With the same methods, we can prove the rank of global sections of any other functorially defined bundles of $\mathcal{K}_X$ is birational invariance, e.g. Hodge numbers. ⌟

Proof: For any rational map $U \to Y$, there is a subset $V \in U$ and a local isomorphism V and $f(V)$, that will define an isomorphism of global sections. Because a nonzero section of an invertible sheaf cannot vanish on a dense open set $f(V)$, the morphism of global sections is injective into $\Gamma(U, \mathcal{O}_U)$. Now we find a U that $\operatorname{codim}(X-U) > 1$, then we can use(5.3.5.11) to get $\Gamma(U) = \Gamma(X)$, then $p_g(X) \geq p_g(X')$, and the converse is also true. For this, we use valuation criterion of properness, then for any codimension 1 point, the stalk is a DVR, thus we find a $\operatorname{Spec}\mathcal{O}_p \to X'$, this extends to a nbhd of p because X' is of f.t.. □

Cor. (6.11.1.19). By(6.5.5.7), $\mathcal{K}_{\mathbf{P}^n_k} \cong \mathcal{O}(-n-1)$, so it has no global section by(6.7.2.1), $p_g(\mathbb{P}^n_k) = 0$. Hence every rational variety over a field k, i.e. one that is birational to $\mathbb{P}^n_k$, has geometric genus 0. ⌟

<u>**Complete Varities**</u>

Lemma (6.11.1.20)[Rigidity Lemma]. Let $k \in \mathtt{Field}$, $X, Y \in \mathcal{V}\mathrm{ar}/k$, $Z \in \mathcal{S}\mathrm{ch}^{\mathrm{sep}}/k$ and $f : X\times Y \to Z \in \mathcal{S}\mathrm{ch}/k$. If X is complete and $p \in X(k), y \in Y(k)$ s.t. $f(\cdot, y) : X \to Z$ is constant, then f factors through the projection $\mathrm{pr}_Y : X \times Y \to Y$. ⌟

Proof: The equalizer is a closed subscheme of $X \times Y$ as Z is separated(6.4.4.89), and $X \times Y$ is a variety(6.11.1.9), thus we can check on closed points. Let $g(y) = f(p, y) : Y \to Z$, then we want to show $f = g \circ \mathrm{pr}_Y$.

Let U be affine open in Z, then because X is universally closed, pr_Y is closed, so $V = \mathrm{pr}_Y(f^{-1}(Z\backslash U))$ is closed in Y. But if $y \notin V(\overline{k})$, then $f(X, y) \subset U$, and X is complete and connected, so $f(\cdot, y)$ is constant(6.4.5.4), and $f(x, y) = f(p, y)$. Thus $f = g \circ \mathrm{pr}_Y$ on a non-empty open subset of $X \times Y$, which is a variety, so this is true on all of $X \times Y$ by(6.11.1.11). □

Prop. (6.11.1.21)[See-Saw Principle]. Let X be a complete variety over a field k and Y a k-scheme, then for any line bundle $\mathcal{L}$ on $X \times Y$, there is a closed subscheme $Y_1 \subset Y$ s.t. for any morphism $f : S \to Y$, $(1\times f)^*\mathcal{L}$ is trivial on $X \times S$ iff f factors through Y_1. ⌟

Proof: This $\mathcal{L}$ corresponds to a morphism $Y \to \underline{\mathrm{Pic}}_{X/k}$, and clearly Y_1 is the fiber of Y over $e \in \underline{\mathrm{Pic}}_{X/k}$. □

Cor. (6.11.1.22). Let X be a complete variety over a field k and Y a reduced locally algebraic k-scheme, if $\mathcal{L}, \mathcal{M}$ are two line bundles on $X \times Y$ s.t. $\mathcal{L}_y \cong \mathcal{M}_y$ for all closed points $y \in Y$, and for some $x \in X(k)$, $\mathcal{L}_x \cong \mathcal{M}_x$, then $\mathcal{L} \cong \mathcal{M}$. ⌟

Prop. (6.11.1.23) [Theorem of the Cube]. If X, Y are complete varieties over a field k, and Z is a connected, locally Noetherian k-scheme, if x, y are rational points of X, Y resp. and $z \in Z$. Supposed $\mathcal{L} \in \mathrm{Pic}(X \times Y \times Z)$ that is trivial on $x \times Y \times Z, X \times y \times Z, X \times Y \times z$, then $\mathcal{L}$ is trivial. ⌟

Proof: Let Z' be the maximal closed subscheme of Z given by(6.11.1.21). We show that Z' is open, thus it is all of Z: If $\zeta \in Z'$, let $I \subset \mathcal{O}_{Z,\zeta}$ be the ideal defining Z', we show $I = (0)$, which is equivalent to Z' containing a nbhd of ζ(locally Noetherian used). If not, then because $\cap \mathfrak{m}^n = 0$ by Krull's theorem(locally Noetherian used), there is an $n \geq 1$ that $I \subset \mathfrak{m}^n, I \not\subseteq \mathfrak{m}^{n+1}$. Let $\mathfrak{a}_1 = (I, \mathfrak{m}^{n+1})$, and $\mathfrak{m}^{n+1} \subset \mathfrak{a}_2 \subset \mathfrak{a}_1$ that $\dim_{k(\zeta)}(\mathfrak{a}_1/\mathfrak{a}_2) = 1$(so $\mathfrak{a}_1 = \mathfrak{a}_2 + k(\xi)a$ for some $a \in \mathfrak{a}_2$), and let $Z_i \subset \mathrm{Spec}\,\mathcal{O}_{Z,\xi}$ be the closed subscheme defined by a_i. Let $\mathcal{L}_i$ be the restriction of L on $X \times Y \times Z_2$. If we show that $\mathcal{L}_2$ is trivial, then Z_2 is contained in Z', which is contradiction because $I \not\subseteq \mathfrak{a}_2$.

For this, notice that $\mathcal{L}_1$ is trivial, and to show that $\mathcal{L}_2$ is trivial, it suffices to lift a non-vanishing global section s of $\mathcal{L}_1$ to $\mathcal{L}_2$, because Z_1, Z_2 has the same underlying set.

For this, notice there is an exact sequence $0 \to k(\xi) \xrightarrow{a} \mathcal{O}_{Z_2} \to \mathcal{O}_{Z_1} \to 0$, where $k(\xi)$ is the skyscraper sheaf at ξ. So the obstruction of the lifting is an element $\xi \in H^1((X \times Y)_{k(\xi)}, \mathcal{O}_{(X\times Y)_{k(\xi)}})$. But now the conditions show that ξ is zero under the pullback along $x \times Y \hookrightarrow X \times Y$ and $X \times y \hookrightarrow X \times Y$. So by Kunneth formula(6.7.1.10) and(6.11.1.12), ξ vanishes. □

2 Projective Varieties

Example (6.11.2.1) [Non-Projective Smooth Proper Varieties]. There are proper smooth complex varieties that are not projective. Examples are given in [Har77]P443**?**. ⌟

Prop. (6.11.2.2)[Affine Dimension Theorem]. Suppose X, Y are subschemes of $\mathbb{A}^n_k$ of codimensions d and e resp., and $d + e \leq n$, then every non-empty irreducible component of $X \cap Y$ has dimension $\geq n - d - e$. ⌟

Proof: If Y is an intersection of e hypersurfaces, then this follows from Krull's height theorem(5.2.4.18). In general, notice the diagonal map $\Delta : \mathbb{A}^n_k \to \mathbb{A}^n_k \times \mathbb{A}^n_k$ is an isomorphism onto the diagonal T defined by $\{X_i = Y_i\}_{i=1,\ldots,n}$, thus it is a complete intersection in $\mathbb{A}^n_k \to \mathbb{A}^n_k \times \mathbb{A}^n_k$, and Δ induces an isomorphism $X \cap Y \cong X \times Y \cap T$, so we are done. □

Cor. (6.11.2.3) [Projective Dimension Theorem]. Suppose X, Y are subvarieties of $\mathbb{P}^n_k$ of codimensions d and e resp., and $d + e \leq n$, then X and Y intersect. ⌟

Proof: Take the affine cone, then item2 shows any irreducible component of $\overline{X} \cap \overline{Y}$ containing the origin has dimension≥ 1, which means $X \cap Y \neq 0$. □

Prop. (6.11.2.4)[Transversal Intersection]. Show that if X is a closed subscheme of $\mathbb{P}^n_k$ of dimension r, then there is an intersection of $r + 1$ non-empty hypersurfaces missing X. And if k is infinite, these hypersurfaces can be chosen to be hyperplanes.

If k is infinite, there is an intersection of r non-empty hypersurfaces intersecting X at f.m. points. ⌟

Proof: Let $\eta_1, \ldots, \eta_n$ be the generic points of X, we want to find a hypersurface F that doesn't contain any of these generic points. We use induction on n. If $n = 1$, then there is clearly a hyperplane missing η_1. If we find a hypersurface missing $\eta_1, \ldots, \eta_{n-1}$, if it also misses η_n, we are done, if it contains η_n, we can change η_n to η_i and consider again. If we find polynomials $F_1, \ldots, F_n$

that $F_i(\eta_i)=0, F_i(\eta_j)\neq 0$, we may assume $\deg(F_i)$ are the same, so $\sum_i F_1\ldots\widehat{F_i}\ldots F_n$ is a polynomial non-zero on each of η_i. If moreover k is infinite, then we want to find a hyperplane missing every generic point of X. But each generic point corresponds to a graded ideal I_i of $k[T_0,\ldots,T_n]$, and $(I_i)_1\neq k\{T_0,\ldots,T_n\}$ are proper linear subspaces. As k is infinite, we can choose a $a_0T_0+\ldots+a_nT_n$ not in these subspaces, thus non-zero on any generaic point of X.

Now $X\cap F$ is a closed subscheme of $\mathbb{P}^n_k$ of dimension $r-1$, thus we can use conduction on r to finish. □

3 Birational Geometry

Prop. (6.11.3.1). Any variety over K is birational to a hypersurface in $\mathbb{A}^n_K$ for some n. ⌟

Proof: Cf.[Diophantine Geometry, P575]. □

Prop. (6.11.3.2) [Prevarieties and Function Fields]. The following categories are equivalent.

- The category of prevarieties over k with dominant rational morphisms.
- The dual category of f.g. field extensions over k.

⌟

Proof: Cf.[Sta]0BXN.? □

Prop. (6.11.3.3). Let $\varphi: X\to X'$ be a rational map of K-varieties with X smooth. If the base change $\varphi_{\overline{K}}$ extends to a morphism $X_{\overline{K}}\to X'_{\overline{K}}$, then φ extends to a morphism $X\to X'$. ⌟

Proof: Let U be an open dense subset that φ is defined. For a point x, let $x'=\varphi_{\overline{K}}(x)$, then x' is in the closure of $\varphi(U)$. By(6.4.6.2), it suffices to construct a morphism $\mathcal{O}_{X',x'}\to\mathcal{O}_{X,x}$, i.e., to prove for any rational function f regular at x', $\varphi\circ f$ is regular at x. The argument is the same as that of(6.4.5.14).

For any such f, $f_{\overline{K}}\circ\varphi_{\overline{K}}$ is regular at x, thus no pole of $\mathrm{div}(f_{\overline{K}}\circ\varphi_{\overline{K}})$ passes through x. For the rest, Cf.[Diophantine Geometry, P576].? □

Prop. (6.11.3.4) [Generic Separable Degree]. Let $\varphi: X\to X'$ be a dominant morphism of varieties over a field k of the same dimension, then there exists an open dense subscheme U' of X' s.t. $\varphi^{-1}(U')\to U'$ is finite and the fibers all have cardinality $\deg_s(\varphi)$. ⌟

Proof: By(6.11.3.2), we can decompose φ and assume it is either separable or purely inseparable, and also primitive. If it is separable, let it be generated by t. After shrinking(and cutting closure of images), we may assume the coefficients of t are regular functions, and $\Gamma(X)=\Gamma(X')[t]/(q(t))$. As q is separable, there exists $a,b\in K(X')$ s.t. $aq+bq'=1$. We may shrink X' and assume $a,b\in\Gamma(X')$, so q is also separable over any fiber of X, which means the fibers all have cardinality $\deg_s(\varphi)$.

If it is purely inseparable, let $q(t)=t^{p^k}-h$ be the minimal polynomial of t over $K(X')$, h$\in K(X')$. Then after shrinking, we may assume $h\in\Gamma(X')$, thus $q(t)$ is purely inseparable over any fiber of X, which means □

Def. (6.11.3.5) [Kodaira Dimensions]. For $k\in\texttt{Field}$ and $X\in\mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}^n/k$, the **Kodaira dimension** $\mathrm{Kod}(X)$ of X is defined to be $-\infty$ if $h^0(X,\mathcal{K}_X^d)=0$ for d large, or

$$\mathrm{Kod}(X)=\sup\{k\in\mathbb{R}_+|h^0(X,\mathcal{K}_X^d)/d^k\text{ is bounded}\}.$$

Then $\mathrm{Kod}(X)\in\{-\infty\}\cup(\mathbb{Z}\cap[0,n])$. ⌟

4 Others

Prop. (6.11.4.1). Varieties are triangulable. ⌟

Proof: Cf.[Triangulation of Algebraic Sets, Hironaka]. □

Fano Varieties

Def. (6.11.4.2) [Fano Varieties]. A **Fano variety** is a complete smooth variety X over a field K s.t. $\mathcal{K}_X^*$ is ample. ⌟

Prop. (6.11.4.3). a smooth complete intersection of hypersurfaces in $\mathbb{P}_K^n$ is Fano if and only if the sum of their degrees is at most n. ⌟

Prop. (6.11.4.4) [Kollár-Miyaoka-Mori]. Fano varieties over an alg.closed field are rationally chain connected. ⌟

Proof: Cf.[Rational connectedness and boundedness of Fano manifolds, Kollar]. □

Rationally Connected Varieties

Def. (6.11.4.5) [Rationally Connected Varieties]. A variety X over K is called **rationally connected** if any two points of $X(\overline{K})$ can be connected by a rational curve(6.12.1.1) over $\overline{K}$. ⌟

5 Relative Varieties

Def. (6.11.5.1) [Varieties over Schemes]. Let $S \in \mathcal{S}\mathrm{ch}$, a (proper/smooth)**variety over** S is a (proper/smooth) flat morphism $f : X \to S$ s.t. all the geometric fibers of f are geo.integral over the resp. residue field $k(s)$. It can be regarded as a family of (proper/smooth)varieties parametrized by S. the category of varieties over S is denoted by $\mathcal{V}\mathrm{ar}/S$.

Being a (proper/smooth) variety is stable under base change. ⌟

Prop. (6.11.5.2) [Global Sections]. Let $S \in \mathcal{S}\mathrm{ch}$ be locally Noetherian and X a proper variety over S, then $\mathcal{O}_S \to f_*\mathcal{O}_X$ is an isomorphism. ⌟

Proof: For any closed point $s \in S$, $k(s) \to H^0(X_s, \mathcal{O}_{X_s})$ is an isomorphism by(6.11.1.12), and this isomorphism factors through $k(s) \to f_*(\mathcal{O}_X) \otimes k(s) \to H^0(X_s, \mathcal{O}_{X_s})$. So $f_*(\mathcal{O}_X) \otimes k(s) \to H^0(X_s, \mathcal{O}_{X_s})$ is surjective, thus it is an isomorphism by item4 $\to$ 3 of (9.7.2.16). Thus the first map is also an isomorphism.

Now $\mathcal{O}_S \to f_*(\mathcal{O}_X)$ is a surjection at s by Nakayama. Let $\mathcal{Q}$ be the coherent sheaf on S associated to $\mathcal{F}$, then by(9.7.2.16), it is free at s, and $\mathcal{Q}_s = H^0(X_s, \mathcal{O}_{X_s})$ is of rank 1, but also $\mathcal{Q}^\vee \cong f_*(\mathcal{O}_X)$, so $\mathcal{O}_S \to f_*(\mathcal{O}_X)$ is in fact a surjection at s. Now s is arbitrary, so $\mathcal{O}_S \to f_*(\mathcal{O}_X)$ is an isomorphism. □

Prop. (6.11.5.3). Let $(\mathcal{O}_K, K, k)$ be a DVR and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{sm}}/R$ s.t. X_K is geo.integral and X_k is proper, then $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}\mathcal{V}\mathrm{ar}/\mathcal{O}_K$. ⌟

Proof: Cf.[Good Reduction of Abelian Varieties, P495]**?** □

6.12 Curves

Main references are [黎曼曲面, 伍鸿熙], [Vak17]Chap19, [?], [Har77]Chap4 and [Sta]Chap53. In this section, properties to morphisms of relative dimension≤ 1 are studied.

Notation (6.12.0.1).

- Use notations defined in Cohomology of Schemes.
- Use notations defined in Varieties.

⌟

1 Basics

Def. (6.12.1.1) [Rational Curve]. A **rational curve** over a field k is a curve that is birational to $\mathbb{P}^1_k$. ⌟

Lemma (6.12.1.2). If X is an integral separated scheme and $U\subset X$ is an non-empty affine open that $X\backslash U$ is a finite set of points with $\mathcal{O}_{X,x_i}$ Noetherian of dimension 1, then there exists a base-point free invertible sheaf $\mathcal{L}\in\mathrm{Pic}(X)$ and a section s s.t. $U=X_s$. ⌟

Proof: Cf.[Sta]09NB. □

Prop. (6.12.1.3). A Noetherian separated scheme of dimension≤ 1 has an ample invertible sheaf. ⌟

Proof: First reduce to the case when X_{red}, because(6.12.2.19) shows any invertible sheaf on X_{red} is a pullback of a sheaf of X and(6.5.4.15) shows this sheaf is ample.

Second we reduce to the case X is integral. Let X_i are the integral irreducible components of Z, Cf.[Sta]09NX?

Finally, for X integral, the assertion follows from(6.12.1.2) and(6.5.4.10). □

Cor. (6.12.1.4) [Complete Precurves are Projective]. A separated algebraic scheme X of dimension 1 over a field k is H-(quasi)projective, by(6.12.1.3) and(6.5.4.24). If X is proper, then it is projective. ⌟

Prop. (6.12.1.5) [Completion of Curves]. For a separated algebraic k-scheme X of dimension≤ 1, there is an open immersion $j:X\to\overline{X}$ that

- $\overline{X}$ is projective over k.
- $j(X)\subset\overline{X}$ is dense and schematically dense open subscheme.
- $\overline{X}\backslash X$ consists of f.m. closed points $\{x_i\}$ of $\overline{X}$.

This $\underline{X}$ is called a **completion curve** of X. And when X is reduced, the stalk at x_i are DVRs. In particular, it is non-singular if X is non-singular. ⌟

Proof: By(6.12.1.3), we can assume X is a locally closed subscheme of $\mathbb{P}^n_k$. Let $\overline{X}$ be the scheme theoretic image(6.4.4.62) of the inclusion, then $1,2$ holds by(6.4.4.70). 3 holds because $\overline{X}\backslash X$ is Noetherian of dimension 0.

For the last assertion, Cf.[Sta]0BXW. □

Cor. (6.12.1.6). A morphism of prevarieties $X\to Y$ with X a precurve(thus reduced) and Y proper over a field k factors through the completion $\overline{X}$ of X by(6.4.5.14). In particular, the completion curves of X are unique. ⌟

Prop. (6.12.1.7) [Affine or Projective]. A precurve over a field k is either affine(not proper) or H-projective(proper). ⌟

Proof: Cf.[Sta]0A27?, (Hard). □

Cor. (6.12.1.8). Let X be a separated scheme algebraic over a field k. If $\dim X \leq 1$ and no irreducible component of X is proper of dimension 1, then X is affine. ⌟

Proof: Let X_i be f.m. irreducible components of X, then they are precurves in the induced reduced structure, so they are affine by(6.12.1.7). Now $\coprod X_i \to X$ is a finite surjective morphism, so X is affine by(6.4.4.36). □

Prop. (6.12.1.9). A map from a proper connected scheme to a precurve is either constant or surjective. ⌟

Proof: Because the closed subset of a precurve is either itself or f.m. closed points. □

Prop. (6.12.1.10) [Constant or Finite]. Let $f : X \to Y$ be a morphism of schemes over a field k that Y is separated and X is proper of dimension ≤ 1. If the image of every irreducible component of X is not a pt, then f is finite. If Y is a precurve, then it is moreover surjective. ⌟

Proof: Cf.[Sta]0CCL.? □

Def. (6.12.1.11) [Separable Morphisms]. Let $f : X \to Y$ be a non-constant morphism of precurves, then f is finite surjective by(6.12.1.10). so $\deg(f)$ is finite(6.4.4.55), and we can define separable/purely separable morphisms as in(6.4.4.55). ⌟

Non-Singular Curves

Def. (6.12.1.12) [Uniformizer]. Let C be a precurve over a field k, then the local rings of C at a non-singular closed point p is a DVR by(11.2.3.4). Then an element $t \in K(C)$ with valuation 1 is called a **uniformizer at** p. ⌟

Prop. (6.12.1.13). Let C be a precurve over a field K, and $t \in K(C)$ is a uniformizer at some non-singular point, then $K(C)$ is a finite separable extension of the subfield generated by t. ⌟

Proof: $K(C)$ is a finite extension of $K(t)$, because $\operatorname{tr.deg}(K(C)/K) = 1$ and t is not algebraic over K by valuation reasons. Then it suffices to show for any $x \in K(C)$, x is separable over $K(t)$. Let $\Phi(X,T) = \sum a_{ij}T^iX^j$ be a minimal polynomial of x over $K(T)$. It is separable iff for some $(j,p) = 1$ and some i, $a_{ij} \neq 0$. If it is not separable then we can write $\Phi(X,T) = \sum_{k=0}^{p-1} \varphi_k(X,T)^pT^k$. But each $\varphi_k(x,t)^pt^k$ has distinct valuations, unless they are all zero, contradicting the fact Φ is a minimal polynomial. □

Prop. (6.12.1.14) [Non-singular Complete Precurves and DVRs]. Let C be a non-singular complete precurve, then all valuation rings of $K(C)$ containing k are DVRs, and the set of closed points of C correspond to the set of DVRs in $K(C)$ containing k, which is denoted by $\Sigma^0_{K(C)}$. ⌟

Proof: This is a consequence of the valuation criterion(6.4.5.13). Notice that the local rings of C at closed points are all DVRs(11.2.3.4), thus they must equal to the valuation ring given. □

Prop. (6.12.1.15) [Extension of Rational Maps]. Rational map from a non-singular precurve to a complete prevariety is the same as a morphism, by(6.4.5.15). ⌟

Cor. (6.12.1.16). Two birationally equivalent normal proper precurves over a field is isomorphic.

Thus if a normal precurve is birationally equivalent to another normal complete curve, then it is an open immersion, by(6.12.1.5). ⌟

Prop. (6.12.1.17) [Category of Non-singular Projective Precurves]. Let k be a field, the following categories are equivalent:

1. The opposite category of f.g. field extensions of k of trans.deg 1 with injective k-homomorphisms.
2. The category of precurves and dominant rational maps.
3. The category of normal complete precurves over k with non-constant morphisms.
4. The category of non-singular projective precurves over k with non-constant morphisms.

⌟

Proof: 1 and 2 are equivalent by(6.11.3.2).

3 and 4 are equivalent by(6.12.1.7) and the fact normal and regular are the same(6.4.2.11).

For the rest, Cf.[Sta]0BY1.**?** □

Cor. (6.12.1.18) [Non-singular Projective Model]. Comparing this and(6.11.3.2), we see that every precurve over k is birational to a unique non-singular proper precurve over k with the same function field, which is called the **non-singular projective model**. ⌟

Prop. (6.12.1.19) [Flatness and Associated Points]. $f : X \to Y$ with Y integral and regular of dimension 1. Then f is flat iff every associated prime of X is mapped to the generic point of Y.

In particular when X is reduced, this is equivalent to every irreducible component of X dominants Y, by(5.2.5.25). ⌟

Proof: If x is mapped to a closed pt of Y, then $\mathcal{O}_{y,Y}$ is a DVR, let t be a uniformizer, then t is not a zero-divisor, and $f^\sharp(t) \in \mathfrak{m}_x$ is also not a zero-divisor. So x is not an associated point.

Conversely, to show f is flat, if y is the generic point, then $\mathcal{O}_{y,Y}$ is a field, so it is flat. When y is a closed pt, $\mathcal{O}_{y,Y}$ is a DVR, so by(5.4.1.11), we need to show that it is torsion free. If it is not, then $f^\sharp(t)$ must be a zero-divisor for a uniformizer t of $\mathcal{O}_{y,Y}$. But then it is contained in some associated prime p of $\mathcal{O}_{x,X}$(5.2.5.17). Now p is mapped to y, which is a contradiction. □

Cor. (6.12.1.20) [Morphism to a Non-singular Curve is Flat]. If $f : X \to Y$ is a dominant morphism from a prevariety to a non-singular curve over k, then f is flat. ⌟

Cor. (6.12.1.21) [Flat Specializations along Curves]. Let Y be integral and regular of dimension 1 and P a closed pt. X is a closed subscheme in $\mathbb{P}^n_{Y-P}$ that is flat over $Y - P$, then there is a unique closed subscheme $\overline{X}$ closed in $\mathbb{P}^n_Y$ that is flat over Y and restrict to X on $\mathbb{P}^n_{Y-P}$. ⌟

Proof: Choose the scheme-theoretic closure of X in $\mathbb{P}^n_Y$. Cf.[Hartshorne P258]. □

Cor. (6.12.1.22) [Finite Flatness]. Any non-constant morphism from a precurve to a nonsingular precurve is finite locally free, by(6.12.1.19) and(6.12.1.10). ⌟

Prop. (6.12.1.23). A projective non-degenerate non-singular curve of degree d in $\mathbb{P}^n_k$ is isomorphic to the n-tuple embedding, and $d = n$.

This has easy generalizations to surfaces and higher dimensions. ⌟

Proof: (6.5.3.16)shows $\mathcal{O}_X(1)\cong\mathcal{O}(d)$ over $\mathbb{P}^1_k$, and the restriction of global sections is injective. So the global section is an isomorphism, and it defines the embedding up to a linear automorphism. □

Prop. (6.12.1.24) [Genera Equal]. For a complete smooth curve X over a field k,

$$p_a(X)=p_g(X)=\dim_k H^1(X,\mathcal{O}_X)$$

by Serre duality(6.8.6.19) and(6.11.1.18)(6.7.3.6).

So from now on we use genus to denote the arithmetic genus. ⌟

Cor. (6.12.1.25) [Topological Genus]. By GAGA, for a complex complete smooth curve, the genus also equals the topological genus. ⌟

Morphisms Between Non-singular Curves

Prop. (6.12.1.26) [Degree and Analytic Degree]. Let $f:C\to C'$ be a non-constant morphism between smooth complex curves, then the degree defined in(6.4.4.55) is the same as the degree as map of Riemann surfaces. ⌟

Proof: This is because the map is finite locally free(6.12.1.22), thus for an affine open subset $U=\operatorname{Spec}A$ of C', the $f^{-1}(U)=\operatorname{Spec}B$ where $B\cong A^{\otimes n}$ as A-modules, where n is the degree. Then clearly for most $x\in U$, $\sharp f^{-1}(x)=n$(look at the minimal polynomial of a family of generators for B over A). □

Def. (6.12.1.27) [Ramification Degrees]. Let $f:X\to Y$ be a morphism of non-singular precurves over a field k, let $P\in X$ be a closed point and $f(P)=Q$. Because the local rings are DVRs, we define the **ramification degree** $e_P(f)$ where $f^\sharp(\mathfrak{m}_Q)\mathcal{O}_{X,P}=\mathfrak{m}_P^{e_P(f)}$.

f is called **weakly unramified at** P if $e_P(f)=1$, and it is called **unramified at** P if moreover $\kappa(P)/\kappa(f(P))$ is separable. f is called **tamely unramified at** P if**?**

Notice that unramifiedness just means the morphism is unramified, by(6.6.5.8) and(6.12.1.22). ⌟

Prop. (6.12.1.28). Let $f:X\to Y$ be a non-constant morphism of non-singular precurves over a field k, then

- If $g:Y\to X$ be another morphism of non-singular precurves, then for any $P_1\in X$, $e_P(g\circ f)=e_P(f)e_{f(P)}(g)$.
- for any closed point $Q\in C_2$, $\sum_{P\in f^{-1}(Q)}e_P(f)[k(P):k(Q)]=\deg(f)$.
- If k is alg.closed, then for a.e. closed point $Q\in C_2$, $\#f^{-1}(Q)=\deg_s(f)$.

⌟

Proof: 1: Trivial.

2: This follows from(6.12.1.44).

3: This follows from(6.11.3.4). □

Prop. (6.12.1.29). If $f:X\to Y$ is a non-constant morphism of percurves over a field k s.t. X is smooth and Y is non-singular, then Y is also smooth, by(6.1.5.28). ⌟

Prop. (6.12.1.30). Let X be a smooth curve over a field k, $x\in X$ and $\overline{x}\in X_{\overline{k}}$ is a point mapping to x, then the ramification degree of $\mathcal{O}_{X,x}\subset\mathcal{O}_{X_{\overline{k}},\overline{x}}$ equals the inseparable degree of $k(x)/k$. ⌟

Proof: By(6.6.6.7), we can find a étalemap $X \to \mathbb{A}^1_k$, which has ramification degree 1 and separable, so we may assume $X = \mathbb{A}^1_k$. Then the assertion is clear. □

Prop. (6.12.1.31) [Separable Morphisms]. Let $f : X \to Y$ be a morphism of smooth curves over k, then the following are equivalent:

1. f is finite separable.
2. $df^* : f^*\Omega_{Y/k} \to \Omega_{X/k}$ is non-zero.
3. $\Omega_{X/Y}$ is supported on a proper closed subscheme of X.
4. There exists a non-empty open subset $U \subset X$ s.t. f is unramified.
5. There exists a non-empty open subset $U \subset X$ s.t. f is étale.

⌟

Proof: As X, Y are smooth, $\Omega_{X/k}, \Omega_{Y/k}$ are invertible sheaves, and the exact sequence

$$f^*\Omega_{Y/k} \to \Omega_{X/k} \to \Omega_{X/Y} \to 0$$

shows 2, 3 are both equivalent to $\Omega_{X/Y,\xi} = 0$.

3, 4, 5 are equivalent as f is automatically flat(6.12.1.20).

1, 5 are equivalent by(6.6.5.9). □

Prop. (6.12.1.32) [Riemann-Hurewitz for Separable Maps]. If $f : X \to Y$ is a non-constant separable map between two complete smooth curves over a field k, then

$$2g_X - 2 = \deg(f)(2g_Y - 2) + \sum_{x\in X} d_x[\kappa(x) : k],$$

where $d_x = \mathrm{length}_{\mathcal{O}_{X,x}}(\Omega_{X/Y,x}) \geq 0$ satisfies $d_x \geq e_x(f) - 1$, and equality holds iff f is tamely unramified at P. ⌟

Proof: By(6.8.7.12), in this case the vanishing locus R of df^* is an effective Cartier divisor, and $f^*\mathcal{K}_{Y/k} \otimes \mathcal{O}(R) \cong \mathcal{K}_{X/k}$, so by(6.12.2.10)(6.12.2.3)(6.12.2.7),

$$2g_X - 2 = \deg(\mathcal{K}_{X/k}) = \deg(f^*\mathcal{K}_{Y/k} \otimes \mathcal{O}(R)) = \deg(f)\deg(\mathcal{K}_{Y/k}) + \deg(R) = \deg(f)(2g_Y - 2) + \deg(R).$$

For analysis of d_x, Cf.[Sta]0C1F.? □

Cor. (6.12.1.33). The only geo.integral unramified finite covering of $\mathbb{P}^1_k$ is itself. ⌟

Thm. (6.12.1.34) [De Franchis]. Let $k \in$ `Field` and C, C' are two complete smooth curves over k. Then if $g(C) \geq 2$, there are only f.m. non-constant maps $C' \to C$.

In particular, $\#\mathrm{Aut}(C) < \infty$. ⌟

Proof: We prove for $k = \mathbb{C}$? Cf.[Mil08]P146.

Any automorphism of C fixes its set of Weierstrass sets, which is finite, so we only need to consider the case that it fixes all Weierstrass points.

If C is hyperelliptic, consider a hyperelliptic map, this covering has an involution of C, and this is just $C \mapsto C/\tau$. So modulo τ, it suffices to show $\mathbb{P}^1$ has f.m. automorphisms fixing the branch points. But this is true, as $2g + 2 > 3$.

If C is non-hyperelliptic, then there are more than $2g + 2$ Weierstrass points. But we can find a function f on C with $g + 1$ zeros and poles, by Riemann-Roch, then for an automorphism φ of C, $f - \varphi^* f$ has no more than $2g + 2$ poles, so also has no more than $2g + 2$ zeros. But φ fixes all Weierstrass points, so it has more than $2g + 2$ zeros, contradiction. □

Prop. (6.12.1.35)[Hurewitz's Automorphism Theorem]. If C is a complete smooth curve of genus $g \geq 2$ over a field of characteristic 0, then $\#\operatorname{Aut}(C) \leq 84(g-1)$. ⌟

Proof: We may pass to the alg.closure. By(6.12.1.34), $\#\operatorname{Aut}(C) < \infty$. In fact, let G be a finite group acting on C, let C' be the non-singular precurve corresponding to C', then by(3.2.8.5), $C \to C'$ is a Galois cover with Galois group G. Now by Dedekind extension theory, G acts transitively on the preimage of a given point. Suppose there are n branched points with ramification degrees r_i, then by Riemann-Hurewitz(6.12.1.32)(notice in this case it is tamely unramified):

$$(2g-2) = |G|(2g(C') - 2 + \sum_{i=1}^{n} \frac{r_i - 1}{r_i}).$$

Then a combinatorial argument shows the maximal possible $|G|$ is obtained when $g(C') = 0, n = 3$ and $(r_1, r_2, r_3) = (2, 3, 7)$. □

Remark (6.12.1.36). In the case $\operatorname{char} k \neq 0$, there may be more automorphisms. For example, if $p \in \mathbf{P}\backslash\{2\}$, the completion of the affine curve $y^{p^n} = x + x^{p^n+1}$ has genus $g = p^n(p^n-1)/12$ and $\#\operatorname{Aut}(C) = p^{3n}(p^{3n}+1)(p^{2n}-1)$, Cf.[H.Stichtenoth,U¨berdieAutomorphismengruppeeinesalgebraischenFunktionenko¨rpersvon Primzahlcharakteristik. I. Eine Abscha¨tzung der Ordnung der Automorphismengruppe, Arch. Math. (Basel) 24 (1973), 527–544.]. ⌟

Prop. (6.12.1.37) [Frobenius Map]. Let C be a smooth curve over a field k of characteristic p, and $C \xrightarrow{F_{X/k,r}} C^{(r)}$ be the Frobenius, where $C^{(r)} = C \otimes_{k,\mathrm{Frob}^r} k$, then $F_{X/k,r}$ is purely inseparable, and $\deg(F_{X/k,r}) = p^r$. And it is a topological homeomorphism by(5.1.7.26). ⌟

Proof: To show inseparability, we can base change to $\overline{k}$, then the field map is $f/g \mapsto f(\underline{X}^{p^r})/g(\underline{X}^{p^r})$, which is just $K(C_{\overline{k}})^{p^r}$, so purely inseparable of degree p^r. □

Prop. (6.12.1.38) [Inseparable Decomposition]. Let k be a field of characteristic $p > 0$. If C_1 is a smooth complete precurve, then any map of non-singular complete precurves $f : C_1 \to C_2$ over k factors as

$$C_1 \xrightarrow{F_{X/k,r}} C_1^{(r)} \xrightarrow{\lambda} C_2$$

where $C_1^{(r)} = C_1 \otimes_{k,\mathrm{Frob}^r} k$, and λ is separable. ⌟

Proof: By(6.12.1.17), it suffices to show any inseparable morphism is a Frobenius. It suffices to show that any subfield of $K(X)$ of index p equals $K(X^{(1)}) = kK(X)^p$. For this, Cf.[Sta]0CCY**?**. □

Cor. (6.12.1.39). If $C \to C'$ is a non-constant separable map between complete smooth curves, then $g(C) \geq g(C')$. ⌟

Proof: This follows from(6.12.1.38)(6.12.1.32) and the fact $C_1^{(r)}$ is smooth and have the same genus as C_1 by flat base change. □

Divisors on Curves

Def. (6.12.1.40)[Divisors on Curves]. If X is a locally algebraic integral scheme of dimension 1 over an alg.closed field, then a Weil divisor on X are just a locally finite formal sum of closed pts.

If X is integral algebraic over a field k of dimension 1, then the sum is in fact finite, we we can define the **degree** of a Weil divisor $D = \sum n_P P$ as $\deg(D) = \sum n_P [k(P) : k]$.

Similarly, for a Cartier divisor D on X, the **degree of** D is defined to be $\dim_k \Gamma(D, \mathcal{O}_D)$. By(8.1.5.1), a Cartier Divisor on X is equivalent to an effective Weil divisor, and the definition of degrees are compatible. ⌟

Cor. (6.12.1.41) [Non-singular Case]. As a nonsingular precurve C is locally factorial, (6.5.3.15) shows in this case a line bundles on $\mathcal{C}$ is equivalent to a Weil divisor on C. ⌟

Prop. (6.12.1.42) [Pullback of Divisor]. For a non-constant morphism f between two non-singular curves over alg.closed field, e.g. dominant morphism between complete non-singular curves, $\deg f^*D = \deg f \cdot \deg D$. This is because f is finite locally free(6.12.1.22), thus this follows from [Sta]02RH**?**. ⌟

Prop. (6.12.1.43). An element $\notin k$ in the function fields of a projective non-singular curve over an alg.closed k defines a inclusion $k(f) \subset K(X)$ thus a morphism from X to P^1_k(6.11.3.2), and $(f) = \varphi^*(\{0\} - \{\infty\})$. ⌟

Prop. (6.12.1.44). Let $\pi : C \to C'$ be a non-constant separable morphism of precurves over a field k that C' is nonsingular, $p \in C'$ is a closed point, then π is finite locally free by(6.12.1.22), and

- $\pi^{-1}(p) \subset C$ is a dimension 0 scheme.
- $\dim_k(\Gamma(\pi^{-1}(p))) = (\deg \pi)(\deg p)$.
- Let ϖ be a uniformizer of the DVR $\mathcal{O}_{C',p}$, then

$$\deg \pi = \sum_{x \in \pi^{-1}(p)} [k(x) : k(p)] \operatorname{ord}_{\mathcal{O}_{C,x}}(f^*\varpi).$$

⌟

Proof: Look affine locally, then these follow from the fundamental identity(5.2.7.21). □

Prop. (6.12.1.45). For a 1-dimensional integral scheme $c : X \to k$ proper over a field k and a function $f \in K(X)^*$,

$$\sum_{x \text{ closed}} [k(x) : k] \operatorname{ord}_{\mathcal{O}_{X,x}}(f) = 0.$$

In other words, the number of zeros of f equals the number of poles of f. ⌟

Proof: It suffices to show that the pushforward $c_* \operatorname{div}(f) = 0 \in \operatorname{CH}_0(\operatorname{Spec} k)$. consider Y the closure of the graph of f in $X \times \mathbb{P}^1_k$, then there is a commutative diagram

$$\begin{array}{ccc} Y & \xrightarrow{\mathrm{pr}_1} & X \\ \downarrow{\scriptstyle \mathrm{pr}_2} & & \downarrow{\scriptstyle c} \\ \mathbb{P}^1_k & \xrightarrow{c'} & \operatorname{Spec} k \end{array},$$

and $\operatorname{div}_X(f) = \mathrm{pr}_{1*} \operatorname{div}_Y(f)$ by(8.1.2.22). We may assume f is not constant, then pr_2 is finite locally free of degree d, and $\operatorname{div}_Y(f) = \mathrm{pr}_2^*([(0)] - [(\infty)])$, so $\mathrm{pr}_{2*} \operatorname{div}_Y(f) = d([(0)] - [(\infty)])$ is mapped to $0 \in \operatorname{CH}_0(\operatorname{Spec} k)$. □

2 Vector Bundles

Degrees and Riemann-Roch

Def. (6.12.2.1) [Degrees]. The **degree of a locally free sheaf** $\mathcal{E}$ of rank n on a proper scheme X of dimension≤ 1 over a field k is defined to be $\deg(\mathcal{E}) = \chi(X, \mathcal{E}) - n\chi(\mathcal{O}_X)$(6.7.3.1).

If X is integral(e.g. a complete precurve), this definition can extends to any coherent sheaves $\mathcal{F}$, if we define $\operatorname{rank}(\mathcal{F}) = \dim_{k(\eta)} \mathcal{F}_\eta$. ⌟

Prop. (6.12.2.2). The degree function is additive, stable under base change of fields, and stable under birational equivalence of proper scheme X of dimension 1 over a field k. ⌟

Proof: The base change follows from flat base change(6.7.5.1), the additivity follows from the additivity of rank and Euler characteristic(6.7.3.1).

For the birational equivalence, If $f : X \to Y$ is a birational map between proper schemes of dimension≤ 1 over k, then f is proper with finite fibres, so f is finite(6.4.5.5), thus for any $\mathcal{E} \in \mathcal{QC}\mathrm{oh}^{\mathrm{free},n}(Y)$, $f_* f^* \mathcal{E} = \mathcal{E} \otimes_{\mathcal{O}_Y} f_* \mathcal{O}_X$, and there is an exact sequence

$$0 \to \mathcal{K} \to \mathcal{O}_Y \to f_* \mathcal{O}_X \to \mathcal{Q} \to 0$$

where $\mathcal{K}, \mathcal{Q}$ are coherent sheaves on Y with supported dimension0. Then by(6.7.3.5) and(6.7.3.3),

$$\begin{aligned}\chi(Y, \mathcal{E}) - \chi(X, f^*\mathcal{E}) &= \chi(Y, \mathcal{E}) - \chi(Y, f_* f^* \mathcal{E}) \\ &= \chi(Y, \mathcal{K} \otimes \mathcal{E}) - \chi(Y, \mathcal{Q} \otimes E) \\ &= n\chi(Y, \mathcal{K}) - n\chi(Y, \mathcal{Q}) \\ &= n\chi(Y, \mathcal{O}_Y) - n\chi(X, \mathcal{O}_X)\end{aligned}$$

□

Prop. (6.12.2.3) [Non-reduced Riemann-Roch]. If X is a proper scheme over a field k of dimension≤ 1 with integral components C_i of X of dimension1 with generic points $\eta_1, \ldots, \eta_r$ and multiplicity m_i, and $\mathcal{E} \in \mathcal{V}\mathrm{ect}^n(C), \mathcal{F} \in \mathcal{C}\mathrm{oh}(C)$, then

$$\chi(\mathcal{E} \otimes \mathcal{F}) = \sum_i (\operatorname{length}_{\mathcal{O}_{X,\eta_i}} \mathcal{F}_{\eta_i}) \deg(\mathcal{E}|_{C_i}) + n\chi(\mathcal{F}).$$

⌟

Proof: We use dévissage(6.5.1.55), the condition1 are true by additivity of χ, and for condition2, take $\mathcal{G} = i_* \mathcal{O}_Z$, the equation holds by(6.7.3.5) and projection formula. □

Cor. (6.12.2.4). Let X be a proper scheme of dimension≤ 1 over a field k, and C_i are the irreducible components of X of dimension1 with the induced reduced structure and multiplicity m_i, then for $\mathcal{E} \in \mathcal{C}\mathrm{oh}^{\mathrm{free}}(X)$,

$$\deg(\mathcal{E}) = \sum m_i \deg(\mathcal{E}|_{C_i}).$$

⌟

Cor. (6.12.2.5). Let X be a proper scheme of dimension≤ 1 over a field k, then

- If $\mathcal{E} \in \mathcal{C}\mathrm{oh}^{\mathrm{free},m}(X), \mathcal{F} \in \mathcal{C}\mathrm{oh}^{\mathrm{free},n}(X)$, then $\deg(\mathcal{E} \otimes \mathcal{F}) = m\deg(\mathcal{F}) + n\deg(\mathcal{E})$.
- If $\mathcal{L}, \mathcal{M} \in \operatorname{Pic}(X)$, then $\deg(\mathcal{L} \otimes \mathcal{M}) = \deg(\mathcal{L}) + \deg(\mathcal{M})$.

- If $\mathcal{L} \in \mathrm{Pic}(X)$, $\deg(\mathcal{L}) = -\deg(\mathcal{L}^{-1})$.
- If $\mathcal{E} \in \mathfrak{Coh}^{\mathrm{free}}(X)$, $\deg(\mathcal{E}) = \deg(\wedge\mathcal{E})$.

⌟

Proof: By(6.12.2.4), we can assume X is integral. Then $1, 2$ follow from(6.12.2.3), and 3 follows from the fact there is a modification $X' \to X$ s.t. $f^*\mathcal{E}$ has a filtration with invertible sheaves $\mathcal{L}_i$ as quotients(6.5.1.30). Then by(6.12.2.2), we can work on X'. Then $\deg(\mathcal{E}) = \otimes_i \mathcal{L}_i$, and the assertion follows from additivity and(6.12.2.3). □

Prop. (6.12.2.6). If D is an effective Cartier divisor on a proper scheme of dimension≤ 1 on a field k, then for $\mathcal{E} \in \mathfrak{Coh}^{\mathrm{free},n}(X)$,

$$\deg(\mathcal{E}(D)) = n \dim_k \deg(D) + \deg(\mathcal{E})$$

In particular, $\deg(\mathcal{L}(D)) = \deg(D)$. ⌟

Proof: By(6.8.1.2), D is nowhere dense in X, thus D is finite over k, and there is an exact sequence

$$0 \to \mathcal{E} \to \mathcal{E}(D) \to \mathcal{E}(D)|_D \to 0.$$

So the assertion follows from(6.7.3.5). □

Prop. (6.12.2.7). Let $f : X \to Y$ be a non-constant map of complete precurves over a field k and $\mathcal{E} \in \mathfrak{Coh}^{\mathrm{free}}(Y)$, then $\deg(f^*\mathcal{E}) = \deg(f)\deg(\mathcal{E})$. ⌟

Proof: By(6.12.1.10) and(6.12.2.3),

$$\chi(X, f^*\mathcal{E}) = \chi(Y, \mathcal{E} \otimes f_*\mathcal{O}_X) = \deg(f)\deg(\mathcal{E}) + \mathrm{rank}(\mathcal{E})\chi(X, \mathcal{O}_X).$$

□

Prop. (6.12.2.8)[Degree and Sections]. Let C be a complete precurve over a field k and $\mathcal{L} \in \mathrm{Pic}(C)$, then

- If $\mathcal{L}$ has a non-zero section, then $\deg(\mathcal{L}) \geq 0$.
- If $\mathcal{L}$ has a non-zero section that vanishes at some point, then $\deg(\mathcal{L}) \geq 1$.
- If both $\mathcal{L}, \mathcal{L}^{-1}$ have non-zero sections, then $\mathcal{L} \cong \mathcal{O}_X$.
- If $\deg(\mathcal{L}) \leq 0$ and $\mathcal{L}$ has a non-zero section, then $\mathcal{L} \cong \mathcal{O}_X$.
- If $\mathcal{N} \to \mathcal{L}$ is a non-zero map of invertible sheaves, then $\deg(\mathcal{L}) \geq \deg(\mathcal{N})$, with equality iff this is an isomorphism.

⌟

Proof: If s is a section of $\mathcal{L}$ with vanishing locus D, then D is an effective Cartier divisor and $\mathcal{L} \cong \mathcal{L}(D)$, so $\deg(\mathcal{L}) = \deg(D)$ by(6.12.2.6), so these are all simple now. □

Prop. (6.12.2.9) [Riemann-Roch]. Let D be a Weil divisor on a complete non-singular precurve X of genus g, then

- If $l(D) = \dim_k H^0(X, \mathcal{L}(D))$, $l(D)$ is finite by(6.7.4.11).
- $[\omega_X]$ is an invertible sheaf by [Sta]0BFQ**?**.
- $l(D) - l([\omega_X] - D) = \deg D + 1 - g$.

- $\deg(D) = \deg(\mathcal{L}(D))$

Notice when X is smooth, $[\omega_X]$ is just $\mathcal{K}_X$(6.8.6.18). ⌟

Proof: 4 is equivalent to 3 by Serre duality(6.8.6.18), and 3 follows from(6.12.2.6). □

Cor. (6.12.2.10). $\deg([\omega_C]) = 2g-2$. ⌟

Proof: By(6.12.2.9) and Serre-duality(6.8.6.18),

$$\deg([\omega_C]) = h^0(X,[\omega_X]) - h^0(X,\mathcal{O}_X) + g - 1 = h^1(X,\mathcal{O}_X) - h^0(X,\mathcal{O}_X) + g - 1 = 2g-2.$$

□

Prop. (6.12.2.11)[Twisting Sheaves]. Let $\mathcal{L}$ be a line bundle on a complete nonsingular precurve C, and $p \in C$ is a closed point of degree d, then $0 \le h^0(\mathcal{L}) - h^0(\mathcal{L}(-p)) \le d$ for any $\mathcal{L} \in \mathrm{Pic}(C)$.

In particular, by(6.12.2.8), if C is a complete non-singular curve, then $h^0(\mathcal{L}) \le \deg L + 1$ for any $\mathcal{L} \in \mathrm{Pic}(C)$. ⌟

Proof: There is an exact sequence $0 \to \mathcal{O}_C(-p) \to \mathcal{O}_C \to \mathcal{O}_C|_p \to 0$, tensoring with $\mathcal{L}$ and take the cohomology, we get an exact sequence $0 \to h^0(\mathcal{L},\mathcal{L}(-p)) \to h^0(\mathcal{L},\mathcal{L}) \to H^0(C,\mathcal{L}|_p)$, and notice that $h^0(C,\mathcal{L}|_p) = d$. □

Prop. (6.12.2.12)[Riemann-Roch for High Degree D]. If $\deg(D) \ge 2g-1$, then $\deg([\omega_X]-D) < 0$, so by(6.12.2.8), $l([\omega_X]-D) = 0$, thus $l(D) = d-g+1$. ⌟

Cor. (6.12.2.13)[Characterizing $[\omega_C]$]. Any degree $2g-2$ divisor D satisfies $l(D) = g-1$ or g, and the latter case happens iff $D = [\omega_C]$. ⌟

Proof: $l([\omega_C]-D) = 1$ iff $[\omega_C] = D$ by(6.12.2.8). □

Def. (6.12.2.14)[Special Divisors]. A **special divisor** on a complete non-singular curve is a divisor D that $h^0([\omega_C]-D) > 0$. ⌟

Prop. (6.12.2.15). For any complete smooth curve C of genus $g > 1$ over a field k, there is a closed point on C of degree$\le 2g-2$. And if $g \ge 2$, we can assume this point is a geometric point. ⌟

Proof: The canonical sheaf $\mathcal{K}_C$ is a line bundle of degree $2g-2$ and $h^0(\mathcal{K}_C) = g \ge 1$, so we can assume $\mathcal{K}_C$ is an effective divisor, then one of its support point has degree$\le 2g-2$.

For the last assertion, Cf.[Sta]0CD4. □

<u>**Vector Bundles**</u>

Prop. (6.12.2.16)[Torsion-Free Sheaves]. Let C be a non-singular precurves over a field k, then

- Any torsion-free coherent sheaf $\mathcal{F}$ on C is locally free.
- Any $\mathcal{F} \in \mathfrak{Coh}(X)$ factors as $0 \to \mathcal{F}_{\mathrm{tor}} \to \mathcal{F} \to \mathcal{F}_{\mathrm{lf}} \to 0$, where $\mathcal{F}$ is a torsion sheaf(6.5.1.44) and $\mathcal{F}_{\mathrm{lf}}$ is Qco and locally free, by(6.5.1.47)

⌟

Proof: □

Prop. (6.12.2.17)[$\mathrm{Pic}^0(C)$]. For a smooth complete curve C over a field k with a rational point, $\mathrm{Pic}^0(C)$ are exactly the set of line bundles of degree 0, by(15.7.10.1). In particular, there is an exact sequence

$$0 \to \mathrm{Pic}^0(C) \to \mathrm{Pic}(C) \to \mathbb{Z} \to 0.$$

⌟

Prop. (6.12.2.18)[Torsion Elements]. Let C be a smooth complete curve of genus g over an alg.closed field, then for $m \in \mathbb{Z} \cap k^*$, $\mathrm{Pic}(C)[m] = \mathrm{Pic}^0(C) \cong (\mathbb{Z}/(m))^{2g}$. ⌟

Proof: This follows from(15.7.10.1)(6.12.2.17) and(15.7.6.14). □

Prop. (6.12.2.19). If $Z \to X$ is a closed immersion and $\dim X \leq 1$, then $\mathrm{Pic}\, X \to \mathrm{Pic}\, Z$ is a surjection. ⌟

Proof: Use the exact sequence $0 \to (1 + \mathcal{I}) \cap \mathcal{O}_X^* \to \mathcal{O}_X^* \to i_*\mathcal{O}_Z^* \to 0$, $\dim X \leq 1$ and the Grothendieck vanishing theorem gives the desired result, also notice i is affine. □

Ample Line Bundles

Prop. (6.12.2.20). A line bundle $\mathcal{L}$ over a complete precurve C over a field k is ample iff $\deg(\mathcal{L}) > 0$. ⌟

Proof: If C is non-singular, the proof is easy: $\mathcal{L}$ is ample iff $\mathcal{L}^{\otimes n}$ is very ample for n large(6.5.4.24). If $\deg(\mathcal{L}) < 0$, this cannot happen, by(6.12.2.8). For $\deg L \geq 0$, $\mathcal{L}^{\otimes n}$ is very ample for n large by(6.12.2.26).

In general, Cf.[Sta]0B5X**?** □

Cor. (6.12.2.21)[Ample and Nef Line Bundles]. Let $\mathcal{L}$ be an invertible $\mathcal{O}_X$-module over a proper scheme of dimension≤ 1 over k, let C_i be the integral components of X of dimension 1, then $\mathcal{L}$ is a ample iff $\deg(\mathcal{L}|_{C_i}) > 0$ for all i. ⌟

Proof: This follows from(6.5.4.14) applied to the reduced structure of the irreducible components of X, together with the fact a line bundle on an irreducible component $\mathrm{Spec}\, k(x)$ of dimension 0 is obviously ample. □

Prop. (6.12.2.22). Let $\mathcal{L}$ be a line bundle on a complete non-singular precurve C of degree d that is basepoint-free, then it determines a morphism $\pi : C \to \mathbb{P}_k^1$ of degree d. ⌟

Proof: This follows from(6.12.1.44). □

Prop. (6.12.2.23). Let C be a complete precurve over a field k with genus $g > 0$, and p, q are rational points on C, then $\mathcal{O}_C(p) \cong \mathcal{O}_C(q)$ iff $p = q$, and $h^0(C, \mathcal{O}_C(p)) = 1$. ⌟

Proof: The hypothesis shows $\mathcal{L} = \mathcal{O}_C(p)$ has degree 1 and is basepoint-free, thus defines a degree 1 map $C \to \mathbb{P}_k^1$, which is an isomorphism, by(6.12.1.15) and(6.12.1.17), contradiction.

If $h^0(C, \mathcal{O}_C(p)) \geq 2$, then for any section s, $\mathrm{div}(s) = q$ for some rational point q, so by the above argument, $q = p$, so any two such f is proportional. □

Prop. (6.12.2.24). Let C be a complete curve over a field k with genus $g > 0$, and $\mathcal{L}$ is a line bundle of degree 2, then $h^0(C, \mathcal{L}) \leq 2$, and if the equality holds, then it is basepoint-free. ⌟

Proof: We can base change to $\overline{k}$. $h^0(C,\mathcal{L})\leq 3$ by(6.12.2.11). If equality holds, then then $h^0(C,\mathcal{L}(-p))=2$ for some p, contradiction by(6.12.2.23). If $h^0(C,\mathcal{L})=2$, then $h^0(C,\mathcal{L}(-p))<2$ for any p, so it is basepoint-free. Conversely, if it is basepoint free, then $\mathcal{L}\cong\mathcal{O}(p)$ for some rational point p, and $h^0(C,\mathcal{L})=h^0(C,\mathcal{O}_C)+1=2$. □

Prop. (6.12.2.25) [Criterion of Very Ampleness]. Let $\mathcal{L}$ be a line bundle on a curve over an alg.closed field k, then

- $\mathcal{L}$ is basepoint-free iff $h^0(\mathcal{L})-h^0(\mathcal{L}-p)=1$ for any closed point $p\in\mathcal{L}$.
- $\mathcal{L}$ is very ample iff $h^0(\mathcal{L})-h^0(\mathcal{L}-p-q)=2$ for any closed points $p,q\in\mathcal{L}$.

⌟

Proof: Cf.[Vakil, P509].**?** □

Cor. (6.12.2.26). Any line bundle $\mathcal{L}$ on a complete non-singular curve of genus g that $\deg(\mathcal{L})\geq 2g$ is basepoint-free, and if $\deg(\mathcal{L})\geq 2g+1$, then it is very ample. ⌟

Proof: When $k=\overline{k}$, this follows from(6.12.2.25) and Riemann-Roch(6.12.2.9). For general k, use the fact being basepoint-free, closed embedding and degree are all stable and reflective under base change of fields(6.12.2.2)(6.5.3.3)(6.1.5.26). □

Prop. (6.12.2.27) [Very Ample Line Bundles]. Let X be a complete curve over a field k, then

- If $\mathcal{L}$ is effective and $H^1(X,\mathcal{L})=0$, then $\mathcal{L}^{\oplus 6}$ is very ample.
- If $\mathcal{L}$ is globally generated and $H^1(X,\mathcal{L})=0$, then $\mathcal{L}^{\oplus 2}$ is very ample.

⌟

Proof: Cf.[Sta]0E8V, 0E8W.**?** □

Curves in Low Dimension

Prop. (6.12.2.28) [Projection Along a Point]. Let $C\subset\mathbb{P}^n_k$ be a non-singular precurve, then for any rational point $p\in C$, there is a **projection along** p map $v_p:C\to\mathbb{P}^{n-1}_k$ that is the projection along p for $q\in C\backslash\{p\}$, and extend to whole C by(6.12.1.15), which corresponds to the line bundle $\mathcal{O}_C(1)(-p)$. ⌟

Prop. (6.12.2.29). Let C be a smooth plane precurve of degree $e>2$ and D_1,D_2 are two polynomials of degree d not vanishing on C. Suppose there is a divisor E on C of degree $de-1$ and rational points p_i on C that $D_i|_C=E+p_i$, then $\mathcal{O}_C(-E)$ is not base-free. ⌟

Proof: Notice by genus formula $g>0$, and $\mathcal{O}_C(-E)\cong\mathcal{O}_C(p_i)$ has degree 1, then $p_1=p_2$ by(6.12.2.23). □

Prop. (6.12.2.30). Let C be a smooth conic plane curve over a field of characteristic$\neq 2$, show the dual variety of C is also a smooth conic. In particular, for a general point in the plane, there are two tangents to C.(This can be also proved using Riemann-Hurewitz by projection through this point). ⌟

Proof:

□

Prop. (6.12.2.31). The number of plane conics containing i generally chosen points and $5-i$ generally chosen lines is $1,2,4,4,2,1$ resp. for $i=0,1,\dots,4,5$. (The duality comes from the duality between the conic and the dual conic(6.12.2.30)). ⌟

Proof: □

Prop. (6.12.2.32) [Curves in $\mathbb{P}^1 \times \mathbb{P}^1$]. Let C be a curve in $\mathbb{P}^1 \times \mathbb{P}^1$ given by a bi-homogenous polynomial of type (a, b). Then $g(C) = (a-1)(b-1)$. ⌟

Proof: We have $\mathcal{K}_C = (\mathcal{K}_{\mathbb{P}^1\times\mathbb{P}^1} + C)|_C$(6.11.1.17). We have $\mathrm{Pic}(\mathbb{P}^1 \times \mathbb{P}^1) \cong \mathbb{Z}H_1 \oplus \mathbb{Z}H_2$, thus

$$\begin{aligned}\deg(\mathcal{K}_C) &= \deg((\mathcal{K}_{\mathbb{P}^1\times\mathbb{P}^1} + C)_C) \\ &= \deg((-2H_1 - 2H_2 + aH_1 + bH_2)|_C) \\ &= \deg(((a-2)H_1 + (b-2)H_2)|_C) \\ &= (a-2)b + (b-2)a = 2ab - 2a - 2b \\ &= 2g - 2.\end{aligned}$$

Thus $g = (a-1)(b-1)$.

? For non-smooth case, see AG psets. □

Prop. (6.12.2.33) [Genus Formula]. Let C be a closed subscheme of $\mathbb{P}^2_k$ defined by a homogenous polynomial $f(x_0, x_1, x_2)$ of degree d, then it has arithmetic genus $p_a(C) = (d-1)(d-2)/2$. ⌟

Proof: This follows from(6.7.2.4). □

Cor. (6.12.2.34). Let C be a complete smooth plane curve of degree d, then it has genus $g = (d-1)(d-2)/2$. ⌟

Proof: Alternative proof: By adjunction formula, $\mathcal{K}_C = \mathcal{K}_{\mathbb{P}^2}(C)|_C = \mathcal{O}_C(d-3)$ which has degree $d(d-3)$. But this also equals $2g-2$(6.12.2.10), thus $g = (d-1)(d-2)/2$. □

Prop. (6.12.2.35)[Cubic Curves in $\mathbb{P}^3$]. A twisted cubic(rational) C in $\mathbb{P}^3$ is contained in a quadric. ⌟

Proof: Calculate that $h^0(\mathcal{O}_{\mathbb{P}^3}(2)) = C_5^2 = 10$ and $\deg(\mathcal{O}_C(2)) = 6$, thus $h^0(\mathcal{O}_C(2)) = 6 + 1 = 7$ by Riemann-Roch. Then C is contained in 3 quadrics. □

3 Singularities and δ-Invariants

Def. (6.12.3.1) [Different Kinds of Singularities]. Let X be a curve over an alg.closed field k, a point $p \in X$ is called a

- **node** if the completion of $\mathcal{O}_{X,p}$ at $\mathfrak{m}_{X,p}$ is isomorphic to $k[[x,y]]/(xy)$ as topological local rings.
- **cusp** if the completion of $\mathcal{O}_{X,p}$ at $\mathfrak{m}_{X,p}$ is isomorphic to the completion of $k[x,y]/(x^2 - y^3)$ at (x,y).
- **tacnode** if the completion of $\mathcal{O}_{X,p}$ at $\mathfrak{m}_{X,p}$ is isomorphic to the completion of $k[x,y]/(x^2 - y^4)$ at (x,y).
- **triple point** if the completion of $\mathcal{O}_{X,p}$ at $\mathfrak{m}_{X,p}$ is isomorphic to the completion of $k[x,y]/(x^3 - y^3)$ at (x,y).

⌟

Def. (6.12.3.2) [δ-Invariants]. ⌟

4 Linear Series

Def. (6.12.4.1) [Moduli Spaces]. Define the **Hilbert scheme** $\mathcal{H}_{d,g,r} = \{\text{Curves } C \text{ of degree } d \text{ and genus } g\}$.

Define the **moduli space of curves** $\mathcal{M}_g = \{\text{isomorphism classes of smooth projective curves of genus } g\}$.

Define $W_d^r(C) = \{L \in \mathrm{Pic}^d(C), h^0(L) \geq r+1\}$. ⌟

Def. (6.12.4.2) [Linear Series]. A **linear series** is a line bundle L together with a vector space $V \subset H^0(L)$.

A $\mathfrak{g}_d^r$ is a line bundle L together with a vector space $V \subset H^0(L)$ of dimension $r+1$.

For a line bundle $\mathcal{L}$, denote by $|L|$ the linear series $(L, H^0(L))$. ⌟

Cor. (6.12.4.3) [$r \leq d$]. If $\mathfrak{g}_d^r$ exists on a complete curve C, then $r \leq d$. And if $r = d$, then $g(C) = 0$. ⌟

Proof: Let s be a section of $\mathcal{L}$, then the vanishing locus of s is an effective Cartier divisor D, $\mathcal{L} \cong \mathcal{L}(D)$, and there is an exact sequence

$$0 \to \mathcal{O}_X \to \mathcal{L} \to \mathcal{L}|_D \to 0.$$

As D is an Artinian scheme, $\mathcal{L}|_D$ is trivial as D is discrete, so by(6.12.2.6), $h^0(\mathcal{L}|_D) = \deg(D)$, and $h^0(X, \mathcal{O}_X) = 1$, so $r = h^0(X, \mathcal{L}) \leq d$.

If the equality holds, then $H^0(X, \mathcal{L}) \to H^0(X, \mathcal{L}|_D)$ is surjective, so to show $g(C) = 0$, it suffices to show that $h^0(X, \mathcal{L}) = 0$. As $\mathcal{L}|_D$ is trivial, there is a section t of $\mathcal{L}$ that generate $\mathcal{L}|_D$. Consider the exact sequence

$$0 \to \mathcal{L} \to \mathcal{L}^2 \to \mathcal{L}^2|_D \to 0,$$

$H^0(X, \mathcal{L}^2) \to H^0(X, \mathcal{L}|_D)$ is surjective because $\sigma \otimes t$ is mapped to σ. Then by(6.12.2.5),

$$h^0(X, \mathcal{L}^2) = 2r + 1 = \deg(\mathcal{L}^2) + 1.$$

So we may replace $\mathcal{L}$ by arbitrarily large powers of $\mathcal{L}$. Now $\mathcal{L}$ is ample by(6.12.2.20), so for r large, $H^1(X, \mathcal{L}^r) = 0$. □

Prop. (6.12.4.4) [Linear Series and Maps]. For any $\mathfrak{g}_d^r$ (L, V) on a non-singular precurve C, there is a map $\varphi : C \to \mathbb{P}^r$ and a map $\varphi^* \mathcal{O}_{\mathbb{P}^r}(1) \to \mathcal{L}$ s.t. the coordinates $T_0, \ldots, T_r$ are mapped to a basis of V.

This map is injective iff for any $p \neq q$, V_{p+q} has codimension 2. This map is an immersion iff for all p, V_{2p} has codimension 2. So in particular, this map is an embedding iff for any effective divisor D of degree 2, V_D has codimension 2. ⌟

Proof: Take a basis $s_0, s_1, \ldots, s_r \in V$, as C is non-singular, the image of the map $(s_0, \ldots, s_r) : \mathcal{O}_X^{r+1} \to \mathcal{L}$ is an invertible sheaf as it is torsion-free. Then take the corresponding embedding induced by(6.5.2.4). □

Cor. (6.12.4.5). If $\mathcal{L}$ is a very ample line bundle of degree d on a curve C, then $\varphi_{|\mathcal{L}|}$ embeds C as a closed subscheme of degree d. ⌟

Proof: Use(6.12.4.4), The pullback of $\mathcal{O}_{\mathbb{P}^r}(1)$ under φ is just $\mathcal{L}$, so the assertion follows from(6.12.2.7). □

Lemma (6.12.4.6). Let $\mathcal{L} \in \mathrm{Pic}^d(C)$ be general, then $h^0(\mathcal{L}) = \max\{1, d - g + 1\}$. ⌟

Proof: If $D = \sum p_i$ is a general effective divisor, notice $h^0(K) = g$, $h^0(K - p_1) = g - 1$, $h^0(K - p_1 - p_2) = g - 2$, and repeating this, we get $h^0(K - D) = \max\{0, g - d\}$, when we choose p_i that are as independent as possible(any section has f.m. zeros). Then by Riemann-Roch, $l(D) = d - g + 1 + \max\{0, g - d\} = \max\{1, d - g + 1\}$. As every divisor of degree $d \geq g$ is effective, this settles the $d \geq g$ case.

If D is non-effective and $d \leq g - 1$, we need to show W_d^0 is not dominant in Pic^d. But J has dimension g by**??**nd W_d^0 has dimension at most d, so this is true. □

Prop. (6.12.4.7). Suppose D is a divisor of degree $g + 3$, then for D general, $\varphi_D = \varphi_{|\mathcal{L}(D)|}$ is an embedding. ⌟

Proof: By(6.12.4.6), for a general D, $l(D) = 4$. Thus φ_D being not an embedding is equivalent to the existence of a divisor $D_0 = p+q$ that $l(D-D_0) \geq 3$. This means $D - D_0 \in W_{g+1}^2 = K - W_{g-3}^0$. So the divisor $D = D_0 + (D - D_0) \in W_2^0 + (K - W_{g-3}^0)$ which has dimension at most $2 + (g-3) = g-1$. But a general divisor D doesn't lie on this $g-1$-dimensional subvariety by(15.7.10.10), so a general D defines an embedding φ_D. □

Def. (6.12.4.8) [Canonical Map]. For a smooth curve C of degree g over a field k of genus $g \geq 1$, the canonical divisor $\mathcal{K}_C$ is basepoint-free, and defines a **canonical map** to $\mathbb{P}_k^{g-1}$. ⌟

Proof: By(6.12.2.2)(6.5.3.3)(6.1.5.26), it suffices to prove for $\overline{k}$, thus for any closed point p, $h^0(\mathcal{K}_C - p) = 2g - 3 - g + 1 + h^0(\mathcal{O}_C(p)) \leq g - 1 < h^0(\mathcal{K}_C) = g$ by(6.12.2.23), so it is basepoint-free. □

Prop. (6.12.4.9) [Base-Free Pencil Trick]. Let $\mathcal{L}, \mathcal{M}$ be line bundles on C. Let s_1, s_2 be sections of $H^0(\mathcal{L})$ without common zero, then the kernel of the map

$$s_1 H^0(\mathcal{M}) \oplus s_2 H^0(\mathcal{M}) \to H^0(\mathcal{L} \otimes \mathcal{M})$$

is $H^0(\mathcal{M} \otimes \mathcal{L}^{-1})$. ⌟

Proof: Indeed, there is an exact sequence of sheaves:

$$\mathcal{M} \otimes \mathcal{L}^{-1} \to \mathcal{M} \oplus \mathcal{M} \xrightarrow{(s_1,s_2)} \mathcal{M} \otimes \mathcal{L} \to 0.$$

Where the first map maps a section t to the pair $(ts_2, -ts_1)$. This is a Koszul regular sequence(on a common trivialization U of $\mathcal{M}, \mathcal{L}$, $s_1, s_2 \in C(U)$, thus this is just $0 \to A \to A \oplus A \xrightarrow{s_1,s_2} A \to 0$). Taking the global section functor gives the desired result. □

Prop. (6.12.4.10) [Geometric Riemann-Roch]. Let C be a non-hyperelliptic curve of genus $g \geq 2$. Then the canonical map φ_K is an embedding, so we can assume $C \subset \mathbb{P}^{g-1}$. Then for a divisor $D = \sum p_i$,

$$r(D) = d - 1 - \dim \overline{D},$$

where $\overline{D}$ is the linear subspace generated by p_i. Thus $r(D)$ can be interpreted as the number of linear relations between p_i. ⌟

Proof: By the definition of the canonical embedding, $l(K-D)$ is just the dimension of hypersurfaces containing p_i, thus it is equal to $g - 1 - \dim \overline{D}$. Now by Riemann-Roch, $r(D) = d - g + l(K - D) = d - g + g - 1 - \dim \overline{D} = d - 1 - \dim \overline{D}$. □

Prop. (6.12.4.11). ⌟

Cor. (6.12.4.12) [Special Divisors]. Let $U^{(g)}$ be the open subscheme of $C^{(g)}$ corresponding to the set of non-special divisors of degree g.**?** ⌟

Proof: □

Prop. (6.12.4.13) [Clifford Theorem]. For a divisor D of degree $0 \leq d \leq 2g-2$ on a curve of genus g,

$$r(D) \leq \frac{d}{2}.$$

with equality iff one of the following holds:

- $r = d = 0, D = 0$.
- $d = 2g-2, r = g-1, D = \mathcal{K}_C$.
- C is hyperelliptic and $D = mg^1_2$.

⌟

Proof: Cf.[Algebraic Curves, Harris, P32].**?** □

5 Hyperelliptic Curves

Def. (6.12.5.1) [Hyperelliptic Curves]. A **hyperelliptic curve** over k is a complete non-singular curve C together with a finite degree 2 map $C \to \mathbb{P}^1_k$. Such a map is called a **hyperelliptic map**. For $g > 0$, this is equivalen to the existence of a g^1_2 on C(such a linear series must be basepoint-free, by(6.12.2.24). ⌟

Cor. (6.12.5.2) [Genus 2 Curves are Hyperelliptic]. Any complete nonsingular curve of genus 2 is hyperelliptic, because $\mathcal{K}_C$ has degree 2 and $h^0(\mathcal{K}_C) = 2$(6.12.2.10). ⌟

Prop. (6.12.5.3) [Equation of Hyperelliptic Curves]. Any image of a hyperelliptic map from a hyperelliptic curve of genus g over an alg.closed field k of characteristic $k \neq 2$ is isomorphic to the projective curve that is the completion(6.12.1.18) of the affine curve in $\mathbb{A}^2$ defined in an affine chart by $y^2 = \prod_{i=0}^{2g+2}(x-\alpha_i)$ or $y^2 = \prod_{i=0}^{2g+1}(x-\alpha_i)$, depending on whether the ∞ is branched or not. And given $2g+2$ points in $\mathbb{P}^1_k$, there is exactly one degree 2 covering of $\mathbb{P}^1$ branched over these points. ⌟

Proof: Given any r points of $\mathbb{P}^1_k$, we can use a transformation of $\mathbb{P}^1$ to assume that all branch points are finite, denoted by $\alpha_1, \ldots, \alpha_r$. Consider the curve C' defined by $y^2 = \prod_{i=0}^{2g+2}(x-\alpha_i)$, then it is a smooth curve by Jacobian criterion. Now let C be the smooth model of C', and consider $\pi : C \to \mathbb{P}^1$ by projecting to the x-coordinates and extend to the whole C by(6.12.1.15). This is finite separable of degree 2, and π is simply branched at the points α_i, and simply branched over ∞ if r is odd, thus it has genus $\lfloor \frac{r-1}{2} \rfloor$ by Riemann-Hurwitz(6.12.1.32).

Conversely, by Riemann-Hurwitz(6.12.1.32), any degree 2 covering of $\mathbb{P}^1$ has $2g+2$ branch points, because the branch points must be simply branched. The map $k(x) \to k(C)$ is Galois of degree 2, take a $y \in k(C)$ that $\sigma(y) = -y$, then $y^2 = g \in k(x)$. We can modify y s.t. g is a monic polynomial with no repeated factors. Then it is of the form $g(x) = \prod_{i=1}^{r}(x-x_i)$. Then it is isomorphic to the curve constructed above, and branched over $x_1, \ldots, x_r$ and possibly ∞. In particular, it is determined by the set of branched points, so we get the desired assertion. □

Remark (6.12.5.4). The completion of C can be explicitly constructed, by gluing another affine chart defined by $(\frac{y}{x^{g+1}})^2 = \prod_{i=0}^{2g+2}(1-\alpha_i\frac{1}{x})$ or $(\frac{y}{x^{g+1}})^2 = \frac{1}{x}\prod_{i=0}^{2g+1}(1-\alpha_i\frac{1}{x})$. ⌟

Prop. (6.12.5.5). If C is a nonsingular complete curve of genus $g \geq 2$ over k and $\mathcal{L}$ is a line bundle that corresponds to a hyperelliptic map $C \to \mathbb{P}^1_k$, then $\mathcal{L}^{\otimes(g-1)} \cong \mathcal{K}_C$.

In particular, the image of C under the canonical map is the rational curve in $\mathbb{P}^{g-1}_k$. ⌟

Proof: Consider the composition of the hyperelliptic map and the Veronese map

$$C \xrightarrow{|\mathcal{L}|} \mathbb{P}^1_k \xrightarrow{v_{g-1}} \mathbb{P}^{g-1}_k,$$

which corresponds to the line bundle $|\mathcal{L}^{\otimes(g-1)}|$. This line bundle has degree $2g-2$, and the map $H^0(\mathbb{P}^{g-1}, \mathcal{O}(1)) \to H^0(C, \mathcal{L}^{\otimes(g-1)})$ is injective, because the Veronese map is non-degenerate. Thus $h^0(\mathcal{L}^{\otimes(g-1)}) \geq g$, thus isomorphic to $\mathcal{K}_C$, by(6.12.2.13). Hence this map is just the canonical map. □

Cor. (6.12.5.6). For a hyperelliptic curve, the smallest degree of an embedding $C \to \mathbb{P}^r$ is $g+r$. Note that hyperelliptic curves cannot be embedded into $\mathbb{P}^2$, i.e. smooth plane curves are non-hyperelliptic. ⌟

Proof: Firstly we show a special divisor cannot induce an embedding: A special divisor is a divisor that is contained in a hypersurface intersection of C under the canonical map, thus by geometric Riemann-Roch(6.12.4.10), $r(D)$ is just the number of points of D mapped to the same point under the canonical map, because intersection with the rational normal curve are all linearly independent. Now this means D contains g^1_2, so φ_D factors through π, thus not an embedding.**?** Cf.[Algebraic Curves, Harris, P21]. □

Prop. (6.12.5.7) [Hyperelliptic and Canonical Map]. A complete smooth curve of genus $g \geq 1$ is hyperelliptic iff the canonical map(6.12.4.8) is not a closed embedding. ⌟

Proof: The canonical map is not an embedding iff there exists an effective divisor D of degree 2 that $l(K-D) > l(K) - 2$. Now $l(K-D) = 2g-4-g+1+l(D)$, so this is equivalent to $l(D) > 1$, which is equivalent to a g^1_2, which is equivalent to hyperelliptic(6.12.5.1). □

Prop. (6.12.5.8) [Uniqueness of Hyperelliptic Maps]. For a hyperelliptic curve of genus $g \geq 2$, up to automorphic of $\mathbb{P}^1$, there are at most one hyperelliptic map, or equivalently there is exactly one g^1_2 on C.

But for (hyperelliptic)curve of genus 1, thus is not unique: any divisor of degree 2 is effective, but they are not unique, because $\mathrm{Pic}^2(C) \cong J(C)$(15.7.10.10). ⌟

Proof: If $\mathcal{L} \neq \mathcal{M}$ are two line bundles on C with $h^0 = 2$, then $h^0(\mathcal{L} \otimes \mathcal{M}) \geq 4$ by base-free pencil trick(6.12.4.9), and in fact $h^0(\mathcal{L} \otimes \mathcal{M}) = 4$ by(6.12.4.3). Now we can tun the same argument again to $\mathcal{L}$ and $\mathcal{L} \otimes \mathcal{M}$, to show that $h^0(\mathcal{L}^2 \otimes \mathcal{M}) = 6$. And inductively $h^0(\mathcal{L}^n \otimes \mathcal{M}) = 2n+2$. But then for n large, Riemann-Roch shows $2n+2 = 2n+2-g+1$, thus $g = 1$, contradiction. □

Gonal Curves

Def. (6.12.5.9) [Gonal Curves]. A **trigonal curve** is a complete non-singular curve C with a degree 3 map $C \to \mathbb{P}^1$. Similarly, a **k-gonal curve** is a complete non-singular curve C with a degree k map $C \to \mathbb{P}^1_k$. Being k-gonal is equivalent to having a basepoint-free g^1_k.

Notice also for non-hyperelliptic curves, any g^1_3 must be basepoint-free. ⌟

Def. (6.12.5.10) [Hurewitz Spaces]. Let the **Hurewitz space** be

$$\mathcal{H}_{d,g} = \{(C, f) | C \in \mathcal{M}_g, f : C \to \mathbb{P}^1 \text{ of degree } d \text{ with simple branching}\}.$$

In particular, $\mathcal{H}_{2,g}$ is just the space of hyperelliptic curves together with a hyperelliptic map. ⌟

Prop. (6.12.5.11) [Dimension of Hurewitz Spaces]. $\dim \mathcal{H}_{d,g} = 2d + 2g - 2$. ⌟

Proof: Let $b = 2d + 2g - 2$, then the branch divisor will consist of an unordered b-tuple of distinct points. Then we obtain a map $\mathcal{H}_{d,g} \to \mathbb{P}^b \backslash \Delta$, where we regard $\mathbb{P}^b$ as the set of polynomials of degree b and Δ the determinant, and the fiber is finite by cut-paste technique. □

Cor. (6.12.5.12) [Dimension of Moduli Space of Curves]. $\dim \mathcal{M}_g = 3g - 3$. ⌟

Proof: There is a map $\mathcal{H}_{d,g} \to \mathcal{M}_g$. When d is large, we can analyze the fiber of this map, that is, given a curve of genus g, how many simply branched maps $C \to \mathbb{P}^1$ of degree d are there? Such a map is equivalent to a line bundle of degree d and a pair of base free sections $\sigma_0, \sigma_1 \in H^0(L)$. The base-free condition is an open condition, thus the dimension of the fiber is $g + 2(d - g - 1) - 1 = 2d + g - 1$. Thus the dimension of $\mathcal{M}_g = 2d + 2g - 2 - (2d - g + 1) = 3g - 3$. □

Cor. (6.12.5.13). The space of hyperelliptic curves has dimension $2g - 1$. ⌟

Proof: $\mathcal{H}_{2,g}$ has dimension $2g+2$, and for any hyperelliptic curve, there is exactly one hyperelliptic map up to automorphism of $\mathbb{P}^1$, by(6.12.5.8), thus the space of hyperelliptic curves has dimension $2g + 2 - 3 = 2g - 1$. □

Cor. (6.12.5.14). If $g \geq 3$, then not all curves of genus g is hyperelliptic. ⌟

Proof: Because when $g \geq 3$, $2g - 1 < 3g - 3$. □

Lemma (6.12.5.15). For a line bundle of degree 3 on a curve of genus $g \geq 3$, $h^0(L) \leq 2$, by Clifford's theorem(6.12.4.13). Thus a trigonal map must be associated to a complete linear series g^1_3. ⌟

Prop. (6.12.5.16) [Hyperelliptic are not Trigonal]. A curve of genus $g \geq 3$ cannot be both hyperelliptic and trigonal. ⌟

Proof: Suppose there are two basepoint-free line bundles $\mathcal{L}, \mathcal{M}$ of degree 2 and 3 on C that $h^0(\mathcal{L}) = h^0(\mathcal{M}) = 2$(6.12.5.15), then the base-free pencil trick(6.12.4.9) implies that $h^0(\mathcal{M} \otimes \mathcal{L}) \geq 4$. If $g = 3$, then this contradicts Riemann-Roch. If $g \geq 4$, then this contradicts Clifford's theorem(6.12.4.13). □

Prop. (6.12.5.17) [Genus 3 Curves are Hyperelliptic or Trigonal]. Any genus 3 non-hyperelliptic complete smooth curve C with a rational point is trigonal. ⌟

Proof: If C is non-hyperelliptic, then the canonical map realizes C as a plane curve of degree 4(6.12.8.6), thus the projection of C along a point on C induces a map $C \to \mathbb{P}^1$. This map is finite of degree 3 because it is non-constant as C is non-degenerate, and has degree 3, by(6.12.2.28). □

Prop. (6.12.5.18) [Uniqueness of Trigonal Divisors]. There exists at most one g^1_3 on a curve of genus $g \geq 5$. ⌟

Proof: If $\mathcal{L} \neq \mathcal{M}$ are two base free line bundles of degree 3 that $h^0 = 2$, then we can use base-free trick to show that $h^0(\mathcal{L} \otimes \mathcal{M}) = 4$. But this contradicts Clifford's theorem(6.12.4.13). Notice the equality cannot hold, because the degree is too low to be the canonical bundle, and also C cannot be both hyperelliptic and trigonal(6.12.5.16). □

6 Castelnuovo's Theory

Lemma (6.12.6.1) [Castelnuovo's Lemma]. Let $\Gamma \in \mathbb{P}^n$ be a configuration of $d \geq 2n + 3$ points in linear general position, and if $h_\Gamma(2) = 2n + 1$, then Γ lies in a rational normal curve. ⌟

7 Plucker Formulas

Def. (6.12.7.1) [Weierstrass Group]. Let C be a smooth of genus $g \geq 2$, $p \in C$, then $S_p = \{-\operatorname{ord}_p(f) | f \in H^0(\mathcal{O}_C(-p))\}$ is a semigroup, called the **Weierstrass semigroup** of $p \in C$. And the **gap sequence** is $\mathbb{N} \backslash S_p$, which is the set of orders of pole of p that doesn't occur. ⌟

Lemma (6.12.7.2). We have $|G_p| = g$. ⌟

Proof: Notice that

$$G_p = \{m : h^0(mp) = h^0((m-1)p)\}, \quad S_p = \{m : h^0(mp) = h^0((m-1)p) + 1\}$$

and we know by(6.12.2.12) that $h^p(mp) = m - g + 1$ for m large, thus there are exactly g jumps, which shows $|G_p| = g$. □

Def. (6.12.7.3)[Weierstrass Points]. A point $p \in C$ is called **Weierstrass point** if the gap sequence is not $\{1, 2, \ldots, g\}$. It is called a **hyperelliptic Weierstrass point** if $G_p = \{1, 3, \ldots, 2g-1\}$, and is called a **normal Weierstrass point** if $G_p = \{1, 2, 3, \ldots, g-1, g+1\}$.

Define the **weight** of the $p \in C$ to be the sum $w(p) = \sum_{i \leq g}(a_i - i)$, where the gap sequence is numbered $\{a_1, \ldots, a_g\}$. ⌟

Prop. (6.12.7.4). For any compact Riemann surface C, $\sum_{p \in C} w(p) = g(g-1)(g+1)$. ⌟

Proof: Cf.[**?**], P274. □

Cor. (6.12.7.5). For general $p \in C$, $G_p = \{1, 2, \ldots, g\}$. ⌟

Prop. (6.12.7.6)[Hyperelliptic Weierstrass Points]. If C is hyperelliptic defined by $y^2 = \prod_{i=0}^{2g+1}(x - \alpha_i)$, then there are $2g+2$ branching point of x, where $S_p = \{0, 2, 4, \ldots, 2g, 2g+1, \ldots\}$. In this way, $w(p) = g(g-1)/2$. Thus there are $2g+2$ Weierstrass points, and these are all of them.

If C is non-hyperelliptic, then by Clifford's theorem(6.12.4.13),

$$h^0(kp) < \frac{k}{2} + 1, k = 1, \ldots, g$$

Thus $h^0((a_i - 1)p) < \frac{a_i - 1}{2} + 1$, and $h^0((a_i - 1)p) = 1 + (a_i - 1) - (i - 1)$. Thus we get

$$a_i \leq 2i - 2, i = 2, \ldots, g.$$

Then $w(p) \leq \sum_{i=2}^{g}(i-2) = \frac{(g-1)(g-2)}{2}$. Thus there are at least

$$\frac{2g(g-1)(g+1)}{(g-1)(g-2)} \geq 2g + 6$$

Weierstrass points.

To sum up, there are no less than $2g+2$ Weierstrass points, and there are exactly $2g+2$ Weierstrass points iff C is hyperelliptic. ⌟

Prop. (6.12.7.7). A generic Riemann surface of genus $g \geq 3$ has no automorphisms. ⌟

8 Curves of Low Genus

In this subsection complete smooth curves of low genus are considered.

Prop. (6.12.8.1) [Genus 0 Curve]. All smooth complete curve C of genus 0 is isomorphic to a plane conic. ⌟

Proof: The curve has a degree 2 line bundle $\mathcal{K}_C^\vee$, thus by Riemann-Roch $h^0(\mathcal{O}(p)) = 3$ and by(6.12.2.26) it induces a closed embedding of C into $\mathbb{P}^2$ of degree 2, thus it is a plane conic. □

Prop. (6.12.8.2). A nonsingular curve C of genus 0 with a k-rational point p is isomorphic to $\mathbb{P}^1_k$: ⌟

Proof: By Riemann-Roch, $h^0(\mathcal{O}(p)) = 2$ and $\deg \mathcal{O}(p) = 1$, thus by(6.12.2.26), $\mathcal{O}(p)$ defines a closed embedding of C into $\mathbb{P}^1$, which must be an isomorphism. □

Prop. (6.12.8.3) [Genus 1 Curve]. By(6.12.2.26), an effective divisor of degree 3 induces an embedding of $\mathbb{C}$ into $\mathbb{P}^2$, So it is a smooth plane cubic by genus formula(6.12.2.33). Conversely, any smooth plane cubic has genus 1.

Similarly, if we take an effective divisor of degree 4, then it gives an embedding $C \to \mathbb{P}^3$. We know that $h^0(\mathcal{O}_{\mathbb{P}^3}(2)) = 10$ and $h^0(\mathcal{O}_C(2)) = 8$, thus C is contained in 2 quadrics. Then C is the intersection of these two quadrics, by Bezout's theorem. ⌟

Prop. (6.12.8.4) [Genus 2 Curves and Degree 4 Divisors]. Let C be a curve of genus 2, and D a divisor of degree 4. Then $l(D - K_C) = 1 + l(2K_C - D) \geq 1$, thus $D - K_C$ is effective. Let $D - K_C = p + q$. Then φ_D maps p, q to the same point.

There are two situations, firstly if $D \neq 2K_C$, then $D - K_C$ can be written uniquely as $p + q$. Then the image of φ_D is a degree 4 curve with a node(if $p = q$) or a cusp(if $p = q$). Counting genus, this has exactly arithmetic genus 2.

If $D = 2K_C$. Then notice φ_{2K_C} is equal to φ_K followed by the normal curve map $\mathbb{P}^1 \to \mathbb{P}^2$. This is because if ω_1, ω_2 are a basis of $H^0(K_C)$, then $\omega_1^2, \omega_1\omega_2, \omega_2^2$ is a basis of $H^0(K_C^2)$. So φ_D is a 2 to 1 map to a rational normal curve in $\mathbb{P}^2$. ⌟

Prop. (6.12.8.5) [Genus 2 Curve and degree 5 Divisors]. Let C be a curve of genus 2 and D a divisor of degree 5, then $\varphi_D : C \to \mathbb{P}^3$ embeds C as a degree 5 curve, by(6.12.2.26).

Notice $h^0(\mathcal{O}_{\mathbb{P}^3}(2)) = 10$ and $h^0(\mathcal{O}_C(2)) = 10 - 2 + 1 = 9$, thus C lies on at least one quadric Q. And it can in fact lie on only one quadric, because if it lies on two quadrics, then C is the intersection, and can have degree at most 4.

Next, notice $h^0(\mathcal{O}_{\mathbb{P}^3}(3)) = 20$ and $h^0(\mathcal{O}_C(3)) = 15 - 2 + 1 = 14$, so C lies on at least 6 cubics. Without the 4 cubics containing the quadric, there are still at least 2 new cubics. Let S be such a cubic, then $S \cap Q$ is a curve of degree 6, so $S \cap Q = C \cup L$, where $L \cong \mathbb{P}^1$. ⌟

Prop. (6.12.8.6) [Genus 3 Non-Hyperelliptic Curve]. For any non-hyperelliptic smooth curve C of genus 3 over a field k, the canonical map(6.12.4.8) embeds C as a smooth quartic curve in $\mathbb{P}^2$. This induces an isomorphism of smooth quartic plane curves up to automorphism of $\mathbb{P}^2$. ⌟

Proof: The canonical embedding is a closed embedding by(6.12.5.7). For the last assertion, any plane curve of degree 4 has genus 3 by(6.12.2.33), and the sheaf $\mathcal{O}_C(1)$ has degree 4 and 3 sections, thus by(6.12.2.13), so this comes from a canonical embedding. In particular, any such curve can be embedded in $\mathbb{P}^2$ in a unique way. □

Prop. (6.12.8.7). Any hyperelliptic smooth curve of genus 3 is a flat limit of non-hyperelliptic smooth curves of genus 3. ⌟

Proof: Cf.[Vak17]P520. □

Prop. (6.12.8.8) [Genus 4 Non-Hyperelliptic Curves]. Any non-hyperelliptic smooth complete canonical curve C of genus 4 is a complete intersection of a quadric surface and a cubic surface. Conversely, any regular complete intersection of a quadric surface and a cubic surface is a canonically embedded non-hyperelliptic curve of genus 4. ⌟

Proof: Looking at the map $H^0(\mathcal{O}_{\mathbb{P}^3}(2)) \to H^0(\mathcal{O}_C(2))$, we see C lies on a unique quadric Q(uniqueness follows from Bezout's theorem and(6.7.3.11), by the same reason as(6.12.8.5)).

Next looking at the map $H^0(\mathcal{O}_{\mathbb{P}^3}(3)) \to H^0(\mathcal{O}_C(3))$, then the kernel has dimension at least 5, thus there is a cubic containing C but not Q. Then $S \cap Q$ is a complete intersection of degree 6 containing C, also it has the same arithmetic genus as C(6.7.3.8), thus the same Hilbert polynomial(linear function), so $C = S \cap Q$ by(6.7.3.11)s. Conversely, any smooth curve of the form $S \cap Q$ is a canonical curve of genus 4, by adjunction formula($\mathcal{K}_C = \mathcal{O}_C(1)$ has degree 6).

Conversely, for any smooth complete intersection of a quadric surface and a cubic surface has arithmetic genus 4 by(6.7.3.8), $\mathcal{O}_C(1)$ has degree 6 and $h^0(\mathcal{O}_C(1)) \geq 4$ because C is non-degenerate: there are no smooth plane curve of genus 4.

Now if Q is non-singular, then C is of type $(3,3)$ in Q, thus the two projections are two trigonal map from C to $\mathbb{P}^1$, and if Q is a cone, the projection from the vertex is a trigonal map from C to $\mathbb{P}^1$. □

Prop. (6.12.8.9) [Non-Hyperelliptic Curve of Genus ≥ 5]. For a non-hyperelliptic curve C of genus 5, we have a canonical map $\varphi : C \to \mathbb{P}^4$. Firstly we consider what quadrics C lies on: $h^0(\mathcal{O}_{\mathbb{P}^4}(2)) = 15$ and $h^0(\mathcal{O}_C(2)) = 12$, so C lies on at least 3 quadrics. There are two cases:

1. $C = \cap Q_i$ where Q_i are the quadrics containing C.
2. C is a strict subset of $\cap Q_i$.

which corresponds to non-trigonal and trigonal curves. ⌟

Proof: The case 1 does occur, because by Bertini's theorem(6.6.4.29), for general three quadrics Q_i, $\cap Q_i$ is a smooth curve, and thus $\mathcal{K}_C = (\mathcal{K}_{\mathbb{P}^4}(-5+2+2+2))|_C = \mathcal{O}_C(1)$. So $d = 8, g(C) = 5$.

In this case, C is not trigonal, because if C is trigonal, then C has a g^1_3, which means C has three colinear point. Then all the quadrics Q_i must contain this line, contradiction.

The case 2: Cf.[Algebraic Curves, Harris, P24].**?** This case corresponds to trigonal curves. □

Prop. (6.12.8.10) [Non-Hyperelliptic Curve of Genus 5 is Tetragonal]. Let C be a canonical embedded curve which is not trigonal admits a map of degree 4 to $\mathbb{P}^1$. ⌟

Proof: Let $\mathbb{P}^2 = \{Q | C \subset Q\}$. We can ask there are singular quadrics in this set. Inside $\mathbb{P}^{14}$ which is the space of all quadrics in $\mathbb{P}^4$, there is a quintic hypersurface of singular quadrics. **?** For the rest, Cf.[Algebraic Curves, Harris, P25]. □

Prop. (6.12.8.11). If $C \subset \mathbb{P}^{g-1}_k$ is a canonical smooth curve of genus $g \geq 6$, then C is not a complete intersection. ⌟

Proof:

□

Correspondences

Complex Tori and Algebraic Varieties

9 Castelnuovo Theory

10 Brill-Noether Theory

11 Relative Curves

Def. (6.12.11.1) [Relative Curves]. Let $S \in \mathcal{S}\mathrm{ch}$, a **smooth curve** over S is a smooth morphism $C \to S$ of relative dimension 1 that is separated and of f.p.. ⌟

Prop. (6.12.11.2). Let $S \in \mathcal{S}\mathrm{ch}$ and C a smooth curve over S, then ⌟

6.13 K3 Surfaces

References are [Lectures on K3 Surfaces Huybrechts].

7 Algebraic Geometry II: Spectral Algebraic Geometry

7.1 Andre-Quillen-Cohomology

Basic references are [Andre-Quillen Cohomology of Commutative Algebras Iyenger]. See also [Quillen Cohomology of Commutative Rings] and [Quillen On the (Co-)homology of Commutative Rings]. [Smoothness, Regularity and Complete Intersections] is a must read.

1 Naive Cotangent Complex

This subsection is obsolete.

Prop. (7.1.1.1) [Polynomial Replacement]. For a morphism of ring morphisms $(R \to S) \to (R' \to S')$, let α, α' be two presentations, then there exists morphism of presentations, and different morphisms induce homotopic maps $NL_{S/R} \to NL_{S'/R'}$. ⌟

Proof: Cf.[[Sta]00S1]. In fact, any surjective formally smooth representation will give the naive cotangent complex, up to quasi-isomorphism(7.1.1.4). □

Cor. (7.1.1.2). If $A = R[X_i]$ be a polynomial algebras, then $NL_{A/R}$ is homotopic to $(0 \to \Omega_{B/A})$ because $A \to A$ is a presentation with zero kernel.

If $R \to A$ is surjective with kernel I, then $NL_{A/R}$ is homotopic to $(I/I^2 \to 0)$. ⌟

Lemma (7.1.1.3) [Formally Smooth Replacement 1]. If $A \to B$ is a ring map that has two surjective presentations $C \to B, D \to B$ with kernels I, J. If there is a map $C \to D$ commutating these two presentation, D formally smooth, and $C \to D$ is surjective or C is formally smooth, then their corresponding naive cotangent complexes are quasi isomorphic. ⌟

Proof: Cf.[Foundations of Perfectoid Geometry P123]. □

Prop. (7.1.1.4) [Formally Smooth Replacement 2]. If B is an A-algebra that has two formally smooth presentation $C \to B, D \to B$ with kernels I, J. then their corresponding naive cotangent complexes are quasi isomorphic. ⌟

Proof: It suffices to prove they are both quasi isomorphic to the canonical cotangent complex. For this, we first consider the diagram $\begin{array}{ccc} D & \longrightarrow & C \\ \downarrow & & \downarrow \\ A[B] & \longrightarrow & B \end{array}$, where $D = A[S]$ and $S = C \coprod A[B]$ as sets. The two map $D \to A[B]$ and $D \to A[B]$ can be chosen because $C \to B$ is surjective. So the results follows from(7.1.1.3). □

Prop. (7.1.1.5) [Jacobi-Zariski Sequence]. Let $A \to B \to C$ be a ring map. Choose a presentation $\alpha : P \to B$ for B/A with kernel I, a presentation $\beta : Q \to C$ for C/B with kernel J, a presentation $\gamma : R \to C$ for the induced representation C/A with kernel K, then there is an exact sequence of complexes:

$$\begin{array}{ccccccccc} & & I/I^2 \otimes_B C & \longrightarrow & K/K^2 & \longrightarrow & J/J^2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Omega_{P/A} \otimes_B C & \longrightarrow & \Omega_{R/A} \otimes C & \longrightarrow & \Omega_{Q/B} \otimes C & \longrightarrow & 0 \end{array}$$

Applying snake lemma, we get

$$H_1(NL_{B/A} \otimes_B C) \to H_1(L_{C/A}) \to H_1(L_{C/B}) \to C \otimes_B \Omega_{B/A} \to \Omega_{C/A} \to \Omega_{C/B} \to 0.$$

⌟

Proof: Cf.[[Sta]00S2]. □

Prop. (7.1.1.6) [Localization]. Let $A \to B$ be a ring map, for a multiplicative set S of B, we have $NL_{B/A} \otimes_B S^{-1}B$ is quasi-isomorphic to $NL_{S^{-1}B/A}$. ⌟

Proof: Because it commutes with colimit, it suffice to prove for $S = f$, and this is the content of lemma(7.1.1.7) below. □

Lemma (7.1.1.7). If $A \to B$ is a ring map and $\alpha : P \to B$ is a presentation of B with kernel I, then $\beta : P[X] \to B_g : X \to 1/g$ is a presentation of B_g with kernel $J = I + (gX - 1)$. Then we have

- $J/J^2 = (I/I^2)_g \oplus B_g(fX - 1)$.
- $\Omega_{P[X]/A} \otimes_{P[X]} B_g = \Omega_{P/A} \otimes_P B_g \oplus B_g dX$.
- $NL(\beta) \cong NL(\alpha) \otimes_B B_g \oplus (B_g \xrightarrow{g} B_g)$.

Hence $NL_{B/A} \otimes_B B_g \to NL_{B_g/A}$ is a homotopy equivalence. ⌟

Proof: Cf.[[Sta]08JZ]. □

2 Cotangent Complex

Def. (7.1.2.1) [Cotangent Complex]. The adjunction of $A \ltimes -$ and $A \otimes_- \Omega_{-/R}$(5.4.3.5) extends to an adjunction between $(sCAlg_R)_{/A}$ and $s\mathcal{M}od_A$. Theses categories are model categories by(5.8.2.11)(5.8.2.14) and(4.5.4.1), and $A \ltimes -$ preserves all weak equivalences and fibrations, so it is a Quillen adjunction(4.5.2.1). Then the **cotangent complex** $L_{A/R}$ as a simplicial A-module is defined to be the total left derived functor applied to the trivial simplicial algebra A. Equivalently, it is

$$L_{A/R} = A \otimes_X \Omega_{X/R}$$

where X is a cofibrant replacement(4.5.1.12) of A.

Because of the Dold-Kan equivalence, we sometimes also call $NL_{A/R}$ the cotangent complex. ⌟

Def. (7.1.2.2) [André-Quillen Homology and Cohomology]. The **André-Quillen homology** is defined to be

$$D_q(A/R) = \pi_q(L_{A/R}) = H_q N(L_{A/R})(5.8.2.2).$$

More generally, if M is an A-module, then let

$$D_q(A/R, M) = \pi_q(L_{A/R} \otimes_A M).$$

The **André-Quillen cohomology** is defined to be

$$D^q(A/R, M) = \mathrm{Ext}^n(NL_{A/R}, M).$$

⌟

Prop. (7.1.2.3) [Functoriality]. The cotangent complex is functorial in arrows $R \to A$: If there is a commutative diagram

$$\begin{array}{ccc} R & \longrightarrow & S \\ \downarrow & & \downarrow \\ A & \longrightarrow & B \end{array}$$

then there is a natural morphism $L_{A/S} \otimes_A B \to L_{B/R}$. This is because if X is a cofibrant replacement for A, then $X \otimes_R S$ is also cofibrant object, because $B \otimes_A -$ is a Quillen adjunction, by(5.8.2.15), then it factors through $X \otimes_R S \to Y \to B$ where Y is a cofibrant replacement of B, thus Y is also cofibrant. Then the functor $L_{A/S} \otimes_A B \to L_{B/R}$ is induced by

$$B \otimes_A (A \otimes_X \Omega_{X/R}) \to B \otimes_Y \Omega_{Y/S}.$$

The formation of Kähler differential commutes with arbitrary colimit as it is a left adjoint, so the formation of cotangent complex commutes with filtered colimits, both in A and B. Especially, it commutes with taking stalks, hence the sheaf of cotangent complexes of a map between schemes can be constructed as in the case of Kähler differentials, and it is a Qco sheaf. ⌟

Def. (7.1.2.4) [Canonical Resolution]. By the Dold-Kan correspondence, we will say that two simplicial A-modules are quasi-isomorphic iff their normalized nerves are quasi-isomorphic. Then $P_A(B) \to B$ is a quasi-isomorphic resolution of B, where B is the trivial complex. ⌟

Proof: There is a homotopy d between id and 0 for $n \leq 0$, where

$$d_n : F(GF)^n G(B) \to F(FG)^n \circ GFG(B)$$

using counit map, and on degree $0, -1$, it is $A[A[B]] \xrightarrow{\partial_1 - \partial_2} A[B] \to B \to 0$, which is clearly 0, so this is a zero map.

Thus $Tot(P_A(B)) \cong B$, and $N_*(A) \cong Tot(A)$ by Dold-Kan correspondence, so we are done. □

Cor. (7.1.2.5).

$$D_0(L_{B/A}, M) = \Omega_{B/A} \otimes M, \quad D^0(A/R, M) = \mathrm{Der}_R(A, M)$$

by the generator-relation definition of Kähler differential. ⌟

Prop. (7.1.2.6) [The fundamental Distinguished Triangle]. If $\mathcal{T}$ is a site and $A \to B \to C$ are morphisms of sheaves of rings over $\mathcal{T}$, then there is a morphism of simplicial A-modules that corresponds to distinguished triangles in $D^{\leq 0}(C)$ via Dold-Kan correspondence:

$$L_{B/A} \otimes^L_B C \to L_{C/A} \to L_{C/B}.$$

In particular, if M is a B-module, then there are long exact sequences

$$\ldots \to D_1(A/R, M) \to D_1(B/R, M) \to D_1(B/A, M) \to M \otimes_A \Omega_{A/R} \to M \otimes_A \Omega_{B/A} \to M \otimes_B \Omega_{B/A} \to 0$$

$$\ldots \to D^1(A/R, M) \to D^1(B/R, M) \to D^1(B/A, M) \to \mathrm{Der}_R(A, M) \to \mathrm{Der}_A(B, M) \to \mathrm{Der}_A(B, M) \to 0$$

⌟

Proof: Choose a simplicial resolution $X \to A$ where X is free, then we factor the morphism $X \to A \to B$ to get a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{i} & Y \\ \downarrow & & \downarrow \\ A & \longrightarrow & B \end{array}$$

where i is free, then we have an exact sequence(in $Ch_{\geq 0}(R)$ via Dold-Kan) of simplicial modules

$$0 \to B \otimes_X \Omega_{X/R} \to B \otimes_Y \Omega_{Y/R} \to B \otimes_Y \Omega_{Y/X} \to 0$$

because each $X_n \to Y_n = X_n \otimes \bigoplus_{\varphi:[n]\twoheadrightarrow[k]} \varphi^* P_k$ has a retraction, and use(5.4.3.7).

Notice we have a simplicial map $A \otimes_X Y \to B$ which is a weak equivalence and $A \otimes_X Y$ is a free simplicial A-algebra. Then it suffices to note that $X_n \to Y_n = X_n \otimes \bigoplus_{\varphi:[n]\twoheadrightarrow[k]} \varphi^* P_k$ is projective implies

$$B \otimes_Y \Omega_{Y/X} \cong B \otimes_{A\otimes_X Y} \Omega_{A\otimes_X Y/A}$$

, and $\Omega_{X/R}$ is termwise projective. □

Prop. (7.1.2.7) [Properties of Cotangent Complexes].

- If $B = s(P)$ where P is a projective A-module, then $L_{B/A}$ is weakly equivalent to $\Omega^1_{P/A}[0]$.
- (Kunneth Formula) If B, C are Tor independent over A, then

$$L_{B\otimes C/A} \cong (L_{B/A} \otimes_A C) \oplus (L_{C/A} \otimes_A B).$$

- (Flat Base Change)If B, C are Tor independent over A, $L_{B/A} \otimes_A C \cong L_{B\otimes_A C/C}$.

⌟

Proof:

- $S_R(P)$ is already cofibrant in $(sCAlg_R)_{/A}$.
- Let $X \to B, Y \to C$ be cofibrant replacement of A, B respectively, then $X \otimes_R Y \to B \otimes_A C$ is a cofibrant replacement, as $X \otimes_A Y$ is cofibrant, and Tor independence shows

$$\pi_*(X \otimes_A Y) = \pi_*(X) \otimes_A \pi_*(Y) = B \otimes_A C.$$

  thus the result follows from(5.4.3.6).
- The same as Künneth formula, noticing that $X \otimes_A C \to B \otimes_A C$ is a weak equivalence by Tor independence, and $X \otimes_A C$ is cofibrant.

□

3 Relations with Algebraic Properties

Cf.[Andre-Quillen Homology].

Prop. (7.1.3.1) [Acyclicity for Smooth Algebras]. If $A \to B$ is smooth, then $L_{B/A} \cong \Omega^1_{B/A}[0]$. In particular, if $A \to B$ is étale, then $L_{B/A} = 0$, and $L_{C/A} \cong L_{B/A} \otimes_B C$, by distinguished triangle(7.1.2.6). ⌟

Proof: The cotangent complex is local, so we may assume it is standard smooth, so it factors as $A \to A[X_1, \ldots, X_k] \xrightarrow{g} B$, where g is étale, so using the distinguished triangle and polynomial case, the result follows. □

Prop. (7.1.3.2) [Compatibility with p-adic Completion]. If A is a p-adically complete commutative ring with bounded p-torsion and B is a flat A-module, then B also has bounded p^∞-torsion by(5.9.2.4), let $\widehat{B}$ be the p-adic completion of B, then the cotangent complex $L_{\widehat{B}/B}$ vanishes after derived p-completion.

In particular, by the distinguished triangle(7.1.2.6), if B is a smooth algebra, then $L_{\widehat{B}/A} \cong \Omega^1_{\widehat{B}/A}$ is a finite projective $\widehat{B}$-module. ⌟

Proof: This is true after base change $- \otimes^L_A A/p$ by flat base change(7.1.2.7),(5.9.7.4) and derived Nakayama(5.9.6.10). □

4 Deformations

Prop. (7.1.4.1) [Topological Invariance of Étale Site]. Let A be a ring, consider the following category: $\mathcal{C}_A$ of flat A-algebras B that $L_{B/A} = 0$, then if $\widetilde{A} \to A$ is surjective with locally nilpotent kernel, then the base change defines an isomorphism of categories $\mathcal{C}_{\widetilde{A}} \cong \mathcal{C}_A$.

By(7.1.2.7), $L_{B/A}$ vanish is equivalent to being étale, thus the properties characterize the invariance of étale site under infinitesimal thickening. ⌟

Proof: ? □

Prop. (7.1.4.2) [Relative Perfect Case]. If A is a ring of char$p$ and B is an A-algebra which is relatively perfect, i.e. $B^{(1)} = B \otimes_{A,\mathrm{Frob}} A \to B$ is an isomorphism, then $L_{B/A} = 0$. ⌟

Proof: Notice for any A-algebra C, the relative Frobenius induces zero map $L_{C^{(1)}/A} \to L_{C/A}$, because by using the canonical polynomial resolution, $d(x^p) = px^{p-1}xs = 0$. Now the relative Frobenius is an isomorphism $B^{(1)} \to B$, thus induces an isomorphism $L_{B^{(1)}/A} \to L_{B/A}$ by Functoriality, thus $L_{B/A} = 0$. □

Cor. (7.1.4.3) [Witt Vector Construction]. There is an equivalence of categories of $\mathcal{C}_n$ = flat $\mathbb{Z}/p^n$-algebras that A/p is perfect and $\mathcal{C}_1$ = perfect rings over $\mathbb{Z}/p$.

moreover, taking limit, this is even equivalent to the category of flat p-adically complete $\mathbb{Z}_p$ algebras that A/p is perfect. Which is just the construction of Witt vectors. ⌟

Proof: It suffices to show that $\mathcal{C}_n \subset \mathcal{C}_{\mathbb{Z}/p^n}$: By(7.1.4.2) and flat base change(7.1.2.7), $L_{A/(\mathbb{Z}/p^n)} \otimes_{\mathbb{Z}/p^n} \mathbb{Z}/p \cong L_{(A/p)/(\mathbb{Z}/p)} = 0$, so $L_{A/(\mathbb{Z}/p^n)} \otimes_{\mathbb{Z}/p^n} \mathbb{Z}/p^k \cong 0$ by induction, and so $L_{A/(\mathbb{Z}/p^n)} \cong 0$.

For the last assertion, it is flat because it is torsion-free, which is because if $p(x_n) = 0$, then by $0 \to p^n\mathbb{Z}/p^{n+1} \to \mathbb{Z}/p^{n+1} \xrightarrow{p} \mathbb{Z}/p^n \to 0$ and the flatness of A_{n+1}, $x_{n+1} \in p^n A_{n+1}$, thus $x_n = 0$, and $x = 0$. □

Prop. (7.1.4.4) [Adjointness of Witt Vectors]. Using a more careful analysis of cotangent complex(embedded deformation), we can show that if $A \to B \in \mathcal{C}_A$ and there is a infinitesimal deformation $C \to C'$ of A-algebra, then a map $B \to C'$ can be lifted to an A-algebra map $A \to C$.

In particular, taking inverse image, we get that

$$\mathrm{Hom}_{\mathbb{F}_p}(A, B/p) \cong \mathrm{Hom}_{\mathcal{CRing}_{\mathbb{Z}_p}}(W(A), B).$$

which is the usual adjointness of the Witt vector construction. ⌟

5 Algebra Extension

Cf.[Perfectoid Geometry Appendix B].

Def. (7.1.5.1) [Algebra Extensions]. Let $A \to B$ be a ring map and M be a B-module, then an **A-algebra extension** of B by M is a short exact sequence of A-modules $0 \to M \to B' \to B \to 0$ that B' is an A-algebra with M being an ideal of it.

The set of such extensions are denoted by $\mathrm{Exal}_A(B, M)$. ⌟

Prop. (7.1.5.2). $\mathrm{Exal}_A(B, M)$ is a group under Baer sum, where the sum of two extension is the extension given by pushout, i.e. $(B_1 \oplus B_2)/\{(m, -m)|m \in M\}$. Moreover, it is a B-module, where the multiplication is the pushout along multiplication of b on M. ⌟

Prop. (7.1.5.3). There is a trivial extension given by $D_B(M) = B \oplus M$(5.4.3.5), and the automorphism of $D_B(M)$ is isomorphic to $\mathrm{Der}_A(B, M)$ via $d \mapsto \mathrm{id} \oplus d$. ⌟

Proof: Cf.[Foundations of Perfectoid Spaces Masullo P118]. □

Prop. (7.1.5.4). Let $A \to B \to C$ be ring maps, then for any C-module M, there is an exact sequence

$$0 \to \mathrm{Der}_B(C, M) \to \mathrm{Der}_A(C, M) \to \mathrm{Der}_A(B, M) \xrightarrow{\partial} \mathrm{Exal}_B(C, M) \to \mathrm{Exal}_A(C, M) \to \mathrm{Exal}_A(B, M)$$

functorial in M. Where ∂ is given by(7.1.5.3). ⌟

Proof: Cf.[Foundations of Perfectoid Spaces Masullo P119]. □

Prop. (7.1.5.5). Let $A \to B$ be a ring map or a map of sheaves of rings, and let M be a B-module, then there is an isomorphism of B-modules that is natural in M:

$$\mathrm{Exal}_A(B, M) = \mathrm{Ext}^1_B(NL_{B/A}, M).$$

⌟

Proof: Cf.[Foundations of Perfectoid Spaces, P127]. □

Infinitesimal Deformation

Def. (7.1.5.6). An **infinitesimal deformation** of a f.g. k-algebra is defined as a algebra A' flat over $D = k[t]/(t^2)$ that $A' \otimes_D k = A$.

A f.g. k-algebra is called **rigid** if it has no infinitesimal deformations. ⌟

Prop. (7.1.5.7). Let A be a f.g. k-algebra, write A as a quotient of a polynomial ring over k with kernel J, then there is an exact sequence $J/J^2 \to \Omega_{P/k} \otimes_P A \to \Omega_{A/k} \to 0$ by(5.4.3.7), then we apply $\mathrm{Hom}_A(-, A)$ and let $T^1(A) = \mathrm{Coker}(\mathrm{Hom}_A(\Omega_{P/k} \otimes_A A, A) \to \mathrm{Hom}_A(J/J^2, A))$. Then $T^1(A)$ parametrize infinitesimal deformations of A. ⌟

7.2 Spectral Algebraic Geometry(Lurie)

Main references are Lurie's work, [Derived Algebraic Geometry, Thesis, Lurie].

Notation (7.2.0.1).
- Use notations from Derived Commutative Algebras.

⌟

Prop. (7.2.0.2) [$\mathcal{D}_{\mathcal{QC}oh}(\operatorname{Spec} R)$]. For $R \in \mathcal{CR}ing$, there exists a unique sheaf of ∞-categories $\mathcal{D}_{\mathcal{QC}oh}$ on $\operatorname{Spec} R$ s.t. for any affine open subset U,

$$\mathcal{D}_{\mathcal{QC}oh}(U) = \mathcal{D}(\mathcal{O}(U)).$$

⌟

Proof: Cf.[Clausen, deRham Cohomology]L8P3. □

Cor. (7.2.0.3). For $R \in \mathcal{CR}ing$ and any $M \in \mathcal{M}od(R)$, there exists an associated sheaf of derived modules $M^\sharp$ on $\operatorname{Spec} R$ s.t. for any affine open $U \subset \operatorname{Spec} R$, $M^\sharp(U) = M \otimes_R \mathcal{O}_{\operatorname{Spec} R}(U)$. (I think this sheaf is just the derived shifification of the associated sheaf $\widetilde{M}$ on $\operatorname{Spec} R$ defined in(6.5.1.1).) ⌟

Proof: Cf.[Clausen, deRham Cohomology]L8P3. □

Cor. (7.2.0.4). Let $X \in \mathcal{A}ff$ and $\mathcal{F} \in \mathcal{QC}oh(X)$, then $H^q(X;\mathcal{F}) = 0$ for $q > 0$. ⌟

Proof: This is because the sheaf cohomology is the global section of the derived shifification, and the derived shifification of $\mathcal{F}(X)^\sharp$ equals $\widetilde{\mathcal{F}(X)}$ on any affine opens by(7.2.0.3). Thus $H^*(X;\mathcal{F}) = \mathcal{F}(X) \in D(\mathcal{O}_X(X))$. □

Cor. (7.2.0.5). For $R \in \mathcal{CR}ing$, there is a sheaf of Abelian categories on $X = \operatorname{Spec} R$ with assigns $\mathcal{M}od_{\mathcal{O}_X(U)}$ for any affine open subset $U \subset X$. ⌟

Proof: It suffices to show the discrete elements in $\mathcal{D}_{\mathcal{QC}oh}(\operatorname{Spec} R)$ form a sheaf, i.e. if $M \in \mathcal{D}_{\mathcal{O}_X(U)}$ is locally discrete, then it is discrete. And this is because the ring extensions are flat. □

Def. (7.2.0.6) [$\mathcal{D}(X)$]. Let $X \in \mathcal{S}ch$, then $\mathcal{D}(X) = \mathcal{M}od_{\mathcal{O}_X}(\mathcal{S}h(X;\mathcal{D}(Z)))$ is an ∞-category, and the assignment $\mathcal{D}_X : U \mapsto \mathcal{D}(U)$ is a sheaf of ∞-categories on X. ⌟

Proof: ? □

Def. (7.2.0.7) [$\mathcal{D}_{\mathcal{QC}oh}(\operatorname{Spec} R)$]. Let $X \in \mathcal{S}ch$, then there is a sub-∞-category

$$\mathcal{D}_{\mathcal{QC}oh}(X) \subset \mathcal{D}(X)$$

consisting of elements $\mathcal{M}$ s.t. for any inclusion of affine opens $U \subset V$, there is a natural isomorphism

$$\mathcal{M}(V) \otimes_{\mathcal{O}_X(V)} \mathcal{O}_X(U) \cong \mathcal{M}(U).$$

And the assignment $\mathcal{D}_{\mathcal{QC}oh,X} : U \mapsto \mathcal{D}_{\mathcal{QC}oh}(X)$ is a sheaf of ∞-categories on X.

Moreover, when X is affine, the global section functor defines an equivalence $\mathcal{D}(X) \cong D(\mathcal{O}_X(X))$.

⌟

Proof: ?
This follows from(7.2.0.6) and the fact that the Qco requirement is local:.
The last assertion is trivial. □

Prop. (7.2.0.8) [Compact Objects in $\mathcal{D}(R)$]. For $R \in \mathcal{CR}\mathrm{ing}$ and $M \in \mathcal{D}(R)$, the following are equivalent:

- M is a compact object.
- M lies in the thick (stable-∞)subcategory generated by R.
- M is dualizable w.r.t. the tensor product.
- M can be represented by a bounded chain of finite projective R-modules.

In particular, there is a full sub-∞-category of $D_{\mathcal{QC}\mathrm{oh}}(R)$ consisting of perfect objects, denoted by $\mathcal{P}\mathrm{erf}(R)$. ⌟

Proof: Cf.[Clausen, deRham Cohomology]L8P8. □

Cor. (7.2.0.9). For $R \in \mathcal{CR}\mathrm{ing}$, $X = \operatorname{Spec} R$, the assignment $\mathcal{P}\mathrm{erf} : U \mapsto \mathcal{P}\mathrm{erf}(\mathcal{O}_X(U))$ on affine opens is a subsheaf of $D_{\mathcal{QC}\mathrm{oh},X}$ on affine opens. ⌟

Proof: Cf.[Clausen, deRham Cohomology]L8P9. □

Def. (7.2.0.10) [Perfect Objects]. For $X \in \mathcal{S}\mathrm{ch}$, a **perfect quasi-coherent sheaf** on X is an object $\mathcal{F} \in \mathcal{D}_{\mathcal{QC}\mathrm{oh}}(X)$ s.t. for any affine open $U \subset X$, $\mathcal{F}|_U \in \mathcal{D}(U)$ is a compact object(?i.e. $\mathrm{Hom}(\mathcal{M}, -) : \mathcal{D}_{\mathcal{QC}\mathrm{oh}}(X) \to s\,\mathcal{S}\mathrm{et}$ commutes with filtered colimits). ⌟

Prop. (7.2.0.11) [Pull and Push]. For $f : X \to Y \in \mathcal{S}\mathrm{ch}$, there is a pushforward functor $f_* : \mathcal{D}(X) \to \mathcal{D}(Y)$ s.t.

- $f_* \mathcal{D}_{\mathcal{QC}\mathrm{oh}}(X) \subset \mathcal{D}_{\mathcal{QC}\mathrm{oh}}(Y)$.
- $f_* : \mathcal{D}_{\mathcal{QC}\mathrm{oh}}(X) \to \mathcal{D}_{\mathcal{QC}\mathrm{oh}}(Y)$ preserves colimits and limits.

And it has a left adjoint $f^* : \mathcal{D}(Y) \to \mathcal{D}(X)$ s.t.

- $f^* \mathcal{D}_{\mathcal{QC}\mathrm{oh}}(Y) \subset \mathcal{D}_{\mathcal{QC}\mathrm{oh}}(X)$.
- If $X, Y \in \mathcal{A}\mathrm{ff}$, then f^* is just the derived base change functor.
- f_* commutes with base change?.
- f_* satisfies projection formula?.

⌟

Proof: Cf.[Clausen, deRham Cohomology]L8P7. □

Prop. (7.2.0.12). If f is smooth and proper, $f_* : \mathcal{D}_{\mathcal{QC}\mathrm{oh}}(X) \to \mathcal{D}_{\mathcal{QC}\mathrm{oh}}(Y)$ preserves perfect objects. ⌟

Proof: Cf.[Clausen, deRham Cohomology]L8P8. □

Prop. (7.2.0.13) [Grothendieck Duality]. If $f : X \to Y \in \mathcal{S}\mathrm{ch}$ is proper and smooth, then there is a right adjoint $f^!$ to $f_* : \mathcal{D}(X) \to \mathcal{D}(Y)$, and it satisfies

- There is a natural isomorphism of functors: $f^* \otimes f^!(\mathcal{O}_Y) \cong f^!$.
- If f has relative dimension d, then there is a natural isomorphism $f^!(\mathcal{O}_Y) \cong \Omega^d_{X/Y}[d]$.

⌟

Proof: ? □

7.3 Elliptic Cohomology Theory(Lurie)

Main references are [Elliptic Cohomology,1, 2, Lurie].

8 Weil Cohomologies, Motives and Motivic Cohomology

8.1 Intersection Theory

Main references are [Sta]Chap43, 44 and [Ful98].

1 Setups

Def. (8.1.1.1) [Setups]. The setup is a universally catenary(hence locally Noetherian) scheme S(6.4.1.31) endowed with a dimension function δ(4.12.3.36), which will be fixed. ⌟

Example (8.1.1.2). There are some examples of (S,δ) in(8.1.1.1):

- $k\in\texttt{Field}, S=\operatorname{Spec}k$ and $\delta(|S|)=0$.
- A is a Noetherian domain of dimension 1, $\delta(\mathfrak{p})=0$ if $\mathfrak{p}$ is a maximal ideal and $\delta(\eta)=1$ for the generic point η.
- S is a C.M. scheme and let $\delta(s)=-\dim(\mathcal{O}_{S,s})$.

⌟

Proof: These follow from(6.4.1.33). □

Prop. (8.1.1.3). Let (S,δ) be in(8.1.1.1), S Jacobian and $\delta(s)=0$ for any closed point $s\in S$. If $Z\subset S$ is an integral closed subscheme with generic point ξ, then

$$\delta(\xi)=\dim(Z)=\dim(\mathcal{O}_{Z,z})$$

where $z\in Z$ is a closed point. ⌟

Proof: Cf.[Sta]02QO. □

Prop. (8.1.1.4) [δ-Dimenision]. For $f:X\to S$ locally of f.t., the function

$$\delta(x)=\delta(f(x))+\operatorname{tr.deg}_{k(f(x))}k(x)$$

is a dimension function on X. In particular, this equation is satisfied for any morphisms between schemes of f.t. over S.

For a closed subscheme Z of X, define $\dim_\delta(Z)=\sup\dim_\delta(\eta)$ where η are generic pts of irreducible components of Z. ⌟

Proof: Cf.[Sta]02JW.? □

2 Chow Homologies

Cycles

Def. (8.1.2.1) [Cycles]. An **algebraic cycle** on a scheme $X \in \mathcal{S}\mathrm{ch}^{\text{loc.ft}}/S$ is a formal sum of integral closed subschemes of X with integer coefficients that is locally finite. A k-cycle is a cycle that is a sum of integral closed subschemes of dimension k that is locally finite. The group of k-cycles over X is denoted by $Z_k(X)$.

If $\dim_\delta(X) = d$, then we also denote $Z^k(X) = Z_{d-k}(X)$. ⌟

Prop. (8.1.2.2). Let X be a scheme locally of f.t. over S, and $X = X_1 \cup X_2$ is a decomposition as closed subschemes, then there are exact sequences

$$Z_k(X_1 \cap X_2) \to Z_k(X_1) \oplus Z_k(X_2) \to Z_k(X) \to 0$$

⌟

Prop. (8.1.2.3) [Cycle associated to a Closed Subscheme]. For a closed subscheme Z of a scheme $X \in \mathcal{S}\mathrm{ch}^{\text{loc.ft}}/S$, if $\dim_\delta(Z) \leq k$ and $\eta \in Z$ has dimension k, then η is a generic pt of an irreducible component Z' of Z, and $m_{Z,Z'} = \mathrm{length}_{\mathcal{O}_{X,\eta}} \mathcal{O}_{Z,\eta}$ is finite.

So we may define the k**-cycle associated to** Z as: $[Z]_k = \sum_{Z' \subset Z} m_{Z,Z'}[Z']$, where the sum is over all integral components of Z of δ-dimension k. ⌟

Proof: $m_{Z,Z'}$ is finite because $\mathrm{length}_{\mathcal{O}_{Z,\eta}} \mathcal{O}_{Z,\eta} = \mathrm{length}_{\mathcal{O}_{X,\eta}} \mathcal{O}_{Z,\eta} < \infty$ because it is Noetherian and have 0 dimension(5.1.3.4). The sum is locally finite by(6.4.1.23). □

Prop. (8.1.2.4) [Cycle associated to a Coherent Sheaf]. For $X \in \mathcal{S}\mathrm{ch}^{\text{loc.ft}}/S$ and $\mathcal{F} \in \mathcal{C}\mathrm{oh}(X)$, if $\dim_\delta \mathrm{Supp}(\mathcal{F}) \leq k$ and $\eta \in \mathrm{Supp}(\mathcal{F})$ has dimension k, then η is a generic pt of an irreducible component Z' of Z, and $m_{Z,\mathcal{F}} = \mathrm{length}_{\mathcal{O}_{X,\eta}} \mathcal{F}_\eta < \infty$.

So we may define the k**-cycle associated to** $\mathcal{F}$ as: $[\mathcal{F}]_k = \sum_{Z \subset X} m_{Z,\mathcal{F}}[Z]$, where the sum is over all integral components of $\mathrm{Supp}\, \mathcal{F}$ of δ-dimension k. ⌟

Proof: $\mathrm{length}_{\mathcal{O}_{X,\eta}} \mathcal{F}_\xi < \infty$ by(5.2.5.7). □

Prop. (8.1.2.5). Let $X \in \mathcal{S}\mathrm{ch}^{\text{loc.ft}}/S$ and $Z \subset X$ a closed subscheme with $\dim_\delta(Z) \leq k$, then $[Z]_k = [\mathcal{O}_Z]_k$. ⌟

Prop. (8.1.2.6). Let $X \in \mathcal{S}\mathrm{ch}^{\text{loc.ft}}/S$, the cycle map from $\mathcal{C}\mathrm{oh}^{\leq k}(X)$ to $Z_k(X)$ is additive. ⌟

Pushforward and Pullback

Lemma (8.1.2.7) [Degree of Maps]. Let $f : X \to Y$ be a map between schemes integral and locally of f.t. over S, if $\dim_\delta X = \dim_\delta Y$, then either $f(X)$ not dominant or the function field extension is finite. If f is dominant, the the degree of f(6.4.4.55) is a finite number. ⌟

Proof: Because X is irreducible, so does $f(X)$ and $\overline{f(X)}$. If $f(X)$ is dominant, then f maps the generic point of X to that of Y. Now $\deg_{K(Y)}(K(X)) = 0$ and $K(X)/K(Y)$ is f.g., thus it is a finite extension. □

Lemma (8.1.2.8). Let $f : X \to Y$ be a qc map between schemes integral and locally of f.t. over S, and $\{Z_i\}$ is a locally finite collection of closed subschemes of X, then $\{\overline{f(Z)}\}$ is also a locally finite collection of closed subschemes of X. ⌟

Proof: This is a simple topological proof and omitted. □

Def. (8.1.2.9)[Proper Pushforward]. Let $f : X \to Y$ be a proper morphism in $\mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, we define a map
$$p_* : Z_k(X) \to \mathrm{CH}_k(X)$$
as follows: If $Z \subset X$ is an integral closed subscheme of X that $\dim_\delta(Z) = k$, then we define
$$f_*[Z] = \begin{cases} 0 & \dim_\delta(f(Z)) \leq k \\ \deg(Z/f(Z))[f(Z)](8.1.2.7) & \dim_\delta(f(Z)) = k \end{cases}.$$
where we regard $f(Z)$ as an integral closed subscheme of Y using its scheme-theoretical image. In general
$$f_*(\sum n_Z[Z]) = \sum n_Z f_*([Z]).$$
The sum is locally finite by(8.1.2.8).

It can be easily verified that $f_* \circ g_* = (f \circ g)_*$. ⌟

Prop. (8.1.2.10)[Pushforward of Coherent Sheaves]. Let $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, then

- If $Z \subset X$ is an integral closed subscheme of X that $\dim_\delta(Z) \leq k$, then
$$f_*[Z]_k = [\mathcal{O}_Z]_k.$$
- If $\mathcal{F} \in \mathcal{C}\mathrm{oh}^{\leq k}(X)$, then
$$f_*[\mathcal{F}]_k = [f_*\mathcal{F}]_k.$$

⌟

Proof: 1 follows from 2 and(8.1.2.5). To show 2, by restricting to $\mathrm{Supp}(\mathcal{F})$ and taking the scheme-theoretic image, it suffices to show for both closed immersions and proper dominant maps. The closed immersions case are easy. For the proper dominant case, it suffices to show $f_*[\mathcal{F}]_k$ and $[f_*\mathcal{F}]_k$ have the same coefficients in each integral subscheme $Z \subset X$ of dimension k. By looking at the inverse image of the generic point of Z, we may assume that f is finite by(6.4.4.53). Thus we can assume f is finite. Then it reduces to the affine case, which follows from(5.1.2.7). □

Lemma (8.1.2.11). Let $f : X \to Y$ be a flat morphism of relative dimension r in $\mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, then for any closed subscheme $Z \subset Y$, $\dim_\delta(f^{-1}(Z)) = \dim_\delta(Z) + r$ if $f^{-1}(Z) \neq \varnothing$. If Z is irreducible and $Z' \subset f^{-1}(Z)$ is an irreducible component, then Z' dominants Z and $\dim_\delta(Z') = \dim_\delta(Z) + r$. ⌟

Proof: By passing to the integral components, we may assume $Z = Y$ is integral and $X \to Y$ is surjective, then notice f is open, and use(8.1.1.4) and(6.6.3.7). □

Def. (8.1.2.12) [Flat Pullbacks]. Let $f : X \to Y$ be a flat morphism of relative dimension r in $\mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, for $Z \subset X$ an integral closed subscheme that $\dim_\delta(Z) \leq k$, define
$$f^* : Z_k(Y) \to Z_{k+r}(X) : f^*([Z]) = [f^{-1}(Z)]_{k+r}$$
which is definable by(8.1.2.11). In general, define $f^*(\sum n_Z[Z]) = \sum n_Z f^*([Z])$, which is locally finite. ⌟

Prop. (8.1.2.13). If $f : X \to Y, g : Y \to Z \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ is flat of relative dimensions r and s, then $f^* \circ g^* = (g \circ f)^*$. ⌟

Proof: Firstly $g\circ f$ is flat of relative dimension $r+s$ by(6.6.3.18). And the assertion follows from(5.1.2.9). □

Prop. (8.1.2.14). Let $X\in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $i:Y\to X$ a reduced closed subscheme of X, $j:U=X\backslash Z\to X$, then for any $k\in\mathbb{Z}$, there is an exact sequence

$$Z_k(Y)\xrightarrow{i_*}Z_k(X)\xrightarrow{j^*}Z_k(U)\to 0.$$

⌟

Prop. (8.1.2.15) [Pullback of Coherent Sheaves]. If $f:X\to Y\in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ is flat of relative dimensions r, $\mathcal{F}\in \mathcal{C}\mathrm{oh}^{\leq k}(\mathcal{O}_Y)$, then $f^*\mathcal{F}\in\mathcal{C}\mathrm{oh}^{\leq k+r}(\mathcal{O}_X)$, and

$$f^*[\mathcal{F}]=[f^*\mathcal{F}]_{k+r}.$$

In particular, for a closed subscheme $Z\subset X$ with $\dim_\delta(Z)\leq k$, $f^*[Z]_k=[f^{-1}Z]_{k+r}$, by(5.1.2.8). ⌟

Proof: This follows from(5.1.2.9). □

Prop. (8.1.2.16) [Push and Pull].

- Let

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X\\ \downarrow{f'} & & \downarrow{f}\\ Y' & \xrightarrow{g} & Y\end{array}$$

be a diagram in $\mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ where f is proper and g is flat of relative dimension r, then

$$g^*f_*=(g')^*f'_*:Z_k(X)\to Z_{k+r}(Y').$$

- Let $f:X\to Y\in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ be a finite locally free morphism of degree d, then it it both proper and flat of relative dimension 0, and $f_*f^*=[d]:Z_k(Y)\to Z_k(Y)$.

⌟

Proof: 1: It suffices to prove for a closed subscheme $W\subset X$ of δ-dimension k. Then $[W]=[\mathcal{O}_W]$(8.1.2.5). Then by(8.1.2.10) and(8.1.2.15), the assertion follows from flat base change.

2: Similarly this follows from the fact $f_*f^*\mathcal{O}_Z$ is a finite locally free $\mathcal{O}_Z$-sheaf of rank d. □

Rational Equivalences and Chow Groups

Def. (8.1.2.17)[Prime Weil Divisors]. Let $X\in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft,int}}/S$, then an integral closed scheme $W\subset X$ of δ-codimension 1 is called a **prime Weil divisor**. ⌟

Prop. (8.1.2.18)[Principal Weil Divisor]. Let $X\in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft,int}}/S$, $f\in\mathcal{K}$, for any prime Weil divisor Z with generic pt η, we can define $\mathrm{ord}_Z(f)=\mathrm{ord}_{\mathcal{O}_{X,\eta}}(f)$(5.1.2.10). It is multiplicative, and the closed integral subschemes Z that $\mathrm{ord}_Z(f)\neq 0$ is locally finite.

So, we can define the **principle Weil divisor** $\mathrm{div}(f)=\sum_Z \mathrm{ord}_Z(f)[Z]$. ⌟

Proof: There is an open subset U that $f\in\Gamma(U,\mathcal{O}_X^*)$, so all Z are irreducible components of $X-U$, which is locally finite because X is locally Noetherian and(6.4.1.23). □

Def. (8.1.2.19)[Principle Divisors]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $f \in K(X)^*$, then the **principle divisor associated to** f is defined to be

$$\mathrm{div}(f) = \sum \mathrm{ord}_Z(f)[Z] \in Z^1(X)$$

as defined in(8.1.2.18). This is truly a k-cycle. ⌟

Def. (8.1.2.20)[Rational Equivalence]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ has δ-dimension $k+1$. Given any locally finite collection of integrally closed subschemes $W_i \subset X$ of δ-dimension $k+1$ and rational functions f_i on W_i, we can consider the k-cycle $\sum (i_j)_*(\mathrm{div}(f_i))$ on X. This is a cycle because $\coprod W_i \to X$ is proper. Two k-cycles are called **rational equivalent** if they differ by a k-cycle of the this form.

Define the **Chow group of k-cycles** $\mathrm{CH}_k(X)$ to be $Z_k(X)$ modulo the rational equivalence relation. $\mathrm{CH}_k(X)$ is also denoted by $\mathrm{Cl}(X)$. ⌟

Lemma (8.1.2.21) [Push and Pull of Principle Divisors].

- If $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft,int}}/S$ is flat of relative dimension r, and $g \in K(Y)^*$, then $f^* \mathrm{div}(f) = \mathrm{div}(f)$.
- If $\varphi : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft,int},\delta=d}/S$ is a dominant proper morphism, $f \in K(X)^*$, and $g = \mathrm{Nm}_{K(X)/K(Y)}(f) \in K(Y)^*$, then $f_* \mathrm{div}(f) = \mathrm{div}(g)$.

⌟

Proof: 1: Cf.[Sta]0EPH**?**.

2: Cf.[Sta]02RT**?**. □

Lemma (8.1.2.22). If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft,int},\delta=n}/S$ $U \subset X$ be an open subscheme and $f \in \Gamma(U, \mathcal{O}_X)^* \subset K(X)^*$, let Y be the graph of f in $X \times_S \mathbb{P}^1_S$, then

- the projection $\mathrm{pr}_1 : Y \to X$ is an isomorphism $\mathrm{pr}^{-1}(U) \to U$, thus $\dim_\delta(Y) = n$.
- the closed subschemes $Y_0 = \mathrm{pr}_2^{-1}(\{0\})$ and $Y_\infty = \mathrm{pr}_2^{-1}(\{\infty\})$ of Y are effective Cartier divisors. In particular, they have δ-dimension $n-1$ by(8.1.5.2).
- $\mathrm{div}_Y(f) = [Y_0] - [Y_\infty]$.
- $\mathrm{div}_X(f) = \mathrm{pr}_{1*} \mathrm{div}_Y(f) = [Y_0] - [Y_\infty]$.

⌟

Proof: 1 is clear.

2 follows from(6.8.1.7) as $\mathrm{pr}_2 : Y \to \mathbb{P}^1$ is dominant.

3 is clear.

4 follows from item1 and(8.1.2.21). □

Prop. (8.1.2.23) [Rational Equivalence via Rational Functions]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, then $\alpha \in Z_k(X)$ is rationally trivial iff

$$\alpha = \sum([(W_i)_0]_k - [(W_i)_1]_k) = j_0^*(\sum[W_i]) - j_\infty^*(\sum[W_i])$$

where $\{W_i\}$ is a locally finite family of integral closed subschemes of $X \times_S \mathbb{P}^1_S$ of δ-dimension k.(j_0^*, j_∞^* are the Gysin maps, which will be defined in(8.1.4.2)) ⌟

Proof: Firstly such a $\sum([(W_i)_0]_k - [(W_i)_\infty]_k)$ is locally finite, and each $[(W_i)_0]_k - [(W_i)_\infty]_k$ is rationally trivial: Similar as in(8.1.2.22), $[(W_i)_0] - [(W_i)_\infty]$ is rationally trivial on W_i, and then it pushforward via pr_1 is also rationally trivial, by(8.1.2.21).

Conversely, if $\alpha = \sum (V_i \to X)_* \operatorname{div}(f_i)$, where $\{V_i\}$ is a locally finite family of integral closed subschemes of X of δ-dimension $k+1$ and $f_i \in K(V_i)^*$. Let $W_i \subset V_i \times \mathbb{P}^1_k \subset X_i \times \mathbb{P}^1_k$ be the the graph of f, then $(V_i \to X)_* \operatorname{div}(f_i)$ equals $[(W_i)_0]_k - [(W_i)_1]_k$ by(8.1.2.22) again.(We are secretly using the fact Gysin map commutes with pushforwards(8.1.6.9), but in this case it is trivial trough). □

Prop. (8.1.2.24) [Push and Pull for Chow Groups].

- If $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ is flat of relative dimension r, then f^* induces a map $\mathrm{CH}_k(Y) \to \mathrm{CH}_{k+r}(X)$ for each $k \in \mathbb{N}$.
- If $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ is proper, then f_* induces a map $\mathrm{CH}_k(X) \to \mathrm{CH}_k(X)$ for each $k \in \mathbb{N}$.

⌟

Proof: Cf.[Sta]02S2, 02S1. □

Prop. (8.1.2.25) [Restriction of Divisors]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $i : Y \to X$ a reduced closed subscheme of X, $j : U = X \backslash Z \to X$, then for any $k \in \mathbb{Z}$, there is an exact sequence

$$\mathrm{CH}_k(Y) \xrightarrow{i_*} \mathrm{CH}_k(X) \xrightarrow{j^*} \mathrm{CH}_k(U) \to 0.$$

⌟

Proof: Cf.[Sta]02RX?. □

Prop. (8.1.2.26) [Excision]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and X_1, X_2 be closed subschemes of X s.t. $X_1 \cup X_2 = X$ as sets, then for any $k \in \mathbb{Z}$, there is an exact sequence

$$\mathrm{CH}_k(X_1 \cap X_2) \to \mathrm{CH}_k(X_1) \oplus \mathrm{CH}_k(X_2) \to \mathrm{CH}_k(X) \to 0.$$

⌟

Proof: Cf.[Sta]0F94. □

Def. (8.1.2.27) [Degree of 0-Cycles]. Let X be a proper scheme over a field k, the **degree of a zero cycle** is given by the proper pushforward

$$p_* : \mathrm{CH}_0(X) \to \mathrm{CH}_0(\operatorname{Spec} k) \cong \mathbb{Z}.$$

Equivalently, if $\alpha = \sum n_i [Z_i] \in Z_0(X)$, $\deg(\alpha) = \sum n_i \deg(Z_i)$. deg is also denoted by $\int_X$. ⌟

Def. (8.1.2.28) [Stratification by Dimension]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, then the following are equivalent:

- There exists a decomposition $X = \coprod_n X_n$ where X_n is pure of δ-dimension n.
- For any $x \in X$, there exist s nbhd $x \in U$ s.t. U is pure of δ-dimension n.
- For an $x \in X$, the irreducible components of X containing x are all of the same δ-dimension n_x.

These conditions are satisfied if X is normal or Cohen-Macaulay. ⌟

Proof: $1 \to 2 \to 3$ is trivial. $3 \to 1$ follows from the fact $x \mapsto n_x$ is continuous.

If X is normal, it is a disjoint union of integral schemes by(6.4.2.3). For X Cohen-Macaulay, Cf.[Sta]0FE3.? □

Def. (8.1.2.29) [Cohomological Chow Groups]. If X satisfies(8.1.2.28), we define

$$Z^p(X) = \prod_n Z_{n-p}(X_n), \quad Z^*(X) = \bigoplus_p Z^p(X)$$

and the **Chow group of codimension p cycle**

$$\mathrm{CH}^p(X) = \prod_n \mathrm{CH}_{n-p}(X_n), \quad \mathrm{CH}^*(X) = \bigoplus_p \mathrm{CH}^p(X).$$

⌟

Def. (8.1.2.30) [Fundamental Class]. If X satisfies(8.1.2.28), define

$$[X] = \prod [X_n]_n \in \mathrm{CH}^0(X)$$

to be the **fundamental class of X**. ⌟

3 Chow Groups and K-Groups

Cf.[Sta]42.22, 42.56 and42.68.

4 Gysin Maps

Def. (8.1.4.1) [Gysin Maps for Virtual Divisors]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S, \mathcal{L} \in \mathrm{Pic}(X), s \in H^0(X, \mathcal{L})$, denote $D = Z(s)$, and $i : D \to X$ the closed immersion. Then for any $k \in \mathbb{Z}$, there is a **Gysin homomorphism**

$$i^* : Z_{k+1}(X) \to \mathrm{CH}_k(D)$$

that for an integral closed subscheme $Z \subset X$ with $\dim_\delta(Z) = k+1$,

$$i^*([Z]) = \begin{cases} [D \cap Z]_k & , Z \nsubseteq D \\ i'_*(c_1(\mathcal{L}|_Z) \cap [Z]) & , Z \subset D \text{ via } i' : Z \to D \end{cases}$$

and extends linearly to $Z_{k+1}(X)$, which is also locally finite.

We will see this is map i^* in fact factor through rational equivalence relations in(8.1.6.9). ⌟

Proof: To show this is well defined, Cf.[Sta]02TO.? □

Remark (8.1.4.2). If $\mathcal{L}|_D \cong \mathcal{O}_D$, the $c_1(\mathcal{L}|_Z)$ term is trivial, so the Gysin homomorphism factors through $Z_k(D) \to \mathrm{CH}_k(D)$. ⌟

Cor. (8.1.4.3). Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S, (\mathcal{L}, s, i : D \to X)$ as in(8.1.4.1), then for any $\alpha \in \mathrm{CH}_*(X)$,

$$i_* i^* \alpha = c_1(\mathcal{L}) \cap \alpha$$

⌟

Def. (8.1.4.4) [Intersection with Cartier Divisors]. If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S, D \in \mathrm{Cart}^{\mathrm{eff}}(X)$, denote $D \cap \alpha = c_1(\mathcal{O}_X(D)) \cap \alpha$ for $\alpha \in Z_*(X)$.? ⌟

Def. (8.1.4.5)[Gysin Map for Local Complete Intersection Maps]. Let $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ be a local complete intersection map s.t. $f = g \circ i$ where g is smooth and i is a regular immersion, then we define the **Gyin map** for f to be $f^! = i^! \circ g^* \in A^*(X \to Y)$. This is independent of the decomposition $f = g \circ i$ chosen. In this case, we say the Gysin map for f exists. ⌟

Proof: Cf.[Sta]0FF2.? □

Prop. (8.1.4.6) [$f^!$ and f^*]. Let $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ be a local complete intersection map, then if the Gysin map $f^!$ exists and f is flat, then f^* can be defined and $f^! = f^* \in A^*(X \to Y)$. ⌟

Proof: Cf.[Sta]0FF4.? □

5 Weil Divisors

Prop. (8.1.5.1) [Weil-Cartier]. For $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, there is a map from Cartier divisors on X to Weil divisors mapping (D, s_D) to $[Z(s_D)]_k$. Notice this is defined because a Cartier divisor is locally defined by a regular element and Krull's principal ideal theorem.

Moreover, if X is locally factorial, this map is an isomorphism $\mathrm{CaCl}(X) \to \mathrm{Cl}(X)$ by(6.8.1.4), and (effective)Cartier divisors correspond (effective)Weil divisors.

This in particular applies to non-singular varieties over a field, by(5.3.5.19). ⌟

Prop. (8.1.5.2). Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $Z \subset X$ be an integral closed subscheme, then Z is a Weil divisor iff $\dim_\delta(Z) = \dim_\delta(X) - 1$. In particular, this holds for any irreducible component of a Cartier divisor by(8.1.5.1). ⌟

Def. (8.1.5.3) [$\mathbb{Q}$-Cartier Divisors]. A **$\mathbb{Q}$-Cartier divisor** on a locally Noetherian integral scheme is a Weil divisor that some multiply of it is the image of a Cartier divisor. ⌟

Example (8.1.5.4)[Non-$\mathbb{Q}$-Cartier Divisors]. It is easy to show some Weil divisor is not an $\mathbb{Q}$-Cartier divisor (on a singular variety), by showing its complement is not affine(6.8.1.1). For example, on $X = \mathrm{Spec}\, k[x, y, z, w]/(xy - zw)$, the Weil divisor cut out by (z, w) is not $\mathbb{Q}$-Cartier, as the closed subscheme $y = w = 0$ of its complement is isomorphic to $\mathbb{A}^2_k \backslash \{(0, 0)\}$, which is not affine by calculating Čech cohomology.

In particular, $k[x, y, z, w]/(xy - zw)$ is normal but not a UFD. ⌟

Prop. (8.1.5.5) [Rational Functions and Poles]. If X is an integral locally Noetherian normal scheme and $f \in K(X)$ has no poles, then $f \in \Gamma(X)$, by(5.3.5.11). ⌟

Prop. (8.1.5.6) [UFD and Class Groups]. For A a Noetherian normal domain, it is a UFD iff $\mathrm{Cl}(\mathrm{Spec}\, A) = 0$. ⌟

Proof: It suffices to show minimal primes of A is principal iff minimal primes of A are principal divisors. This is done by(5.3.5.11) and(3.2.3.7). □

Prop. (8.1.5.7) [Picard Group of Projective Spaces]. Let R be a UFD, then $\mathrm{Cl}(\mathbb{P}^n_R) = \mathbb{Z}$, and it is generated by $[H]$ where H is any hyperplane of $\mathbb{P}^n_R$. And a hypersurface Y of degree d is mapped to d. ⌟

Proof: These follow from(8.1.7.10) and(8.1.5.6). The last assertion follows from the fact $[Y] \sim d[H]$ by direct verification. □

Cor. (8.1.5.8). If $Y \subset \mathbb{P}^n_k$ is a hypersurface of degree d, then $\mathrm{Cl}(\mathbb{P}^2 \backslash Y) = \mathbb{Z}/d\mathbb{Z}$. ⌟

Proof: This follows form(8.1.2.25) and(8.1.5.7). □

Cor. (8.1.5.9). If $k \in \texttt{Field}$, $\mathrm{Cl}(\mathbb{P}^1_k \times \mathbb{P}^1_k) = \mathbb{Z} \oplus \mathbb{Z}$, by(8.1.7.10). ⌟

Prop. (8.1.5.10). If X is a non-singular cubic surface in $\mathbb{P}^3_k$, then $\mathrm{Cl}(X) \cong \mathbb{Z}^7$. ⌟

Proof: Cf.[Har77]Chap5.4.8. □

6 Bivariant Classes

Def. (8.1.6.1) [Bivariant Classes]. Let $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $p \in \mathbb{Z}$, a **bivariant class** c of degree p for f is a class of maps

$$c \cap - : \mathrm{CH}_k(Y') \to \mathrm{CH}_{k-p}(Y' \times_Y X)$$

for any $Y' \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/Y$ and $k \in \mathbb{Z}_+$ that satisfies

- If $Y'' \to Y' \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/Y$ is proper, $c \cap -$ commutes with proper pushforwards.
- If $Y'' \to Y' \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/Y$ is flat of relative dimension $r \in \mathbb{Z}$, $c\cap -$ commutes with flat pullbacks.
- Let $(\mathcal{L}, s, i : D \to Y')$ be a triple on Y' as in(8.1.4.1), then $c \cap -$ commutes with Gysin homomorphisms i^*.

The set of bivariant classes of degree p for f is denoted by $A^p(X \to Y)$. And denote $A^*(X \to Y) = \oplus_{p \in \mathbb{Z}} A^p(X \to Y)$. ⌟

Prop. (8.1.6.2). For any $f : X \to Y, g : Y \to X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, $p, q \in \mathbb{Z}$, $A^p(X \to Y)$ is an Abelian group, and the composition defines a bilinear map

$$A^q(Y \to Z) \times A^p(X \to Y) \to A^{p+q}(X \to Z)$$

that is associative w.r.t. compositions in $\mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$. ⌟

Def. (8.1.6.3) [Chow Cohomologies]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, denote $A^p(X) = A^p(\mathrm{id}_X)$, and $A^*(X) = \oplus_{p \in \mathbb{Z}} A^p(X)$ the graded ring, called the **Chow cohomology group** of X. ⌟

Prop. (8.1.6.4) [Restriction of Classes]. Let $X \to Y, f : Y' \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $X' = X \times_Y Y'$, then obviously there is a map $f^* : A^p(X \to Y) \to A^p(X' \to Y')$. In particular, if $Z \subset X$ is a closed subscheme, then $f^*(c) \cap \alpha = c \cap f_*(\alpha)$ for $c \in A^p(Z \to X), \alpha \in A^p(Z)$ by proper pushforward(8.1.6.1). ⌟

Cor. (8.1.6.5) [Product of Classes]. Let $X \to Y, X' \to Y' \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, $c \in A^p(X \to Y), c' \in A^q(X' \to Y')$, then the product $c \circ c'$ is defined to be the element in $A^{p+q}(X \times_S X' \to Y \times_S Y')$ defined by the map

$$\mathrm{CH}_*(Y \times_S Y') \xrightarrow{c' \cap -} \mathrm{CH}_{*+q}(Y \times_S X') \xrightarrow{c \cap -} \mathrm{CH}_{*+p+q}(X \times_S X')$$

and all base change variants of this.

Notice $c' \circ c$ is also in $A^{p+q}(X \times_S X' \to Y \times_S Y')$, so it makes sense to talk about when two classes commute. Maybe $c' \circ c$ can be defined on smaller base changes, but to say c, c' commute always means $c \circ c' = c' \circ c \in A^{p+q}(X \times_S X' \to Y \times_S Y')$. ⌟

Lemma (8.1.6.6) [Gysin Factors Through Rational Equivalences]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, Gysin homomorphism for a triple $(\mathcal{L}, s, j : D \to X)$ on X that are base change of $(\mathcal{O}(1), x, j : S \times (0) \to \mathbb{P}^1_S)$ factors through rational equivalences. ⌟

Proof: This follows from the characterization of rational equivalences in(8.1.2.23) and the fact in this case Gysin maps are easy to describe: They are just k-parts of the inverse images. □

Prop. (8.1.6.7) [Weakening Bivariant Conditions]. Let $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and c is a class of maps

$$c \cap - : Z_k(Y') \to \mathrm{CH}_{k-p}(Y' \times_Y X)$$

for any $Y' \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/Y$ that is compatible with Gysin homomorphism for triples $(\mathcal{L}, s, j : D \to Y')$ that are base change of $(\mathcal{O}(1), x, j : S \times (0) \to \mathbb{P}^1_S)$, then c factors through rational equivalences

And if moreover c commutes with proper pushforwards and flat pullbacks(up to rational homotopy), then it induces a bivariant class $c \in A^p(X \to Y)$. ⌟

Proof: For the first assertion: As $\mathcal{L}|_D = \mathcal{O}_D$, the Gysin homomorphism is defined on the level of cycles by(8.1.4.2) and pass to CH_*(8.1.6.6), so compositions with Gysin homomorphisms are well-defined. Then c factors through rational equivalence by the characterization of rational equivalences in(8.1.2.23).

For the last assertion, Cf.[Ful98]P321 or [Sta]0F9A.**?** □

Prop. (8.1.6.8). Let $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $X = \coprod_I X_i, Y = \coprod_J Y_j$ be clopen subschemes and $\alpha : I \to J$ is a map of sets s.t. $f(X_i) \subset Y_{\alpha(i)}$, then for any $p \in \mathbb{Z}_+$,

$$A^p(X \to Y) = \prod_I A^p(X_i \to Y_{\alpha(i)}).$$

⌟

Proof: Cf.[Sta]0FDZ**?**. □

Prop. (8.1.6.9)[Gysin Homomorphisms are Bivariant]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $(\mathcal{L}, s, i : D \to X)$ be a triple on X as in(8.1.4.1), then the Gysin homomorphism $(i')^*$ associated to the base changes of i form a bivariant class in $A^1(D \to X)$. ⌟

Proof: Cf.[Sta]02TA, 0B71, 0B73.**?** and(8.1.6.7).

Let $f : X' \to X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $(\mathcal{L}, s, i : D \to X)$ be a triple on X as in(8.1.4.1), we can define the pullback triple $f^*(\mathcal{L}, s, i) = (\mathcal{L}', s', i' : D' \to X')$, and then

- If f is proper, then Gysin maps commute with proper pushforwards.
- If f is flat of relative dimension r, then the Gysin maps commute with flat pullbacks.
- If $(\mathcal{M}, t, f : X' \to X)$ is a triple on X as in(8.1.4.1), then the different Gysin maps are compatible.

□

Prop. (8.1.6.10) [Flat Pullbacks are Bivariant]. Let $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ be flat of relative dimension r, then the flat pullbacks along base changes of f form a bivariant class of degree $-r$. ⌟

Proof: This follows from(8.1.2.13)(8.1.2.16)(8.1.6.9) and(8.1.6.7). □

Prop. (8.1.6.11)[Proper Pushforwards are Bivariant]. Let $f : X \to Y, g : Y \to Z \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, f is proper, and $c \in A^p(X \to Z)$, then the base change of $f_* \circ c$ form a bivariant class in $A^p(Y \to Z)$. ⌟

Proof: This reduces to the fact proper pushforwards commutes with flat pullbacks, proper pushforwards and Gysin maps, by(8.1.6.10)(8.1.6.9)(8.1.2.9) and(8.1.6.7). □

7 Chern Classes

Invertible Sheaves

Prop. (8.1.7.1) [First Chern Classes]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $\mathcal{L} \in \mathrm{Pic}(X)$, then for any $k \in \mathbb{Z}$, there is a map

$$c_1(\mathcal{L}) \cap - : Z_{k+1}(X) \to \mathrm{CH}_k(X)$$

called intersection with the **first Chern class** of $\mathcal{L}$(the name will be made clear in(8.1.7.5)), defined as follows: If $i : Z \to X$ is an integral subscheme of X with $\dim_\delta(Z) = k+1$, then $c_1(\mathcal{L}) \cap [Z]$ is the the pushforward of the image of $i^*\mathcal{L}$ under the map $\mathrm{Pic}(Z) \to \mathrm{Cl}(Z) \cong \mathrm{CH}_k(Z)$(6.5.3.14), i.e.

$$c_1(\mathcal{L}) \cap [Z] = i_*(c_1(i^*\mathcal{L}) \cap [W]).$$

In general, define $c_1(\mathcal{L}) \cap (\sum n_Z[Z]) = \sum n_Z c_1(\mathcal{L}) \cap [Z]$. We will see the first Chern class factors through rational equivalence relations in(8.1.7.5). ⌟

Lemma (8.1.7.2) [The first Chern Class is Multiplicative]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $\mathcal{L}, \mathcal{N} \in \mathrm{Pic}(X)$, then

$$c_1(\mathcal{L}) + c_1(\mathcal{N}) = c_1(\mathcal{L} \otimes \mathcal{N}) : Z_{*+1}(X) \to \mathrm{CH}_*(X).$$

In particular, $c_1(\mathcal{L}) = -c_1(\mathcal{L}^{-1})$, and $c_1(\mathcal{O}_X) = 0$. ⌟

Prop. (8.1.7.3) [Chern Classes and Zero Cycles]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $\mathcal{L} \in \mathrm{Pic}(X)$, $Y \subset X$ a closed subscheme. If $s \in \Gamma(Y, \mathcal{L}|_Y)$ satisfies

- $\dim_\delta(Y) \le k+1$.
- $\dim_\delta(Z(s)) \le k$.
- For any generic point ξ of irreducible components of $Z(s)$ of δ-dimension k, multiplying by s induces an injection $\mathcal{O}_{Y,\xi} \to (\mathcal{L}|_Y)_\xi$.

Then $c_1(\mathcal{L}) \cap [Y]_{k+1} = [Z(s)]_k$. ⌟

Proof: Cf.[Sta]02SQ.**?** □

Prop. (8.1.7.4) [First Chern Classes Factor Through $\mathrm{CH}_*(X)$]. Situation in(8.1.7.1), then the first Chern class map $c_1(\mathcal{L}) \cap - : Z_{k+1}(X) \to \mathrm{CH}_k(X)$ factors through $Z_{k+1}(X) \to \mathrm{CH}_{k+1}(X)$. ⌟

Proof: Cf.[Sta]02TI. □

Prop. (8.1.7.5) [First Chern Classes Form Bivariant Classes]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/X$ and $\mathcal{L} \in \mathrm{Pic}(X)$, then the first Chern class maps $c_1(f^*\mathcal{L}) \cap - : Z_*(X') \to \mathrm{CH}_{*-1}(X')$ factor through rational equivalences for each $f : X' \to X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/X$, and form a bivariant class in $A^1(X)$, called the **first Chern class** $c_1(\mathcal{L})$. ⌟

Proof: Cf.[Sta]02SU, 02SS, 0B72. and(8.1.6.7).
To show it commutes with pullbacks, □

Prop. (8.1.7.6) [First Chern Classes Commute with Bivariant Classes]. Let $f : X' \to X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $\mathcal{L} \in \mathrm{Pic}(X)$, then $c_1(\mathcal{L})$ commutes with every element of $A^*(X' \to X)$.
In particular, $c_1(\mathcal{L})$ is in the center of $A^*(X)$. ⌟

Proof: Cf.[Sta]0B7B.**?** □

Prop. (8.1.7.7). Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $\mathcal{L} \in \mathrm{Pic}(X)$ be an ample invertible sheaf. Assume $d = \dim(X) < \infty$, then for any $\mathcal{L}_1, \ldots, \mathcal{L}_{d+1} \in \mathrm{Pic}(X)$, $c_1(\mathcal{L}_1) \circ \ldots c_1(\mathcal{L}_{d+1}) = 0 \in A^{d+1}(X)$. ⌟

Proof: Use induction on d: $d = 0$ case is trivial as X is discrete thus any invertible sheaf is trivial. In general, by(6.8.1.8) and(8.1.7.2), it suffices to prove for $\mathcal{L}_i = \mathcal{O}_X(D_i)$ being Cartier divisors. If $i : D_{d+1} \to X$, then $c_1(\mathcal{L}_{d+1}) = i_* \circ i^*$ by(8.1.4.3), and $c_1(\mathcal{L}_i)$ commutes with both i_* and i^*, so we can replace X by D and then use induction hypothesis. □

Lemma (8.1.7.8). If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $0 \to \mathcal{L}_1 \to \mathcal{E} \to \mathcal{L}_2 \to 0$ is an exact sequence with $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Pic}(X)$, and there is a non-vanishing section s of $\mathcal{E}$, then $c_1(\mathcal{L}_1) \cap c_1(\mathcal{L}_2) = 0 \in A^2(X)$. ⌟

Proof: Consider the image $\overline{s}$ of s in $\Gamma(X, \mathcal{L}_2)$, then we can consider the Gysin map associated to $(\mathcal{L}_2, \overline{s}, j)$. Then

$$c_1(\mathcal{L}_1) \cap c_1(\mathcal{L}_2) \cap \alpha = j_*(c_1(j^*\mathcal{L}_1) \cap j^*\alpha).$$

$j^*\mathcal{L}_1$ is trivialized by s now, so this one is vanishes. □

Lemma (8.1.7.9). If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S, r \in \mathbb{Z}_+, \mathcal{L} \in \mathcal{V}\mathrm{ect}^r(X)$, let $\pi : \mathbf{P}(\mathcal{E}) \to X$ be the projective space of $\mathcal{E}$, then for any $k \in \mathbb{Z}$ and $\alpha \in \mathrm{CH}_k(X)$,

$$\pi_*(c_1(\mathcal{O}_{\mathbf{P}(\mathcal{E})}(1))^s \cap \pi^*\alpha) = \begin{cases} 0 & , s < r-1 \\ \alpha & , s = r-1 \end{cases} \in \mathrm{CH}_{k+r-1-s}(X).$$

⌟

Proof: Cf.[Sta]02TW. □

Prop. (8.1.7.10) [Projective Bundles Formula]. If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S, r \in \mathbb{Z}_+, \mathcal{L} \in \mathcal{V}\mathrm{ect}^r(X)$, let $\pi : \mathbf{P}(\mathcal{E}) \to X$ be the projective space of $\mathcal{E}$, then for any $k \in \mathbb{Z}$, the map

$$\mathrm{CH}_{k+r-1}(\mathbf{P}(\mathcal{E})) = \bigoplus_{i=0}^{r} c_i(\mathcal{O}_{\mathbf{P}(\mathcal{E})}(1))^i \cap \pi^* \mathrm{CH}_{k+i}(X).$$

is an isomorphism.

In particular, if X is integral, then

$$\mathrm{Cl}(\mathbf{P}(\mathcal{E})) = \pi^*(\mathrm{Cl}(X)) \oplus [c_1(\mathcal{O}_{\mathbf{P}(\mathcal{E})}(1))].$$

⌟

Proof: Cf.[Sta]02TX.? □

Prop. (8.1.7.11) [Vector Bundles]. If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S, r \in \mathbb{Z}_+, \mathcal{L} \in \mathcal{V}\mathrm{ect}^r(X)$, let $\pi : \mathbf{E} = \mathbf{Spec}(\mathrm{Sym}(\mathcal{E})) \to X$ be the vector bundle of $\mathcal{E}$, then for any $k \in \mathbb{Z}$, $p^* : \mathrm{CH}_k(X) \to \mathrm{CH}_{k+r}(X)$ is an isomorphism. ⌟

Proof: Cf.[Sta]02TY. □

Prop. (8.1.7.12) [Diagonal Intersections]. For $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}^n/k$,

$$\Delta \cdot \Delta = \deg(c_n(\mathcal{T}_X)).$$

⌟

Proof: Cf.[Mustata, P14]. □

Vector Bundles

Prop. (8.1.7.13) [Splitting Principle]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, $\mathcal{E}_i \subset \mathcal{V}\mathrm{ect}(X)$ be a finite set of finite locally free sheaves, there exists a projective flat morphism $\pi : P \to X$ of relative dimension d s.t.

- For any $Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/X$, the map $\pi_Y^* : \mathrm{CH}^*(Y) \to \mathrm{CH}^*(Y \times_X P)$ is injective.
- Each $\pi^*\mathcal{E}_i$ has a filtration with invertible quotient sheaves.

This is useful in the way that when proving functorial properties of Chern classes of vector bundles, we can reduce to invertible sheaves. ⌟

Proof: Cf.[Sta]02UL. □

Def. (8.1.7.14) [Chern Classes of Vector Bundles]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, $r \in \mathbb{Z}_+, \mathcal{E} \subset \mathcal{V}\mathrm{ect}^r(X)$ with projective bundle $\pi : \mathbf{P}(\mathcal{E}) \to X$, then for any $k, p \in \mathbb{N}$, there is a map

$$c_p(\mathcal{E}) \cap - : \mathrm{CH}_k(X) \to \mathrm{CH}_{k-p}(X)$$

called **intersection with Chern classes** as follows(the name will be made clear in(8.1.7.15)): Let $\alpha \in \mathrm{CH}_k(X)$, by(8.1.7.10) there are unique elements $c_p \in \mathrm{CH}_{k-p}(X)$ s.t. $c_0 = \alpha$ and

$$\sum_{p=0}^{r}(-1)^p c_1(\mathcal{O}_{\mathbf{P}(\mathcal{E})})^p \cap \pi^* c_{r-p} = 0 \in \mathrm{CH}_{k-1}(\mathbf{P}(i^*\mathcal{E})).$$

Then define $c_p(\mathcal{E}) \cap \alpha = c_p$.

In particular, if $\mathcal{E}$ is an invertible sheaf, $c_1(\mathcal{E})\cap$ is just the intersection with the first Chern class $c_1(\mathcal{E}) \cap \alpha$(8.1.7.1)(8.1.7.6). ⌟

Prop. (8.1.7.15) [Chern Classes Form Bivariant Classes]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/X, r \in \mathbb{Z}_+, \mathcal{E} \in \mathcal{V}\mathrm{ect}^r(X)$, then the maps $c_p(f^*\mathcal{E})\cap - : \mathrm{CH}_k(X') \to \mathrm{CH}_{k-p}(X')$ for each $f : X' \to X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/X, k \in \mathbb{Z}_+$ form a bivariant class in $A^p(X)$, called the **Chern classes** $c_p(\mathcal{E})$. By convention, set $c_p(\mathcal{E}) = 0$ for $p > r$.

And $c(\mathcal{E}) = \sum_{i=0}^r c_i(\mathcal{E}) \in A^*(X)$ are called the **total Chern class** of $\mathcal{E}$. ⌟

Proof: For commuting with proper pushforward, use the definition(8.1.7.14) and(8.1.2.24)(8.1.7.5), and push and pull(8.1.2.16).

For commuting with flat pullback, use the definition(8.1.7.14) and(8.1.2.24)(8.1.7.5) and properties of flat pullbacks(8.1.2.13).

For commuting with Gysin map, use the definition(8.1.7.14) and(8.1.2.24)(8.1.7.5) and properties of Gysin maps(8.1.6.9). □

Prop. (8.1.7.16) [Chern Classes Commute with Bivariant Classes]. Let $f : X' \to X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $\mathcal{E} \in \mathcal{V}\mathrm{ect}^r(X)$, then for any $p \in \mathbb{Z}_+$, $c_p(\mathcal{E})$ commutes with every element of $A^*(X' \to X)$.

In particular, $c_p(\mathcal{E})$ are in the center of $A^*(X)$, and for $\mathcal{E} \in \mathcal{V}\mathrm{ect}^r(X), \mathcal{F} \in \mathcal{V}\mathrm{ect}^s(X), p, q \in \mathbb{Z}_+$, $c_p(\mathcal{E}), c_q(\mathcal{F})$ commute. ⌟

Proof: Reduce to c_1 and(8.1.7.6) as we did in(8.1.7.15). □

Prop. (8.1.7.17) [Chern Classes for Arbitrary Vector Bundles]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/X, \mathcal{E} \in \mathcal{V}\mathrm{ect}^{\delta}(X)$, then constancy of r induces a clopen partition of $X = \coprod_{i=0}^{\infty} X_i$, where X_i are the clopen subscheme s.t. $\delta = i$. Then by(8.1.6.8), $A^p(X) = \prod_{i=0}^{\infty} A^p(X_i)$, so we can define the Chern class $c_p(\mathcal{E})$ to be the product of $c_p(\mathcal{E}|_{X_i})$. Also we can define a **rank class** $r(\mathcal{E}) \in A^0(X) = \prod_{i=0}^{\infty} A^0(X_i)$ that is product of $[i] \in A^0(X_i)$. ⌟

Prop. (8.1.7.18) [Additivity]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $0 \to \mathcal{E}_1 \to \mathcal{E} \to \mathcal{E}_2 \to 0 \in \mathcal{V}\mathrm{ect}(X)$, then

$$c(\mathcal{E}) = c(\mathcal{E}_1)c(\mathcal{E}_2).$$

⌟

Proof: It suffices to check this by their action on $[X]$ where $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft,int}}/S$. Using splitting principle(8.1.7.13), we can easily reduce to the case $\mathcal{E}_1, \mathcal{E}_2 \in \mathrm{Pic}(X)$ by induction on $\mathrm{rank}(\mathcal{E}_1)$ and $\mathrm{rank}(\mathcal{E}_2)$. In this case, let $\mathbf{P}$ be the projective bundle of $\mathcal{E}$ with $\mathcal{O}(1) = \mathcal{O}_{\mathbf{P}}(1)$. By tag02U6, it suffices to show that

$$c_1(\mathcal{O}(1))^2 \cap \pi^*\alpha - c_1(\mathcal{O}(1)) \cap \pi^*(c_1(\mathcal{E}_1) \cap \alpha + c_1(\mathcal{E}_2) \cap \alpha) + \pi^*(c_1(\mathcal{E}_1) \cap c_1(\mathcal{E}_2) \cap \alpha).$$

for which it suffices to show that

$$(c_1(\mathcal{O}(1)) - c_1(\pi^*\mathcal{E}_1)) \cap (c_1(\mathcal{O}(1)) - c_1(\pi^*\mathcal{E}_2)) = c_1(\pi^*\mathcal{E}_1^\vee(1)) \cap c_1(\pi^*\mathcal{E}_2^\vee(1)) = 0$$

There is a surjection $\mathcal{E} \to \mathcal{O}(1)$, which corresponds to a non-zero section of $\mathcal{E}^\vee(1)$. Notice there is an exact sequence

$$0 \to \mathcal{E}_2^\vee \to \mathcal{E}^\vee(1) \to \mathcal{E}_1^\vee \to 0,$$

so the assertion follows from(8.1.7.8). □

Prop. (8.1.7.19). Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $\mathcal{E} \in \mathcal{V}\mathrm{ect}^r(X)$, then $c_1(\wedge\mathcal{E}) = c_1(\mathcal{E})$, and

$$\prod_{p=0}^{r} c(\wedge^p\mathcal{E})^{(-1)^n} = 1 - (r-1)!c_r(\mathcal{E}) + \dots.$$

⌟

Proof: Use splitting principle and Cf.[Sta]0FEE. □

Prop. (8.1.7.20) [Degrees and First Chern Classes]. Let X be a proper scheme over a field k, then

- Let $\mathcal{L}_1, \dots, \mathcal{L}_d$ be invertible sheaves on X and $Z \subset X$ a closed subscheme of dimension d, then

$$(\mathcal{L}_1 \cdot \ldots \cdot \mathcal{L}_d; Z) = \deg(c_1(\mathcal{L}_1) \cap \ldots \cap c_1(\mathcal{L}_d) \cap [Z]_d).$$

  In particular, if $\mathcal{L}$ is an ample invertible sheaf,

$$\deg_{\mathcal{L}}(Z) = \deg(c_1(\mathcal{L})^d \cdot [Z]_d).$$

- If $\dim X \le 1$, for $\mathcal{E} \in \mathcal{C}\mathrm{oh}^{\mathrm{free}}(X)$,

$$\deg(\mathcal{E}) = \deg(c_1(\mathcal{E}) \cdot [X]_1).$$

⌟

Proof: Cf.[Sta]0AZ3, 0BFI.**?** □

Prop. (8.1.7.21) [Chern Characters]. Let $X \in \mathcal{S}ch^{\text{loc.ft}}/S$, r a locally constant $\mathbb{Z}$-valued functions on X and $\mathcal{E} \in \mathcal{V}ect^r(X)$, define the **Chern character** of $\mathcal{E}$ to be

$$\begin{aligned}\operatorname{ch}(\mathcal{E}) &= \operatorname{rank}(\mathcal{E}) + \sum_{p\geq 0} \frac{P_p(c_1(\mathcal{E}),\ldots,c_n(\mathcal{E}))}{p!} \in \prod_{i\geq 0} A^i(X)_{\mathbb{Q}} \\ &= \operatorname{rank}(\mathcal{E}) + c_1(\mathcal{E}) + \frac{1}{2}(c_1(\mathcal{E})^2 - 2c_2(\mathcal{E})) + \frac{1}{6}(c_1(\mathcal{E})^3 - 3c_1(\mathcal{E})c_2(\mathcal{E})3c_3(\mathcal{E})) \\ &+ \frac{1}{24}(c_1(\mathcal{E})^4 - 4c_1(\mathcal{E})^2c_2(\mathcal{E}) + 4c_1(\mathcal{E})c_3(\mathcal{E}) + 2c_2(\mathcal{E})^2 - 4c_4(\mathcal{E})) + \ldots\end{aligned}$$

where P_p are Chern polynomials(3.3.4.3). ⌟

Prop. (8.1.7.22)[Tensor Products]. If $X \in \mathcal{S}ch^{\text{loc.ft}}/S$, r, s, t are locally constant $\mathbb{Z}$-valued functions on X and $\mathcal{E} \in \mathcal{V}ect(X), \mathcal{F} \in \mathcal{V}ect(X), \mathcal{G} \in \mathcal{V}ect(X)$, then

- If there is an exact sequence $0 \to \mathcal{E} \to \mathcal{G} \to \mathcal{F} \to 0$, then $\operatorname{ch}(\mathcal{E}) + \operatorname{ch}(\mathcal{F}) = \operatorname{ch}(\mathcal{G})$.
- $\operatorname{ch}(\mathcal{E} \otimes_{\mathcal{O}_X} \mathcal{F}) = \operatorname{ch}(\mathcal{E})\operatorname{ch}(\mathcal{F})$.
- $\operatorname{ch}_i(\mathcal{E}^\vee) = (-1)^i \operatorname{ch}_i(\mathcal{E})$.

In particular, ch defines a ring homomorphism $\operatorname{ch} : K_0(\mathcal{V}ect(X)) \to \prod_{i\geq 0} A^i(X)_{\mathbb{Q}}$. ⌟

Proof: It suffices to prove for X connected, and then by(8.1.7.13), we can assume $\mathcal{E}, \mathcal{F}$ have filtrations with invertible quotient sheaves $\mathcal{E}_1, \ldots, \mathcal{E}_r$ and $\mathcal{F}_1, \ldots, \mathcal{F}_s$ with first Chern characters $a_1, \ldots, a_r$ and $b_1, \ldots, b_s$, then by additivity(8.1.7.18) and the definition of Chern polynomials(3.3.4.3), we see

$$\operatorname{ch}(\mathcal{E}) = \sum_{i=1}^r \exp(a_i), \quad \operatorname{ch}(\mathcal{F}) = \sum_{j=1}^s \exp(b_j),$$

and $\mathcal{E} \otimes \mathcal{F}$ has a filtration with quotient sheaves $\mathcal{E}_i \otimes \mathcal{F}_j$ with first Chern characters $a_i + b_j$ by(8.1.7.2), so the assertions are now clear. □

Cor. (8.1.7.23) [Chern Classes of Tensor Products]. If $X \in \mathcal{S}ch^{\text{loc.ft}}/S$, r, s are locally constant $\mathbb{Z}$-valued functions on X and $\mathcal{E} \in \mathcal{V}ect^r(X), \mathcal{F} \in \mathcal{V}ect^s(X)$, then

$$c_i(\mathcal{E}^\vee) = (-1)^i c_i(\mathcal{E}) \in A^i(X),$$

$$c_1(\mathcal{E} \otimes \mathcal{F}) = rc_1(\mathcal{E}) + sc_1(\mathcal{F}) \in A^1(X),$$

$$c_2(\mathcal{E} \otimes \mathcal{F}) = rc_2(\mathcal{F}) + sc_2(\mathcal{E}) + \binom{r}{2} c_1(\mathcal{F})^2 + (rs-1)c_1(\mathcal{E})c_1(\mathcal{F}) + \binom{s}{2} c_1(\mathcal{E})^2 \in A^2(X),$$

$$c_2(\mathcal{H}om(\mathcal{E},\mathcal{E})) = 2rc_2(\mathcal{E}) - (r-1)c_1(\mathcal{E})^2 \in A^2(X).$$

⌟

Prop. (8.1.7.24) [Todd Classes]. Let $X \in \mathcal{S}ch^{\text{loc.ft}}/S$ and $\mathcal{E} \in \mathcal{V}ect(X)$, define the **Todd class** $\operatorname{Todd}(\mathcal{E})$ of $\mathcal{E}$ to be

$$\begin{aligned}\operatorname{Todd}(\mathcal{E}) &= \operatorname{Todd}(c_1(\mathcal{E}), c_2(\mathcal{E}), \ldots)(3.3.4.4) = 1 + \frac{1}{2}c_1(\mathcal{E}) + \frac{1}{12}(c_1(\mathcal{E})^2 + c_2(\mathcal{E})) \\ &+ \frac{1}{24}c_1(\mathcal{E})c_2(\mathcal{E}) + \frac{1}{720}(-c_1^4(\mathcal{E}) + 4c_1^2(\mathcal{E})c_2(\mathcal{E}) + 3c_2^2(\mathcal{E}) + c_1(\mathcal{E})c_3(\mathcal{E}) - c_4(\mathcal{E})) + \ldots.\end{aligned}$$

Then if $0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0 \in \mathcal{V}ect(X)$ be an exact sequence, then $\operatorname{Todd}(\mathcal{E})\operatorname{Todd}(\mathcal{E}'') = \operatorname{Todd}(\mathcal{E})$. ⌟

Proof: The proof is the same as that of(8.1.7.22). □

Prop. (8.1.7.25) [Borel-Serre]. Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $\mathcal{E} \in \mathcal{C}\mathrm{oh}^{\mathrm{free},r}(X)$, then

$$\sum_{p=0}^{r}(-1)^p \operatorname{ch}(\wedge^p \mathcal{E}^\vee) = c_r(\mathcal{E})\operatorname{Todd}(\mathcal{E})^{-1}.$$

⌟

Proof: ? □

Prop. (8.1.7.26) [Chern Classes of K-Groups]. $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, by additivity and multiplicativeness(8.1.7.18)(8.1.7.22), we can extend Chern classes and Chern characters to the K-group $K_0(\mathcal{V}\mathrm{ect}(X))$:

$$c : K_0(\mathcal{V}\mathrm{ect}(X)) \to \prod_{p\geq 0} A^p(X), \quad \operatorname{ch} : K_0(\mathcal{V}\mathrm{ect}(X)) \to \prod_{p\geq 0} A^p(X)_{\mathbb{Q}}$$

where c is a group homomorphism and ch is a ring homomorphism. ⌟

Prop. (8.1.7.27) [Adam Operators and Chern Characters]. $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $\alpha \in K_0(\mathcal{V}\mathrm{ect}(X))$, then $c_i(\psi^k(\alpha)) = 2^{ki}c_i(\alpha)$ and $\operatorname{ch}_i(\psi^k(\alpha)) = 2^{ki}\operatorname{ch}_i(\alpha)$. ⌟

Proof: It suffices to prove for $\alpha = [\mathcal{E}]$ where $\mathcal{E} \in \mathcal{V}\mathrm{ect}(X)$, then by splitting principle it suffices to prove for line bundles, and this is clear from(8.1.7.23) and the definition(8.1.7.21)t. □

Perfect Complexes

Lemma (8.1.7.28). Let $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, then for each perfect complex $\mathcal{E}$ in $D(\mathcal{O}_X)$, we can define the Chern classes, Chern characters and ranks of $\mathcal{E}$. But we only define fora subset of E here?Cf.[Sta]0F9E: If $\mathcal{E}$ is represented by a finite complex $\mathcal{E}^\bullet$ of vector bundles on X, define

$$c(\mathcal{E}) = \prod_i c(\mathcal{E}^i)^{(-1)^i} \in \prod_{i\geq 0} A^i(X), \quad \operatorname{ch}(\mathcal{E}) = \sum_i (-1)^i \operatorname{ch}(\mathcal{E}^i) \in \prod_{i\geq 0} A^i(X)_{\mathbb{Q}}, \quad r(\mathcal{E}) = \sum_i (-1)^i r(\mathcal{E}^i).$$

⌟

Proof: To show this is well defined, □

Prop. (8.1.7.29) [Chern Classes via Envelopes]. Let $Y \to X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ be an envelope?, $\mathcal{E}$ perfect in $D(\mathcal{O}_X)$ s.t. $Lf^*\mathcal{E}$ is representable by a finite complex of vector bundles on Y, then there are unique bivariant classes $c(\mathcal{E}) \in \prod_{i\geq 0} A^i(X), \operatorname{ch}(\mathcal{E}) \in \prod_{i\geq 0} A^i(X)_{\mathbb{Q}}, \quad r(\mathcal{E})$ s.t. their restrictions to Y are of the form defined in(8.1.7.28).

Moreover, these bivariant classes are invariant of the envelope chosen. In this case, we say the Chern classes of $\mathcal{E}$ are defined. ⌟

Proof: Cf.[Sta]0GUD. □

Prop. (8.1.7.30). If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and each irreducible components of X are qc, then X has an envelope. In particular, this applies to X qc. ⌟

Proof: Cf.[Sta]0GUE?. □

Prop. (8.1.7.31)[Additivity]. If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $\mathcal{E}_1 \to \mathcal{E}_2 \to \mathcal{E}_3 \to \mathcal{E}_1[1]$ is a distinguished triangle of perfect complexes in $D(\mathcal{O}_X)$, and one of the following holds:

- There exists an envelope $f : Y \to X$ s.t. $Lf^*\mathcal{E}_1 \to Lf^*\mathcal{E}_2$ is representable by a map of finite complexes of vector bundles on Y.
- Each irreducible components of X is irreducible.

Then Chern classes of $\mathcal{E}_i$ are defined, and

$$c(\mathcal{E}_2) = c(\mathcal{E}_1)c(\mathcal{E}_3), \quad \mathrm{ch}(\mathcal{E}_2) = \mathrm{ch}(\mathcal{E}_1) + \mathrm{ch}(\mathcal{E}_3).$$

⌟

Proof: Cf.[Sta]0F9F**?**. □
Se

Prop. (8.1.7.32). If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and $\mathcal{E}$ be a perfect object in $D(\mathcal{O}_X)$ whose Chern classes are defined, then

- Let $f : X' \to X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$, $p \in \mathbb{Z}_+$, then $c_p(\mathcal{E})$ commutes with every element of $A^*(X' \to X)$, i.e. $c \cdot c_p(\mathcal{E}) = c_p(Lf^*\mathcal{E}) \cdot c$.
  In particular, $c_p(\mathcal{E})$ are in the center of $A^*(X)$, and for $\mathcal{E}, \mathcal{F}$ perfect in $D(\mathcal{O}_X)$ whose Chern classes are defined, $p, q \in \mathbb{Z}_+, c_p(\mathcal{E}), c_q(\mathcal{F})$ commute.
- $\log(c(\mathcal{E})) = \sum_{p\geq 0} \frac{P_p(c_1(\mathcal{E}),\ldots,c_n(\mathcal{E}))}{p}$ also holds, where P_p are Chern polynomials(3.3.4.3). Similarly for Chern character $\mathrm{ch}(\mathcal{E})$.
- $c_i(\mathcal{E}^\vee) = (-1)^i c_i(\mathcal{E}), \mathrm{ch}_i(\mathcal{E}^\vee) = (-1)^i \mathrm{ch}_i(\mathcal{E})$.

⌟

Proof: These follow from the splitting principle and the definition(8.1.7.29). □

Prop. (8.1.7.33) [Tensor Products]. If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ and E, F perfect in $D(\mathcal{O}_X)$ whose Chern classes are defined, then

$$\mathrm{ch}(\mathcal{E} \otimes^{\mathrm{L}}_{\mathcal{O}_X} \mathcal{F}) = \mathrm{ch}(\mathcal{E})\,\mathrm{ch}(\mathcal{F}),$$

in particular, formulas in(8.1.7.23) hold. ⌟

Proof: This follows from the splitting principle and the definition(8.1.7.29). □

8 Non-Singular Intersection Theory

Lemma (8.1.8.1). If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{ft,sep}}_{\mathrm{reg},qc}/S$ with bounded δ-dimension, then the composition

$$K_0(\mathcal{V}\mathrm{ect}(X)) \otimes \mathbb{Q} \xrightarrow{\mathrm{ch}} \prod_{p\geq 0} A^p(X) \xrightarrow{-\cap[X]} \mathrm{CH}^*(X) \otimes \mathbb{Q}$$

is an isomorphism. ⌟

Proof: Firstly $K_0(X) = K_0'(X) = K_0(\mathcal{V}\mathrm{ect}(X))$ by(6.8.5.33) and(6.8.5.36).
The rest follows from[Sta]0FEY.**?** □

Prop. (8.1.8.2)[$\mathbb{Q}$-Intersection Products on Regular Schemes]. If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{ft,sep}}_{\mathrm{reg},qc}/S$ with bounded δ-dimension, then the isomorphism $K_0(\mathcal{V}\mathrm{ect}(X)) \otimes \mathbb{Q} \cong \mathrm{CH}^*(X) \otimes \mathbb{Q}$ endows $\mathrm{CH}^*(X)_{\mathbb{Q}}$ with a commutative associative ring structure: If $\alpha = \mathrm{ch}(\alpha') \cap [X], \beta = \mathrm{ch}(\beta') \cap [X]$, then

$$\alpha \cdot \beta = \mathrm{ch}(\alpha) \cap \mathrm{ch}(\beta) \cap [X] = \mathrm{ch}(\alpha') \cap \beta = \mathrm{ch}(\beta') \cap \alpha.$$

And this ring structure preserves the gradation on $\mathrm{CH}^*(X)_{\mathbb{Q}}$. Also it is preserved under morphism in $\mathcal{S}\mathrm{ch}^{\mathrm{ft,sep}}_{\mathrm{reg},qc}$ flat of relative dimension r. ⌟

Proof: To prove it preserves gradation, suppose $\alpha \in \mathrm{CH}^i(X), \beta \in \mathrm{CH}^j(X)$, then α' and $2^{-i}\psi^2(\alpha')$(8.1.7.27) are both inverse images of α, so they are equal. Then $\mathrm{ch}(\alpha') = \mathrm{ch}(2^{-i}\psi^2(\alpha'))$, which means $\mathrm{ch}(\alpha') \in A^i(X)_{\mathbb{Q}}$, and then $\mathrm{ch}(\alpha') \cap \beta \in \mathrm{CH}^{i+j}(X)_{\mathbb{Q}}$. □

Smooth over Dedekind Schemes Case

Smooth over Fields Case

Prop. (8.1.8.3)[Exterior Products]. If $k \in \mathtt{Field}, S = \mathrm{Spec}\, k$, $X, Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/k$, there is a **exterior product map**

$$\mathrm{CH}_n(X) \otimes \mathrm{CH}_m(Y) \to \mathrm{CH}_{n+m}(X \times_S Y)$$

defined by sending $[X'] \otimes [Y']$ to $[X' \times_S Y']_{n+m}$, where $X' \subset X, Y' \subset Y$ are integral closed subschemes of dimension n and m resp. ⌟

Proof: To show this is well defined, consider $i : X' \to X, c : X \to \mathrm{Spec}\, k$, then by(8.1.6.11), $c_* \circ (c \circ i)^* \in A^{-n}(X \to \mathrm{Spec}\, k)$, which sends $[Y']$ to $[X' \times_k Y']_{n+m}$, so this map factors through rational equivalences on Y, and similarly it factors through rational equivalences on X. □

Prop. (8.1.8.4). If $k \in \mathtt{Field}, S = \mathrm{Spec}\, k$ and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/k$, there is a natural isomorphism $A^p(X \to \mathrm{Spec}\, k) \cong \mathrm{CH}_{-p}(X)$ for any $p \in \mathbb{Z}$. ⌟

Proof: The map $A^p(X \to \mathrm{Spec}\, k) \to \mathrm{CH}_{-p}(X)$ is given by $c \mapsto c \cap [\mathrm{Spec}\, k]$. Conversely, for any $\alpha \in \mathrm{CH}_{-p}(X)$, we can define for any $X' \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/k$ a map

$$\mathrm{CH}_n(X') \to \mathrm{CH}_{n-p}(X \times_k X') : \beta \mapsto \alpha \times \beta \text{(8.1.8.3)}.$$

Then this is a bivariant class in $A^p(X \to \mathrm{Spec}\, k)$: Let $\alpha = \sum n_i[X_i]$, and let $g : \coprod_i X_i \to X$, $f : \coprod_i X_i \to \mathrm{Spec}\, k$. Denote $\nu^* \in A^0(\coprod_i X_i)$ the bivariant class that multiplies by n_i at each component X_i, then $g_* \circ \nu \circ f^* \in A^p(X \to \mathrm{Spec}\, k)$ by(8.1.6.10)(8.1.6.11), and this is just the map we defined above.

To show these two maps are inverse to each other, one direction is clear. To show $c(\beta) = (c \cap [\mathrm{Spec}\, k]) \times \beta$, it suffices to show for $\beta = [X']$ is integral, then $\beta = (X' \to \mathrm{Spec}\, k)^*[\mathrm{Spec}\, k]$, then it is easy to see they are equal because c commutes with flat pullbacks $(X' \to \mathrm{Spec}\, k)^*$. □

Cor. (8.1.8.5) [Commutativity and Associativity]. If $k \in \mathtt{Field}, S = \mathrm{Spec}\, k$ and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/k$, then $c \in A^p(X \to \mathrm{Spec}(k))$ commutes with any $c' \in A^q(Y \to Z)$ for any $f : Y \to Z \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/k$. In other words, for any $\alpha \in \mathrm{CH}_*(X), \beta \in \mathrm{CH}_*(Z)$ and $c \in A^*(Y \to Z)$,

$$\alpha \times (c \cap \beta) = c \cap (\alpha \times \beta) \in \mathrm{CH}_*(X \times_k Y).$$

In particular, if $\gamma \in \mathrm{CH}_*(Y)$, then

$$(\alpha \times \beta) \times \gamma = \alpha \times (\beta \times \gamma) \in \mathrm{CH}_*(X \times_k Y \times_k Z).$$

⌟

Proof: This is because $c = g_* \circ \nu \circ f^*$ as in the proof of(8.1.8.4). □

Prop. (8.1.8.6) [Perturbation and Chow Rings]. Any two algebraic cycles $\gamma_1, \gamma_2 \in Z_*(X)$ are rationally equivalent to cycles γ_1', γ_2' s.t. γ_1', γ_2' intersect properly. And the rational class of resulting intersection cycle is well-defined. So there is an intersection on $\mathrm{CH}^*(X)$ making it a commutative ring, called the **Chow ring of** X. ⌟

Proof:

□

Prop. (8.1.8.7) [Bezout]. The Chow ring of $\mathbb{P}^n_k$ is isomorphic to $\mathbb{Z}[x]/(x^{n+1})$. The degree of an irreducible closed variety corresponds to the coefficient of it. ⌟

Proof:

□

Def. (8.1.8.8) [Euler Characteristic]. If X is a smooth scheme over a field k of dimension d with tangent bundle $\mathcal{T}_{X/k} \in \mathcal{V}\mathrm{ect}(X)$, the **Euler characteristic of** X is defined to $\deg(c_d(\mathcal{T}_{X/k}) \cap [X])$, and the **Todd characteristic of** X is defined to $\deg(\mathrm{Todd}_d(\mathcal{T}_{X/k}) \cap [X])$(8.1.7.24). ⌟

Prop. (8.1.8.9). If X is a smooth scheme over a field k and $i : Y \to X$ is a regular closed immersion and Y is equidimensional of dimension e, then

$$[Y]_e \cdot \alpha = i_*(i^!(\alpha)).$$

⌟

Proof: Cf.[Sta]0FFE**?**. □

<u>**Serre's Approach**</u>

Prop. (8.1.8.10). If X is a integral scheme smooth over a field k, and W, V be two integral closed subschemes of X, then $\mathrm{codim}(W \cap V) \le \mathrm{codim}(W) + \mathrm{codim}(V)$. ⌟

Proof: Cf.[Sta]0AZP. □

Def. (8.1.8.11) [Proper Intersections]. Let X be a integral scheme smooth over a field k, then two cycles $\alpha = \sum n_i[W_i]$ and $\beta = \sum m_j[V_j]$ are said to intersect properly iff

$$\mathrm{codim}(W_i \cap V_j) \ge \mathrm{codim}(W_i) + \mathrm{codim}(V_j).$$

And in fact equality holds, by(8.1.8.10). ⌟

Lemma (8.1.8.12) [Tor Sheaves]. Let X be a integral scheme smooth over a field k and $\mathcal{F}, \mathcal{G} \in \mathfrak{Coh}(X)$, then $\mathrm{Tor}_p^{\mathcal{O}_X}(\mathcal{F}, \mathcal{G}) \in \mathfrak{Coh}(X)$, with stalk at $x \in X$ being $\mathrm{Tor}_p^{\mathcal{O}_{X,x}}(\mathcal{F}_x, \mathcal{G}_x)$, and is supported on $\mathrm{Supp}(\mathcal{F}) \cap \mathrm{Supp}(\mathcal{G})$, and nonzero only for $0 \le p \le \dim X$. ⌟

Proof: Cf.[Sta]0AZT. □

Def. (8.1.8.13) [Intersection via Tor]. Let X be a regular scheme and $W, V \subset X$ be integral closed subschemes intersecting properly, by(8.1.8.12) we can define the **intersection product**

$$W \cdot V = \sum_i [\mathrm{Tor}_i^{\mathcal{O}_X}(\mathcal{O}_W, \mathcal{O}_V)]_{r+s-\dim X},$$

and for any irreducible component Z of $W \cap V$ the **intersection multiplicities**

$$e(X, W \cdot V, Z) = \sum_i (-1)^i \operatorname{length}_{\mathcal{O}_{X,Z}} \mathrm{Tor}_i^{\mathcal{O}_{X,Z}}(\mathcal{O}_{W,Z}, \mathcal{O}_{V,Z}).$$

⌟

Proof: Why is this compatible with the definition given before**?**. Why the multiplicity is given by this form**?** □

Remark (8.1.8.14) [Serre Conjecture]. Serre conjectured that in(8.1.8.13), even if W, V doesn't intersect properly, for an irreducible component $Z \subset W \cap V$ of dimension$\geq \dim W + \dim V - \dim X$, we have $e(X, W \cdot V, P) = 0$. ⌟

Prop. (8.1.8.15) [Discrete Case]. Let X be a integral scheme smooth over k and $W, V \subset X$ be closed subvarieties that intersect properly. Let Z be an irreducible component of $V \cap W$ with generic point ξ and $\mathcal{O}_{W,\xi}, \mathcal{O}_{V,\xi}$ are both C.M., then

$$e(X, W \cdot V, Z) = \operatorname{length}_{\mathcal{O}_{X,\xi}}(\mathcal{O}_{V \cap W, \xi}).$$

⌟

Proof: Cf.[Sta]0B02**?**. □

Prop. (8.1.8.16) [Exterior Product of Subvarieties]. Let X, Y be integral schemes smooth over k and $W \subset X, V \subset Y$ be subvarieties, then $[W] \times [V] = ([W] \times [Y]) \cdot ([X] \times [V]) \in Z_*(X \times Y)$. ⌟

Proof: As $W \times V$ is a variety with generic point ξ, and X is smooth over k, $X \times V$ is smooth over V, thus $\mathcal{O}_{X \times V, \xi}$ is regular, hence C.M., and similarly is $\mathcal{O}_{W \times Y, \xi}$, thus(8.1.8.15) applies to show that $([W] \times [Y]) \cdot ([X] \times [V]) = [W] \times [V]$. □

Prop. (8.1.8.17) [Serre]. If X is a integral scheme smooth over a field k, $\mathcal{F} \in \mathfrak{Coh}_{\leq r}(X), \mathcal{G} \in \mathfrak{Coh}_{\leq s}(X)$, and $\dim(\operatorname{Supp}(\mathcal{F}) \cap \operatorname{Supp}(\mathcal{G})) \leq r + s - \dim X$. Then $[\mathcal{F}]_r$ and $[\mathcal{G}]_s$ intersect properly, and

$$[\mathcal{F}]_r \cdot [\mathcal{G}]_s = \sum_p (-1)^p [\mathrm{Tor}_p^{\mathcal{O}_X}(\mathcal{F}, \mathcal{G})]_{r+s-\dim X}$$

⌟

Proof: Cf.[Sta]0B0W. □

Cor. (8.1.8.18). If X is a smooth integral scheme over a field k, the intersection product on $\mathrm{CH}^*(X)$ makes it a commutative graded (associative, unital)ring. ⌟

Proof: To show the intersection is associative, let U, V, W be closed subvarieties of X s.t. $\operatorname{codim}(U \cap V \cap W, X) = \operatorname{codim}(U, X) + \operatorname{codim}(V, X) + \operatorname{codim}(W, X) = p$, then it suffices to show that

$$\sum_i (-1)^{i+j} [\mathrm{Tor}_j(\mathcal{O}_U, \mathrm{Tor}_i(\mathcal{O}_V, \mathcal{O}_W))]_{\dim X - p} = \sum_i (-1)^{i+j} [\mathrm{Tor}_j(\mathrm{Tor}_i(\mathcal{O}_U, \mathcal{O}_V), \mathcal{O}_W)]_{\dim X - p}.$$

This is true because they are both equal to

$$\sum_k (-1)^k [H^k(\mathcal{O}_U \otimes^{\mathrm{L}} \mathcal{O}_V \otimes^{\mathrm{L}} \mathcal{O}_W)]_{\dim X - p}$$

which is because there is an spectral sequence convergence

$$E_2^{p,q} = \mathrm{Tor}_{-p}(\mathcal{O}_U, \mathrm{Tor}_{-q}(\mathcal{O}_V, \mathcal{O}_W)) \Rightarrow H^{p+q}(\mathcal{O}_U \otimes^{\mathrm{L}} \mathcal{O}_V \otimes^{\mathrm{L}} \mathcal{O}_W)$$

and use the fact length functions are additive. □

9 Numerical Geometry

Let $k \in \mathtt{Field}$ and $k = \overline{k}$.

References are http://www.math.columbia.edu/~chaoli/docs/IntersectionTheory.html#sec13.

Prop. (8.1.9.1) [Schubert Cycles of the Grassmannian]. ⌟

Prop. (8.1.9.2). Given 4 curves $C_1, \ldots, C_4$ in $\mathbb{P}^3_k$ of degree $d_1, \ldots, d_4$, there are $2d_1d_2d_3d_4$ lines intersecting all of them. ⌟

Proof: □

Prop. (8.1.9.3). Use the projective bundle formula to show that given 9 lines $L_1, \ldots, L_8 \in \mathbb{P}^3_k$ in general position, there are 92 conics meeting all L_i. ⌟

Proof:

□

Prop. (8.1.9.4). Show that given two general twisted cubic curves $C, C' \in \mathbb{P}^3_k$, they have 10 common chords. ⌟

Proof: □

Prop. (8.1.9.5). Show that given a general quintic surface $S \in \mathbb{P}^3_k$, there are 575 lines meeting S at only one point. ⌟

Proof: □

Prop. (8.1.9.6). Show that given 5 general conics $S_1, \ldots, S_r$ in $\mathbb{P}^3_k$, there are 3264 conics tangent to all S_i. ⌟

Proof: □

10 Riemann-Roch

Main references are[Ful98]Chap15, 18.

Prop. (8.1.10.1) [Grothendieck-Riemann-Roch]. Let $f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}/S$ be proper smooth, and $\mathcal{E} \in \mathcal{C}\mathrm{oh}^{\mathrm{free}}(X)$, $\mathcal{T}_{X/Y} \in \mathcal{C}\mathrm{oh}^{\mathrm{free}}(X)$ is the relative tangent bundle, then

$$f_*(\mathrm{Todd}(\mathcal{T}_{X/Y})\,\mathrm{ch}(\mathcal{E})) = \sum_i (-1)^i \,\mathrm{ch}(R^i f_* \mathcal{E}).$$

⌟

Remark (8.1.10.2). This theorem also has an Arithmetic version. ⌟

Proof: □

Cor. (8.1.10.3) [Hirzebruch-Riemann-Roch]. If $k \in \mathtt{Field}$ and $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}/k$, $\mathcal{E} \in \mathcal{C}\mathrm{oh}^{\mathrm{free}}(X)$, then

$$\chi(X, \mathcal{E}) = \int_X \mathrm{Todd}(\mathcal{T}_{X/k})\,\mathrm{ch}(\mathcal{E}).$$

In particular,

$$\chi(X, \mathcal{O}_X) = \int_X \mathrm{Todd}(\mathcal{T}_{X/k}).$$

⌟

Singular Case

11 Numerical Equivalences

Def. (8.1.11.1) [Numerical Equivalences]. Two cycles $\gamma, \gamma' \in \mathrm{CH}^k(X)$ are called **numerically equivalent** if for any $\delta \in Z_k(X)$, $\gamma \cdot \delta = \gamma' \cdot \delta$. And we can define $GH_k(X)$ the **Grothendieck group of k-cycles** to be $Z_k(X)$ modulo the numerical equivalence relation. ⌟

Prop. (8.1.11.2) [Grothendieck Rings]. There is a group homomorphism $\mathrm{CH}^*(X) \to GH^*(X)$ and the ring structure on $\mathrm{CH}^*(X)$ descends to $GH^*(X)$, making it a ring, called the **Grothendieck ring of X**. ⌟

12 Intersection for Line Bundles

Main references are [FGA, Appendix B].

Algebraic Equivalence

Def. (8.1.12.1) [Algebraically Equivalent Line Bundles]. Let X be a scheme over a field k, then $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Pic}(X)$ are called **algebraically equivalent** if they are equivalent in the equivalence relation $\mathcal{M} \sim \mathcal{N}$ iff there is a connected scheme T and a line bundle $\mathcal{L} \in \underline{\mathrm{Pic}}_{X/k}(T)$ s.t. $\mathcal{N}_{k(t_1)} = \mathcal{L}_{t_1}$ and $\mathcal{M}_{k(t_2)} = \mathcal{L}_{t_2}$ where $t_1, t_2 \in T$. ⌟

Cor. (8.1.12.2)[$\mathrm{Pic}^0(X)$]. The elements in $\mathrm{Pic}(X)$ algebraically equivalent to 0 is a subgroup of $\mathrm{Pic}(X)$, denoted by $\underline{\mathrm{Pic}}^0(X)$. In(8.1.12.4), we will see when X has a rational point and $\underline{\mathrm{Pic}}_{X/k}$ is representable, this is just $\underline{\mathrm{Pic}}^0_{X/k}(k)$, by(9.7.2.7). ⌟

Prop. (8.1.12.3) [Algebraically Equivalent Divisors]. If X be a regular K-prevariety, then $\mathrm{Pic}(X) \cong \mathrm{CH}^1(X)$(6.5.3.15). We call two divisors D_1, D_2 on X **algebraically equivalent** if $\mathcal{O}(D_1)$ and $\mathcal{O}(D_2)$ are algebraically equivalent. ⌟

Proof: Cf.[Diophantine Geometry, P563]. □

Prop. (8.1.12.4) [Moduli Characterization]. If X is a scheme over a field k s.t. $\underline{\mathrm{Pic}}_{X/k}$ is representable, then two line bundles are algebraically equivalent iff they corresponds to points of $\underline{\mathrm{Pic}}_{X/k}$ in the same connected component. ⌟

Proof: By(9.7.2.20), $\underline{\mathrm{Pic}}_{X/k}$ is a locally algebraic group scheme over k, so by(9.1.4.13), every connected components of it is irreducible. Clearly two algebraically equivalent line bundles are in the same connected component of $\underline{\mathrm{Pic}}_{X/k}$. Conversely, the inclusion of their common connected component P corresponds to a line bundle on some fppf covering $T \to P$. Then use the fact fppf covering is open map, and the fact P is irreducible to get an algebraic equivalence chain. □

Prop. (8.1.12.5) [Algebraic Equivalence for Curves]. If C is a smooth complete curve over a field k, then two line bundles $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Pic}(C)$ are algebraically equivalent iff they have the same degree. ⌟

Proof: It suffices to show after base change to $\overline{k}$. Then it suffices to show for any two closed points $x_1, x_2 \in C$, $\mathcal{L}(x_1) \sim \mathcal{L}(x_2)$. Consider the diagonal of $C \times C$ is a Cartier divisor, and its restriction to $C \times \{x_i\}$ is $\mathcal{L}(x_i)$. □

Numerical Intersections

Def. (8.1.12.6). Let X be a proper scheme and $\mathcal{F}$ be a coherent sheaf with $\dim \mathrm{Supp}\, \mathcal{F} \leq n$, and $\mathcal{L}_1, \ldots, \mathcal{L}_n$ are invertible sheaves on X, then we define $(\mathcal{L}_1 \cdot \ldots \cdot \mathcal{L}_n; \mathcal{F})$ to be

$$\sum_{\{i_1,\ldots,i_m\} \subset \{1,\ldots,n\}} (-1)^m \chi(X, \mathcal{L}_{i_1}^\vee \otimes \ldots \otimes \mathcal{L}_{i_m}^\vee \otimes \mathcal{F}).$$

When $\mathcal{F}$ is the structure sheaf of a closed subscheme Y, then denote $(\mathcal{L}_1 \cdot \ldots \cdot \mathcal{L}_n; \mathcal{F})$ by $(\mathcal{L}_1 \cdot \ldots \cdot \mathcal{L}_n; \mathcal{Y})$. This intersection is stable under base change of fields. ⌟

Prop. (8.1.12.7). If X is a complete curve and $\mathcal{L}$ an invertible sheaf on X, then $(\mathcal{L}; X) = \deg(\mathcal{L})$. ⌟

Proof: □

Prop. (8.1.12.8). If k is an infinite field and $X = \mathbb{P}^n_k$, and Y is a dimension n subvariety of X. If $H_1, \ldots, H_n$ are generic chosen hypersurfaces of degree $d_1, \ldots, d_n$ resp., then

$$(\mathcal{O}_X(H_1) \cdot \ldots \cdot \mathcal{O}_X(H_n); Y) = d_1 \ldots d_n \deg(Y).$$

⌟

Proof: □

Prop. (8.1.12.9). If D is an effective Cartier divisor on X that doesn't contain any associated point of $\mathcal{F}$, then

$$(\mathcal{L}_1 \cdot \ldots \cdot \mathcal{L}_n \cdot \mathcal{O}(D); \mathcal{F}) = (\mathcal{L}_1|_Y \cdot \ldots \cdot \mathcal{L}_n|_Y; \mathcal{F}|_D)$$

⌟

Proof:

□

Prop. (8.1.12.10). For a fixed $\mathcal{F}$, $(\mathcal{L}_1 \cdot \ldots \mathcal{L}_n; \mathcal{F})$ is a symmetric multilinear function of $\mathcal{L}_1, \ldots, \mathcal{L}_n$, where the addition is tensor production. Moreover, if $\mathcal{F}$ is a coherent sheaf with support dimension n, then $(\mathcal{L}_1 \cdot \ldots \cdot \mathcal{L}_{n+1}; \mathcal{F}) = 0$. ⌟

Proof: Cf.[Rising Sea, P544]. □

Prop. (8.1.12.11). The numerical intersection $(\mathcal{L}_1\cdot\ldots\cdot\mathcal{L}_n;\mathcal{F})$ only depends on the numerical classes of $\mathcal{L}_i$. ⌟

Prop. (8.1.12.12)[Projection Formula]. Let $\pi: X_1\to X_2$ be a proper morphism of proper schemes, then

$$(\pi^*\mathcal{L}_1\cdot\ldots\cdot\pi^*\mathcal{L}_n;\mathcal{F})=(\mathcal{L}_1\cdot\ldots\cdot\mathcal{L}_n;\pi_*\mathcal{F}).$$

In particular, when X_1,X_2 are integral with the same dimensions and π is a finite map,

$$(\pi^*\mathcal{L}_1\cdot\ldots\cdot\pi^*\mathcal{L}_n)=\deg(\pi)(\mathcal{L}_1\cdot\ldots\cdot\mathcal{L}_n).$$

⌟

Proof:
For the last assertion, notice $\pi_*\mathcal{O}_{X_1}=\deg(\pi)\mathcal{O}_{X_2}+$ coherent sheaves with smaller supper dimensions. □

Prop. (8.1.12.13). Let k be a field and X a proper scheme over k, and $Z\subset X$ a closed subscheme of dimension d. If $\mathcal{L}_1,\ldots,\mathcal{L}_d$ are ample invertible sheaves on X, then $(\mathcal{L}_1\cdot\ldots\cdot\mathcal{L}_d;Z)$ is positive. ⌟

Proof: □

Prop. (8.1.12.14). Let X be a complex projective scheme, then $(\mathcal{L}_1\cdot\ldots\cdot\mathcal{L}_n;Z)$ equals

$$(c_1((\mathcal{L}_1)_{an})\cup\ldots c_1((\mathcal{L}_n)_{an}),Z)$$

where c_1 is the complex Chern class. ⌟

Proof: Cf.[Rising Sea, P547]. □

Def. (8.1.12.15) [First Chern Class]. Let X be a proper scheme and K be the Grothendieck group of $\mathcal{C}\mathrm{oh}(X)$. For $\mathcal{L}\in\mathrm{Pic}(X)$, define $c_1(\mathcal{L})$ to be the endomorphism of K defined by

$$c_1(\mathcal{L})\mathcal{F}=\mathcal{F}-\mathcal{L}^{-1}\otimes\mathcal{F}.$$

⌟

Prop. (8.1.12.16). If $\mathcal{L},\mathcal{M}\in\mathrm{Pic}(X)$, then

- $c_1(\mathcal{L})c_1(\mathcal{M})=c_1(\mathcal{L})+c_1(\mathcal{M})-c_1(\mathcal{L}\otimes\mathcal{M})$.
- $c_1(\mathcal{O}_X)=0$.
- $c_1(\mathcal{L})c_1(\mathcal{L}^{-1})=c_1(\mathcal{L})+c_1(\mathcal{L}^{-1})$.

In particular, $c_1(\mathcal{L})$ and $c_2(\mathcal{M})$ commutes. ⌟

Prop. (8.1.12.17). If X is a proper scheme over a field k and let K^d be the subgroup generated by coherent sheaves over X with support dimension $\leq d$, then if $\mathcal{F}\in K^d$, then $c_1(\mathcal{L})\mathcal{F}\in K^{d-1}$. ⌟

Proof:

□

Prop. (8.1.12.18). If $Y\subset X$ is a closed subscheme, and $\mathcal{L}\in\mathrm{Pic}(X)$ satisfy $\mathcal{L}_Y$ is an effective Cartier divisor D, then $c_1(L)[Y]=[D]$. ⌟

Proof: There is an exact sequence $0\to\mathcal{O}_Y(-D)\to\mathcal{O}_Y\to\mathcal{O}_D$, and $\mathcal{O}_Y(-D)\cong\mathcal{L}^{-1}\otimes\mathcal{O}_Y$. □

τ-Equivalences

Def. (8.1.12.19) [τ-Equivalence]. Let X be a scheme over a field k, then two line bundles $\mathcal{L}_1, \mathcal{L}_2$ are called **τ-equivalent** if there are some $m \in \mathbb{Z}_+$ s.t. $\mathcal{L}_1^{\otimes m} \sim \mathcal{L}_2^{\otimes m}$. ⌟

Prop. (8.1.12.20) [Moduli Characterization]. Let X be a scheme over a field k and $\underline{\mathrm{Pic}}_{X/k}$ is representable, then $\mathcal{L} \in \mathrm{Pic}(X)$ is τ-equivalent to $\mathcal{O}_X$ iff its corresponding point $\lambda \in \underline{\mathrm{Pic}}_{X/k}$ is in $\underline{\mathrm{Pic}}^\tau_{X/k}$. ⌟

Proof: Clear from the definition of $\underline{\mathrm{Pic}}^\tau_{X/k}$. □

Def. (8.1.12.21) [Numerically Equivalence]. Tow line bundles L_1, L_2 on a complete prevariety over a field K is called **numerically equivalent** if $c_1(L_1).\alpha = c_1(L_2).\alpha$ for any complete precurve $C \subset X$. Two divisors on X is called **numerically equivalent** if their corresponding line bundle do.

Numerically trivial line bundles form a group, and are stable under proper pullbacks, by(6.12.2.7)(6.12.2.5). ⌟

Prop. (8.1.12.22) [Algebraic and Numerical Equivalences]. Let $\mathcal{L}_1, \mathcal{L}_2$ be algebraically equivalent line bundles on a proper scheme X/k, then $\deg_{\mathcal{L}_1}(X) = \deg_{\mathcal{L}_2}(X)$. In particular, algebraically equivalent divisors are numerically equivalent. ⌟

Proof: This is because in this case $\mathcal{L}_1, \mathcal{L}_2$ are in the same connected component of $\underline{\mathrm{Pic}}_{X/k}$. □

Cor. (8.1.12.23). Let X be a complete prevariety over K and L_i be line bundles and $Z \in Z_r(X)$, then $\deg(c_1(L_1).c_1(L_2).\ldots.c_r(L_r).Z)$ only depends on algebraic equivalence classes of L_i. ⌟

Proof: Cf.[Diophantine Geometry, P562]. □

Def. (8.1.12.24) [Bounded Set of Line Bundles]. Let X be a scheme over S, then a set $\Lambda \subset \mathrm{Pic}(X_k)$ where $\mathrm{Spec}\, k \to S$ are points are called **bounded** if there is a $T \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}}/S$ and a line bundle $\mathcal{M}$ on X_T s.t. for any $\mathcal{L} \in \Lambda$, there is some schematic point $\mathrm{Spec}\, k \to T$ s.t. $\mathcal{L} \cong \mathcal{M}_k$. ⌟

Prop. (8.1.12.25) [Numerical and τ-Equivalence]. If X is proper over an alg.closed field k and $\mathcal{L} \in \mathrm{Pic}(X)$, then the following are equivalent:

- $\mathcal{L}$ is τ-equivalent to $\mathcal{O}_X$.
- $\mathcal{L}$ is numerically equivalent to $\mathcal{O}_X$.
- The family $\{\mathcal{L}^{\oplus p} | p \in \mathbb{Z}\}$ is bounded.
- For any $\mathcal{F} \in \mathcal{C}\mathrm{oh}(X)$, $\chi(\mathcal{F} \otimes \mathcal{L}) = \chi(\mathcal{F})$.
- For any $p \in \mathbb{Z}$, $\mathcal{L}^{\oplus p}(1)$ is ample.
-

⌟

Proof: Cf.[Kle05]P52, 57. is this true for k separably closed**?** □

Prop. (8.1.12.26). If X is projective over an alg.closed field k, then the set of line bundles numerically equivalent to $\mathcal{O}_X$ is bounded. ⌟

Proof: See the proof of [Kle05]P52. □

Prop. (8.1.12.27). If X is projective over an alg.closed field k, then there exists an $m \in \mathbb{Z}$ s.t. for any $\mathcal{L} \in \mathrm{Pic}(X)$ numerically equivalent to $\mathcal{O}_X$, $\mathcal{L}$ is m-regular and $\chi(\mathcal{L}(n)) = \chi(\mathcal{O}_X(n))$ for any $n \in \mathbb{Z}$. ⌟

Proof: Cf.[Kle05]P55. □

Nef Line Bundles

Def. (8.1.12.28) [Nef Line Bundles]. A **nef line bundle** or **numerically effective line bundle** on a complete prevariety over a field k is a line bundle $\mathcal{L}$ s.t. $c_1(\mathcal{L}).C \geq 0$ for any complete precurve $C \subset X$.

Nef line bundles form a semigroup, and are stable under proper pullbacks, by(6.12.2.7)(6.12.2.5). ⌟

Prop. (8.1.12.29). Ample line bundles are nef, by(6.12.2.20). ⌟

Surface Case

Def. (8.1.12.30) [(−1)-Curves]. Let X be a complete curve over a field k, then a (-1)**-curve** on X is a curve C consisting of smooth points, $C \cong \mathbb{P}^1_k$ and $C \cdot C = -1$. ⌟

Prop. (8.1.12.31) [Hodge Index Theorem]. Let X is a smooth surface over a field k and $\mathcal{L}, \mathcal{H} \in \mathrm{Pic}(X)$ with $\mathcal{H} \cdot \mathcal{H} > 0$ and $\mathcal{L} \cdot \mathcal{H} = 0$, then $\mathcal{L} \cdot \mathcal{L} = 0$, and the equality holds iff $\mathcal{L}$ is numerically trivial. ⌟

Proof: Cf.[Rising Sea, P552]. □

Prop. (8.1.12.32) [$\mathbb{P}^1 \times \mathbb{P}^1$]. Let $X = \mathbb{P}^1 \times \mathbb{P}^1$, $l = \mathbb{P}^1 \times \{0\}$ and $m = \{0\} \times \mathbb{P}^1$, then $l \cdot l = m \cdot m = 0$, and $l \cdot m = 1$. ⌟

8.2 Algebraic de Rham Cohomology

Main references are [algebraic de Rham Cohomology, Clausen] and [Gro15].

Notation (8.2.0.1).

- Use notations from Spectral Algebraic Geometry(Lurie).

⌟

1 de Rham Complexes

Def. (8.2.1.1) [Absolute de Rham Complex]. For $B \in \mathcal{CR}\mathrm{ing}$, let $\Omega_B = \Omega_{B/\mathbb{Z}}$, and $\Omega^i_B = \wedge^i \Omega_B$, then there is a **total de Rham complex** of B:

$$B \to \Omega^1_B \to \Omega^2_B \to \dots$$

as B-modules, which is a complex, where $d(b_0 db_1 \wedge \dots \wedge db_p) = db_0 \wedge db_1 \dots db_p$. ⌟

Proof: d is well-defined on Ω^1_B because it vanishes on the element $d(a+b) - da - db$ and $d(ab) - ad(b) - bd(a)$ by Leibniz rule, and the we get a map

$$\bigotimes_1^p \Omega_B \to \Omega^{p+1}_B : \omega_1 \otimes \dots \omega_p \mapsto \sum (-1)^{i+1} w_1 \wedge \dots \wedge d(\omega_i) \wedge \dots \wedge \omega_p.$$

We want to descend this to a map on Ω^p_B using(5.1.1.21): it is clearly alternating, and it suffices to show it is f-linear, and this is clear by direct calculation.

Finally $d^2 = 0$. □

Prop. (8.2.1.2)[Quotient of de Rham Complexes]. Let B be a ring and $\pi : \Omega_B \to \Omega$ be a surjective map of B-modules. Denote $d : B \to \Omega_B \to \Omega$, and $\Omega^i = \wedge^i \Omega$. Assume that the kernel of π is generated as a B-module by elements ω that $\wedge^2(\pi)(d_B(\omega)) = 0$ in Ω^2, then there is a de Rham complex

$$B \to \Omega^1 \to \Omega^2 \to \dots$$

whose differential is defined by the rules similar to that of(8.2.1.1). ⌟

Proof: Because π is surjective, so do $\wedge^i \pi$, and it suffices to show $\wedge\pi$ gives a connnecting morphism between $\Omega^\bullet_B$ and $\Omega^\bullet$, then the well-definedness of d is automatic. Cf.[[Sta]07HY]. □

Cor. (8.2.1.3) [Relative de Rham Complex]. If B is an A-algebra, the surjection $\Omega_B \to \Omega_{B/A}$ satisfies the condition of(8.2.1.2) thus we can define the **relative de Rham complex** $\Omega^\bullet_{B/A}$. ⌟

Proof: The verification of the condition is routine. □

Prop. (8.2.1.4) [Universality of de Rham Complexes]. Let C be a B-algebra and $(E^\bullet, d)$ a non-negatively graded commutative B-dga and we are given a B-algebra map $\eta : C \to E^0$ that for every $x \in C$, the element $d(\eta(x)) \in E^1$ satisfies $d^2 = 0$, then the map $C \to E^0$ extends uniquely to a map $\Omega^\bullet_{C/B} \to E^\bullet$ of B-dga. ⌟

Proof: One direction is trivial as $\Omega^\bullet_{C/B}$ is strict by construction. Conversely, the composite map $C \to E^0 \to E^1$ is a B-derivation thus extends to a map $\eta^1 : \Omega^1_{C/B} \to E^1$, then the universal property of the exterior product(5.1.1.21) gives maps $\eta^i : \Omega^i_{C/B} \to E^i$, and this gives the desired extension. □

Def. (8.2.1.5) [Connection]. Let B be a ring and $\Omega_B \to \Omega$ be a quotient satisfying the condition of(8.2.1.2), then a **connection** on M is an additive map

$$\nabla : M \mapsto M \otimes_B \Omega : \quad \nabla(b \otimes m) = b\nabla(m) + m \otimes db$$

Given a connection on M, we can define maps

$$\nabla : M \otimes_B \Omega^i \to M \otimes_B \Omega^{i+1}, \quad \nabla(b \otimes \omega) = \nabla(b) \wedge \omega + m \wedge d\omega$$

This is well defined because it commutes it commutes with B-action. The connection is called **integrable** if $\nabla^2 = 0$. ⌟

Def. (8.2.1.6) [Algebraic de Rham Cohomology]. Let $X \to S$ be a morphism of rings, then we define the **algebraic de Rham cohomology** $H^\bullet_{\mathrm{dR}}(X/S)$ of X over S as the image of the de Rham complex $\Omega^\bullet_{X/S}$ in $D(\mathcal{M}\mathrm{od}(\mathcal{O}_X))$.

Notice that if X is affine, then by(6.5.5.1) and(6.7.1.3), $H^n_{\mathrm{dR}}(\Omega^\bullet_X) = H^n(\Gamma(X, \Omega^\bullet_{X/S}))$. ⌟

Prop. (8.2.1.7). There is a similar construction of connections on a f.g. projective R-module M and Weil-Chern theory parallel to that of 3 and 3.

But in this case, the trace map is defined only when M is f.g. projective, which is called the **Hattoris-Stallings trace**: If A is f.g. projective, the natural map $\mathrm{Hom}_R(A, R) \otimes_R A \to \mathrm{End}_A(P)$ is an isomorphism (Because locally it is an isomorphism**??**), and the inverse composed with $\mathrm{Hom}_R(A, R) \otimes_R A \to A$, we get the desired map.

Also, when M is f.g. projective, there is a **Levi-Cevita connection** induced by the $A \to \Omega^1_{A/R}$ because M is a direct summand of some A^n. This is verified to be independent of n, or one can more alggeoly use the fact that projective module is locally free.

The Chern character is important, it defines a ring map from $K_0(R)$ to $H^{ev}_{dR}(A)$. In fact, this can be lifted to a morphism $K_0(A) \to HC_0^{\mathrm{perf}}(A) \to H^{ev}_{\mathrm{dR}}(A)$, Cf.[阳恩林 循环同调 Dennis trace]. ⌟

Prop. (8.2.1.8) [Grothendieck]. For $X \in \mathcal{S}\mathrm{ch}^{\mathrm{sm}}/\mathbb{C}$, there is a functorial equivalence

$$R\Gamma(X; \Omega^\bullet_{X/\mathbb{C}}) \cong R\Gamma(X^{\mathrm{an}}; \Omega^{\mathrm{an},\bullet}_{X^{\mathrm{an}}/\mathbb{C}}).$$

⌟

Proof: □

Remark (8.2.1.9). Notice if X is smooth and proper, then this follows from GAGA. ⌟

Curve case

Prop. (8.2.1.10). Let Y be a smooth curve over $\mathbb{C}$ with a smooth completion X, and denote $S = X \backslash Y$. Then there is an exact sequence of sheaves

$$0 \to \Omega^\bullet_X \to \Omega^\bullet_X(\log S) \xrightarrow{\mathrm{res}} i_*\Omega^{\bullet-1}_S \to 0, \textbf{?}$$

inducing a ⌟

Thm. (8.2.1.11) [Deligne]. Situation as in(8.2.1.10), there is a canonical isomorphism

$$\mathbb{H}^n(\Omega^\bullet_X(\log S)) \cong \mathbb{H}^n(\Omega^\bullet_Y).$$

⌟

2 Infinitesimal Sites

3 Cup Products

Def. (8.2.3.1) [Hodge Cohomologies]. For a morphism $f : X \to S$, define the **Hodge cohomology** to be the graded $H^0(S, \mathcal{O}_S)$-algebra

$$H^*_{\mathrm{Hdg}}(X/S) = \bigoplus_{n\geq 0} H^n_{\mathrm{Hdg}}(X/S) = \bigoplus_{n\geq 0} \bigoplus_{p+q=n} H^p(X, \Omega^q_{X/S})$$

with cup product given by**?**. It is associative and graded commutative. And $S \mapsto H^*_{\mathrm{Hdg}}(X/S)$ is compatible with base change. ⌟

Proof: Cf.[Sta]0FM5. □

Prop. (8.2.3.2) [Hodge-to-deRham Spectral Sequence]. There is a spectral sequence convergence

$$E_1^{p,q} = H^q(X; \Omega^q) \implies H^n_{\mathrm{dR}}(X/\mathbb{C}).$$

And its E_2-page is given by $H^q(X; R^p\Omega)$. ⌟

Proof: **?** □

4 Poincaré Duality

Def. (8.2.4.1) [Situation]. Let S be a qcqs scheme and $f : X \to S$ is a proper smooth morphism of schemes whose fiber are all equidimensional of dimension d. ⌟

Prop. (8.2.4.2) [Relative Poincaré duality]. In situation(8.2.4.1) there is a canonical $\mathcal{O}_S$-module map

$$t : Rf_*\Omega^d_{X/S}[d] \to \mathcal{O}_S$$

s.t. for any p, the pairing

$$Rf_*\Omega^p_{X/S} \otimes^{\mathrm{L}}_{\mathcal{O}_S} Rf_*\Omega^{n-p}_{X/S} \to \mathcal{O}_S$$

induced from relative cup product and t is a perfect pairing of perfect complexes in $D(\mathcal{O}_S)$ that is compatible perfect under base change. And it also induces a perfect $\mathcal{O}_S$-bilinear pairing

$$f_*\mathcal{O}_X \otimes R^d f_*\Omega^d_{X/S} \to \mathcal{O}_S$$

compatible with base change. ⌟

Proof: Cf.[Sta]0G8I. □

Cor. (8.2.4.3). If S is Noetherian and X is a proper smooth variety over S, then there is an isomorphism $R^d f_*\Omega^d_{X/S} \cong \mathcal{O}_S$ that is compatible with base change. ⌟

8.3 Étale Fundamental Groups

References are[K-M85].

1 Étale Connected Components

Def. (8.3.1.1) [Étale Connected Components]. Let X be a scheme over a field k, let $\pi_0(X) = \mathrm{Spec}(\pi(X))$, where $\pi(X)$ is the largest étale subalgebra of $\Gamma(X, \mathcal{O}_X)$(5.4.7.23). ⌟

Prop. (8.3.1.2). Let X be a locally algebraic scheme over a field k, then

- for any field extension k'/k, $\pi_0(X_{k'}) = \pi_0(X)_{k'}$.
- Let Y be a schemes over a field k, then $\pi_0(X \times Y) = \pi_0(X) \times \pi_0(Y)$.

⌟

Proof: 1: Cf.[Mil17b]P15.

2: There is a map $\pi(X) \times_k \pi(Y) \to \pi(X \times Y)$. Because π commutes with base change, we can base change to separable closure. In this case, it suffices to show if X, Y is connected then $X \times Y$ is connected, but this follows from(6.4.3.12). □

Prop. (8.3.1.3). Let X be a locally algebraic scheme over a field k, then

- The mapping $\varphi : X \to \pi_0(X)$ induces a 1 to 1 correspondence of points of $\pi_0(X)$ and connected components of X.
- For all $x \in \pi_0(X)$, the fiber $\varphi^{-1}(x)$ is geo.connected over $k(x)$.
- $X \to \pi_0(X)$ is faithfully flat.

⌟

Proof: $\pi_0(X)$ is discrete, so the inverse image of each point is a sum of connected components of X. But this must be connected, because $\pi_0(X_{k(x)}) = \pi_0(X)_{k(x)} = k(x)$. Also, this implies for the alg.closure $\overline{k}$ of $k(x)$, $\pi_0(X_{\overline{k}}) = \pi_0(X_{k(x)})_{\overline{k}} = \overline{k}$, thus $X_{\overline{k}(x)}$ is geo.connected. □

2 Étale Fundamental Groups

Main references are [Sta]Chap53 and [Fu11]Chap3.

Lemma (8.3.2.1) [Rigidity Lemma]. If $f, g : S' \to S''$ are two S-morphisms where S'' is a separated étale S-scheme and $(S', \overline{s}')$ is a pointed scheme that $f(\overline{s}') = g(\overline{s}')$, then $f = g$. ⌟

Proof: The diagonal $S'' \to S'' \otimes_S S''$ is a closed immersion and also étale hence open(6.6.6.3), so the diagonal is an clopen subset. And now $f \times g : S' \to S'' \otimes_S S''$ intersects the diagonal, and S' is connected, so f, g are identical on the diagonal. □

Def. (8.3.2.2) [Galois Cover]. If $(S, \overline{s})$ is a pointed connected scheme, $S' \to S$ is a finite étale cover of degree n, then there are at most n point over $\overline{s}$, so by(8.3.2.1), $|\,\mathrm{Aut}(S'/S)| \leq n$. If the equality holds, then we call S'/S a **Galois cover** and define $\mathrm{Gal}(S'/S) = \mathrm{Aut}(S'/S)^{op}$. ⌟

Prop. (8.3.2.3). If $S' \to S$ is a connected finite étale cover, then there is a finite étale cover $S'' \to S'$ that $S'' \to S$ is Galois. ⌟

Proof: Cf.[SGA1, Exp.V, §2 − §4]. □

Def. (8.3.2.4)[Étale Fundamental Group]. For any two finite Galois étale cover $S'/S, S''/S$, if there is a S-morphism $S'' \to S'$, then it induces a morphism of Galois groups because the Galois group of S' acts transitively on the fiber over a closed point. And it is surjective by the same reason for S''.

Then we define the **étale cohomology group**

$$\pi_1(S,x) = \varprojlim_{(S',\overline{x}')} \operatorname{Gal}(S'/S)$$

⌟

Prop. (8.3.2.5)[Fundamental Group and Covers]. For X connected smooth scheme and $\overline{x} \to X$ a geometric point, there is a profinite group $\pi_1(X,\overline{x})$ that there is a correspondence:

$$\{\text{finite étale covers } Y \to X\} \leftrightarrow \{\text{Finite sets with a continuous action of } \pi_1(X,x)\}$$

Such a group $\pi_1(X,\overline{x})$ is called the **étale fundamental group** of X w.r.t $\overline{x}$. ⌟

Proof: ? □

Prop. (8.3.2.6). Let (S,s) be a connected scheme, then the functor $S' \mapsto S'_{\overline{s}}$ induces an equivalence of categories between the finite étale covers $S' \to S$ with the category of finite discrete $\pi_1(X,x)$-sets. ⌟

Proof: We may assume S' is connected, then use(8.3.2.3) to find a Galois cover $S'' \to S'$ that S''/S is Galois, then clearly there is a bijection

$$\operatorname{Gal}(S''/S)/\operatorname{Gal}(S''/S') \cong S'(s')$$

And any transitive discrete $\pi_1(X,x)$-sets arise this way.

To prove the essentially surjectivity and fully faithfulness, ? □

Cor. (8.3.2.7). The étale fundamental group is independent of the base point $\overline{s}$ chosen. ⌟

Proof: This is because for two profinite groups, if the categories of their finite sets are equivalent, then they are isomorphic?. □

Cor. (8.3.2.8) [Locally Constant Sheaves and Fundamental Group]. By(8.4.2.19), if X is a connected scheme and $\overline{x}$ be a geometric point of X, then there is an equivalence of categories between finite locally constant Abelian sheaves on X and finite $\pi_1(X,\overline{x})$-modules. ⌟

Prop. (8.3.2.9). For k alg.closed, $\pi_1(\mathbb{P}^1_k) = 0$. ⌟

Proof: □

Prop. (8.3.2.10)[Arithmetic Geometric Exact Sequence]. If X_0 is a variety over $\mathbb{F}_q$, then there is an exact sequence

$$1 \to \pi_1(X,\overline{x}) \to \pi_1(X_0,\overline{x}) \to G(\overline{k}/k) \to 1.$$

⌟

8.4 Étale Cohomology Theory

Basic references are [Fu11], [Sta], [Étale Cohomology, Tamme], [Mil13b], [Con15] and [Notes on étale cohomology of number fields,. Ann. Sci. Éc. Norm. Super. (4) 6, 521–552 (1973), Mazur].

Notation (8.4.0.1).

- Use notations defined in Cohomology of Schemes.
- Use notations defined in More Properties of Morphisms between Schemes.

⌟

1 Basics

Prop. (8.4.1.1). For $X \in \mathcal{S}\mathrm{ch}$, the étale site $X_{\text{ét}}$ is a ringed site, $\mathcal{S}\mathrm{h}(X_{\text{ét}})$ is a Grothendieck Abelian category, and we can define right derived functors of any left exact functor, by(6.3.1.1). ⌟

Étale Topoi

Prop. (8.4.1.2) [Zariski-Étale Comparison]. For $X \in \mathcal{S}\mathrm{ch}$, the inclusion $X_{\mathrm{Zar}} \to X_{\text{ét}}$ of topologies which is a morphism of sites $\varepsilon : X_{\text{ét}} \to X_{\mathrm{Zar}}$, for any $\mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\text{ét}})$, there is a Leray spectral sequence(6.3.1.8)

$$E_2^{pq} = H^p_{\mathrm{Zar}}(X, R^q\varepsilon_*(\mathcal{F})) \Rightarrow \mathrm{H}^{p+q}_{\text{ét}}(X, \mathcal{F}).$$

⌟

Def. (8.4.1.3) [Pushforward & Pullback]. For a morphism of schemes $X \to Y$, there is a continuous functor between sites $f_{\text{ét}} : Y_{\text{ét}} \to X_{\text{ét}}$, which preserves final objects and finite fiber products, so by(6.1.2.14), it induces a morphism of sites(6.1.1.5) $f_{\text{ét}} : X_{\text{ét}} \to Y_{\text{ét}}$, which induces a morphism of topoi

$$f_{\text{ét}} : \mathcal{S}\mathrm{h}(X_{\text{ét}}) \to \mathcal{S}\mathrm{h}(Y_{\text{ét}}).$$

$f^*_{\text{ét}}$ is called the inverse image, it is exact. By definition(6.1.2.11), for $\mathcal{F} \in \mathcal{S}\mathrm{h}(Y_{\text{ét}})$ and $X \in X_{\text{ét}}$, $f^*\mathcal{F}(X')$ equals the colimit over all pairs (Y', φ) where $Y' \in Y_{\text{ét}}$ and $\varphi : X' \to Y' \times_Y X$, equivalently, all $X' \to Y'$ over Y. ⌟

Cor. (8.4.1.4) [Localizations]. By(6.1.2.25), an object $i : X' \to X \in X_{\text{ét}}$ induce a morphism $({}_s i, i^s)$ of topoi $X'_{\text{ét}} \to X_{\text{ét}}$.

Denote $i^s\mathcal{F} = F/X'$, then for $Z' \in X'_{\text{ét}}$, by(6.3.1.4) and(6.1.2.25)

$$F/X'(Z') = F(Z'), \quad H^q(X_{\text{ét}}; Z', F) \cong H^q(X'_{\text{ét}}; Z', F/X').$$

In particular,

$$H^q(X_{\text{ét}}; X', \mathcal{F}) = H^q(X'_{\text{ét}}; X', \mathcal{F}|_{X'}),$$

thus we will omit the ambient sites and the restriction of sheaves, which should cause no confusion. ⌟

Prop. (8.4.1.5). If Z is étale over X, then the canonical morphism

$$f^* \mathrm{Hom}_X(-, Z) \to \mathrm{Hom}_Y(-, Z \times_X Y)$$

is an isomorphism. ⌟

Proof: By definition, $f^* \operatorname{Hom}_X(-,Z)$ is the sheaf associated to the presheaf $f_p \operatorname{Hom}_X(-,Z)$(6.1.2.11), which is identical to the presheaf $\operatorname{Hom}_Y(-,Z)$ on $Y_{\text{ét}}$, but it is already a sheaf(6.1.4.34). □

Prop. (8.4.1.6) [Relative Leray Spectral Sequence]. If $f : X \to Y, g : Y \to Z \in \mathcal{S}\mathrm{ch}$, then for any $\mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\text{ét}})$, there is a relative Leray spectral sequence(6.3.1.8)

$$E_2^{pq} = R^p g_*(R^q f_*(\mathcal{F})) \Rightarrow R^{p+q}(gf)_*(\mathcal{F}).$$

⌟

Cor. (8.4.1.7) [Leray Spectral Sequence]. For a morphism of schemes $f : X \to Y$ and $\mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\text{ét}})$, $Y' \in Y_{\text{ét}}$, there is a Leray spectral sequence**??**:

$$E_2^p = \mathrm{H}^p(Y', R^q f_*(\mathcal{F})) \Rightarrow \mathrm{H}^{p+q}(Y' \times_Y X, \mathcal{F})$$

⌟

Prop. (8.4.1.8) [Commutes with Colimits]. For $X \in \mathcal{S}\mathrm{ch}^{\mathrm{qcqs}}$, by(6.1.4.17)(6.1.4.20) and(6.3.1.14), $\mathrm{H}^q_{\text{ét}}(X,-)$ commutes with filtered colimits. ⌟

Prop. (8.4.1.9). Let $X, Y \in \mathcal{A}\mathrm{ff}$, then for any morphism of ringed sites $(g, g^\sharp) : (X_{\text{ét}}, \mathcal{O}_X) \to (Y_{\text{ét}}, \mathcal{O}_Y)$, there exists a unique morphism of schemes $f : X \to Y \in \mathcal{S}\mathrm{ch}$ s.t. $(g, g^\sharp)$ is 2-isomorphic to $(f, f^\sharp)$. ⌟

Proof: Cf.[Sta]04I6. □

Field case

Thm. (8.4.1.10) [Etále Sites over Fields]. The functor $f : X' \to X'(k_s)$ is an equivalence of topologies from the small étale site $(\operatorname{Spec}(k))_{\text{ét}}$ to the canonnical topology T_G on the category of G-sets, where $G = G(k_s/k)$.

In particular, any Abelian sheaf on $\operatorname{Spec}(k)_{\text{ét}}$ is representable by**?**. ⌟

Proof: First f maps a family of morphisms of schemes to a covering iff this family is a covering itself. This is because both are defined by set-theoretical surjectivity, and this is by(6.6.6.13).

Next we need to show this is an equivalence of categories. f has a left adjoint g because $X' \to \operatorname{Hom}_G(U, X'(k_s))$ is representable for any G-set U, because any G-set is equivalent to disjoint sums of G/H, and both category has arbitrary sums, so it suffice to prove for G/H, but this is represented by $\operatorname{Spec} k'$, where k' is the fixed field of H.

To prove $fg \cong \mathrm{id}$ and $gf \cong \mathrm{id}$, they commutes with direct sums, so the first one is true because $G/H \to fg(G/H) = \operatorname{Spec}(k_s)(k)$ is an isomorphism, and the second follows from(6.6.6.6) as all étale schemes over field k is a disjoint union of spectra of finite separable field extensions of k. □

Cor. (8.4.1.11) [Étale and Galois Cohomologies]. By(8.7.2.1),

$$\mathcal{S}\mathrm{h}((\operatorname{Spec} k)_{\text{ét}}) \to \mathcal{M}\mathrm{od}_G : \mathcal{F} \to \varinjlim_{k \subset k' \subset k^s} \mathcal{F}(\operatorname{Spec} k')$$

is an equivalence of categories, so

$$\mathrm{H}^q_{\text{ét}}(\operatorname{Spec} k, \mathcal{F}) \cong \mathrm{H}^q(G, \varinjlim_{k \subset k' \subset k^s} \mathcal{F}(\operatorname{Spec} k_s)).$$

In particular, if $k = k^s$, then $(\operatorname{Spec} k)_{\text{ét}}$ is equivalent to $\mathcal{A}\mathrm{b}$, and $\mathrm{H}^p_{\text{ét}}(\operatorname{Spec}(k), \mathcal{F}) = 0$ for $p > 0$. ⌟

Stalks

Def. (8.4.1.12) [Stalk]. By(8.4.1.10), for any scheme X and an arithmetic point $x : \operatorname{Spec} k \to X$, the section functor $F \to F(x)$ is an equivalence of categories from $(\operatorname{Spec} k)_{\text{ét}}$ to $\mathcal{A}\text{b}$. Thus for any $\mathcal{F} \in \mathcal{S}\text{h}(X_{\text{ét}})$, we can define the **stalk map**

$$\mathcal{S}\text{h}(X_{\text{ét}}) \to \mathcal{A}\text{b} : \mathcal{F} \mapsto (x^*\mathcal{F})(x).$$

⌟

Prop. (8.4.1.13). For any geometric point P of X,

- the stalk map is exact and commutes with colimits.
- For any morphism $u : P' \to P$ of geometric points over X, $\mathcal{F}_P \cong F_{P'}$.
- If $X \to Y$ is a morphism, then $(f^*F)_P \cong F_P$.

⌟

Proof: 1: taking stalk is a composition of f^* and taking section over P(which is an equivalence), so it is exact and commutes with colimits(8.4.1.3).

2, 3: Trivial. □

Prop. (8.4.1.14) [Stalk is Defined Naturally]. By the definition of f^*(6.1.2.11), if X' be an étale nbhd of P in X, i.e. $P \to X' \to X$, then

$$(f_{\text{ét}})_p(\mathcal{F}(P)) = \varinjlim_{X'} \mathcal{F}(X')$$

and $F_P = f^*F(P)$, thus there is a natural map $\varinjlim_{X'} F(X') \to F_P$.

Then we have:

$$\varinjlim_{X'} G(X') \to (G^\sharp)_P$$

for any presheaf G on $X_{\text{ét}}$. ⌟

Proof: Firstly $(f^\cdot)^\sharp(G) \cong (f^*G)^\sharp$ by(6.1.2.12). Then it suffices to prove that $G(P) \to G^\sharp(P)$ is an isomorphism for any presheaf G on $P_{\text{ét}}$. But this is because $P_{\text{ét}}$ is just $\mathcal{A}b$(8.4.1.10), and $P \xrightarrow{\text{id}} P$ is cofinal in the category of coverings of P. □

Cor. (8.4.1.15). For a morphism of schemes $X \to Y$ and P is a geometric point of Y, then

$$R^p f_*(F)_P \cong \varinjlim_{P \in Y'} H^p(X \times_Y Y', F).$$

⌟

Cor. (8.4.1.16). For $X = \operatorname{Spec} k$, the equivalence(8.4.1.10) of $X_{\text{ét}}$ with continuous G-modules are just induced by taking the stalk at $\operatorname{Spec} k_s$. ⌟

Prop. (8.4.1.17) [Exactness and Stalks]. The exactness, injectivity and surjectivity of maps of sheaves $F' \to F$ on $X_{\text{ét}}$ can be checked on stalks(8.4.1.12). ⌟

Proof: It suffices to prove the isomorphism case, because taking stalks are exact(8.4.1.13) and other maps can be characterized by isomorphisms.

Monomorphism: suppose not, if $s \in F'(X')$ is mapped to 0, by taking base change, we can assume $X' = X$, and then $0 = v(s)_{\overline{x}} = v_{\overline{x}}(s_{\overline{x}})$, thus $s_{\overline{x}} = 0$ by assumption. Now by(8.4.1.14), for any x there is an étale nbhd of x that s vanishes on it. So we find an étale covering of X that s vanishes, thus $s = 0$ because F' is a sheaf.

Epimorphism: Similarly, for any $v \in F(X')$, we can pass to the base change and assume $X' = X$, then find for each x a nbhd that comes from some $v(s_x)$, and they glue together to be a global section of $F'(X)$. □

Prop. (8.4.1.18) [Finite Morphism is Exact]. For a finite morphism f, f_* are exact on étale topos. ⌟

Proof: Check on stalks, □

Properties of Étale Cohomologies

Prop. (8.4.1.19) [Restriction to Small Sites]. If $\mathcal{F} \in \mathcal{S}\mathrm{h}_{\text{ét}}/S$, then the cohomology groups of $\mathcal{F}$ on S agrees with the cohomology of its restriction on $\mathcal{S}\mathrm{h}(S_{\text{ét}})$, by(6.3.1.4). ⌟

Prop. (8.4.1.20) [Čech Comparison, Arin]. If $X \in \mathcal{S}\mathrm{ch}$ is compact and any finite subset of X is contained in an open affine(e.g. X is quasi-projective), then for any covering $\mathcal{U} \in \mathrm{Cov}(\mathcal{S}\mathrm{ch}_{\text{ét}}/X)$ of X, $\check{H}(\mathcal{U}, -)$ is exact.

In particular, by(6.3.2.16), in this case, we can use Čech cohomology to calculate the étale cohomologies. ⌟

Proof: Cf.[Milne, Étale Cohomologies, Prop3.2.17]. □

Prop. (8.4.1.21) [Inverse Limits]. Let $(X_i)_I$ be a projective system in $\mathcal{S}\mathrm{ch}_{qc}$ with affine morphisms, $X_\infty = \varprojlim_{i\in I} X_i$. For any projective system of sheaves $(\mathcal{F}_i)_I, \mathcal{F}_i \in \mathcal{S}\mathrm{h}((X_i)_{\text{ét}})$, let $\mathcal{F}_\infty = \varprojlim_{i\in I} \mathcal{F}_i$, then there are isomorphisms

$$\varinjlim_{i\in I} \mathrm{H}^p_{\text{ét}}(X_i, \mathcal{F}_i) \cong \mathrm{H}^p_{\text{ét}}(X_\infty, \mathcal{F}_\infty).$$

⌟

Proof: Cf. SGA4, Prop7.5.8, or Artin 1962, Chap3.3.**?** □

Prop. (8.4.1.22) [Étale-Zariski Comparison for Qco Sheaves]. Recall by(6.1.4.36) if $M \in \mathcal{Q}\mathcal{C}\mathrm{oh}(X)$ then $\widetilde{M}$ is a fpqc sheaf on X, in particular an étale sheaf on X. Now the edge map of the Zariski-étale comparison for $\widetilde{M}$ is an isomorphism:

$$H^p_{\text{Zar}}(X, M) \cong \mathrm{H}^p_{\text{ét}}(X, \widetilde{M})$$

In particular, $\mathrm{H}^p_{\text{ét}}(X, \mathbb{G}_a) \cong H^p(X, \mathcal{O}_X)$, and the étale cohomology for Qco sheaves vanishes on affine schemes. ⌟

Proof: Cf.[Sta].

We show that $R^p\varepsilon^s(\widetilde{M}) = 0$ for $p > 0$, Cf.[Tamme P109]. Not hard. □

Prop. (8.4.1.23) [Galois Covering and Group Cohomology]. If $\mathcal{U} = \{Y \to X\}$ is a single Galois covering with Galois group G, $\mathcal{P}$ is a presheaf on $\mathcal{S}\mathrm{ch}/X$ s.t.**?** then $\check{H}^r(\mathcal{U}, \mathcal{P}) = H^r(G, \mathcal{P}(Y))$.

In particular, we may not use alternating complex to calculate the étale cohomologies. ⌟

Proof: □

Prop. (8.4.1.24) [Hochschild-Serre Spectral Sequences]. Let $X \in \mathcal{S}\mathrm{ch}$ and $Y \in X_{\text{ét}}$ be a Galois covering with Galois group Γ, then for any $\mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\text{ét}})$, there is a spectral sequence ⌟

Prop. (8.4.1.25) [Mayer-Vietoris Sequences]. Let $X \in \mathcal{S}\mathrm{ch}$ and $f : Y \to X \in X_{\text{ét}}, U \subset X$ s.t. $f(Y) \cup U = X$, then for any $\mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\text{ét}})$, there is a long exact sequence

$$0 \to \mathrm{H}^0_{\text{ét}}(X, \mathcal{F}) \to \mathrm{H}^0_{\text{ét}}(U, \mathcal{F}) \oplus \mathrm{H}^0_{\text{ét}}(Y, \mathcal{F}) \to \mathrm{H}^0_{\text{ét}}(f^{-1}(U), \mathcal{F}) \to \mathrm{H}^1_{\text{ét}}(X, \mathcal{F}) \to \dots$$

that is functorial in $\mathcal{F}$, by(6.3.1.11). ⌟

Def. (8.4.1.26) [Restricted Cohomologies]. Let $X \in \mathcal{S}\mathrm{ch}, Z \subset X$ be a closed subscheme, $U = X \backslash Z$, then there is a functor

$$\Gamma_Z(X, -) : \mathcal{S}\mathrm{h}(X_{\text{ét}}) \to \mathcal{A}\mathrm{b} : \mathcal{F} \mapsto \ker(\Gamma(X, \mathcal{F}) \to \Gamma(U, \mathcal{F})),$$

which is left exact as both $\Gamma(X, -)$ and $\Gamma(U, -)$ are.

The right derived cohomology of $H^r_Z(X, -)$, called the **cohomology of $\mathcal{F}$ with supports in Z**. ⌟

Prop. (8.4.1.27) [Excision Sequences]. Situation as in(8.4.1.26), for any $\mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\text{ét}})$, there is a functorial long exact sequence

$$\dots \to H^r_Z(X, \mathcal{F}) \to \mathrm{H}^r_{\text{ét}}(X, \mathcal{F}) \to \mathrm{H}^r_{\text{ét}}(U, \mathcal{F}) \to H^{r+1}_Z(X, \mathcal{F}) \to \dots .$$

⌟

Proof: Choose a functorial injective resolution(4.10.2.9), and this follows from the fact an injective sheaf is flabby(6.3.4.9). □

Prop. (8.4.1.28) [Excisions]. Let $X \in \mathcal{S}\mathrm{ch}, f : X' \to X \in X_{\text{ét}}$, $Z \subset X$ be a closed subset s.t. $Z' = f^{-1}(Z) \to Z$ is an isomorphism, and $f^{-1}(X\backslash Z, \mathcal{F}) \to X \backslash Z$ is an open immersion, then for $\mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\text{ét}})$, the canonical maps

$$H^r_Z(X, \mathcal{F}) \to H^r_{Z'}(X', \mathcal{F})$$

are isomorphisms. ⌟

Proof: As f^* is exact and preserves injectives by(6.3.4.2), it suffices to prove for $r = 0$. Let $U = X \backslash Z, U' = X' \backslash Z'$. If $s \in \Gamma_Z(X, \mathcal{F})$ restricts to $0 \in \Gamma_{Z'}(X', \mathcal{F})$, then s restricts to 0 in both X' and U. But $\{X', U\}$ is an étale covering of X, so $s = 0$.

Conversely, if $s' \in \Gamma_{Z'}(X', \mathcal{F})$, to show it comes from some $s \in \Gamma_Z(X, \mathcal{F})$, it suffices to show s' and $0 \in \Gamma(U, \mathcal{F})$ defines a cocycle in the Čech complex $\check{C}(\{X', U\}, \mathcal{F})$: They both restrict to $0 \in X' \cap U = U'$, and for $X' \times_X X'$, we can check on stalks: s' restrict to 0 on $U' \times_X U'$ from both sides, and on $Z' \times_X Z' \cong Z'$, the maps $Z' \times_X Z' \to Z$ are equal isomorphisms. □

Cor. (8.4.1.29) [Restricted Cohomology at a point]. Let $x \in X$ be a closed point, then for any $\mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\text{ét}})$, there is an isomorphism

$$H^p_x(X, \mathcal{F}) \cong \mathrm{H}^r_{\text{ét}}(\mathrm{Spec}\, \mathcal{O}^h_{X,x}, j^*\mathcal{F}).$$

⌟

Proof: Take limits over the affine étale nbhds of $x \in X$ and use(8.4.1.21). □

Strict Henselization

Def. (8.4.1.30). ⌟

Frobenius Actions

Notation (8.4.1.31). Use notations as in Frobenius. ⌟

Prop. (8.4.1.32) [Frobenius action on Étale Sheaves]. Let $k \in \mathtt{Field}^p, k \cong \mathbb{F}_{p^r}$ and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,ft}}/k, \mathcal{F} \in \mathcal{S}\mathrm{ch}(X_{\text{ét}})$, we have an isomorphism $\mathcal{F} \cong (\varphi_{r,X})_*\mathcal{F}$ which is the inverse of the isomorphisms

$$(\varphi_{r,X})_*(\mathcal{F})(U) = \mathcal{F}(\varphi_{r,X}^{-1}(U)) \xrightarrow{F_{U/X}^*} \mathcal{F}(U),$$

and its adjoint $\varphi_{r,X}^*\mathcal{F} \to \mathcal{F}$ is denoted by $\varphi_{\mathcal{F}}$.

Then $\varphi_{\mathcal{F}}$ commutes with tensor product and it is an isomorphism. ⌟

Proof: The adjoint is an isomorphism because φ^* induces equivalence of categories of étale site of $X_{\text{ét}}$ with itself, by(6.1.4.22). □

Prop. (8.4.1.33) [Compatibility of $\varphi_{\mathcal{F}}$ wit Pullbacks]. Let $k \in \mathtt{Field}^p, k \cong \mathbb{F}_{p^r}$ and $f : Y \to X \in \mathcal{S}\mathrm{ch}\,\mathrm{sep,ft}/k$ be separated, $\mathcal{F} \in \mathcal{S}\mathrm{ch}(X_{\text{ét}})$, then the morphism $\varphi_Y^* f^*\mathcal{F} \cong f^*\varphi_{r,X}^*\mathcal{F} \xrightarrow{f^*\varphi_{\mathcal{F}}} f^*\mathcal{F}$ is just $\varphi_{f^*\mathcal{F}}$. ⌟

Proof: Cf.[Fu11]P586. □

Prop. (8.4.1.34) [Compatibility of $\varphi_{\mathcal{F}}$ with Higher Direct Image]. Let $k \in \mathtt{Field}^p, k \cong \mathbb{F}_{p^r}$ and $f : X \to Y \in \mathcal{S}\mathrm{ch}\,\mathrm{sep,ft}/k$ be separated, $\mathcal{F} \in \mathcal{S}\mathrm{ch}(X_{\text{ét}})$, so we have a Cartesian diagram about $\varphi_{r,X}$ and φ_Y. Then the composition

$$\varphi_S^* R^i f_*\mathcal{F} \to R^i f_*\varphi_{r,X}^*\mathcal{F} \xrightarrow{R^i f_*(\varphi_{\mathcal{F}})} R^i f_*\mathcal{F}$$

is just $\varphi_{R^i f_*\mathcal{F}}$. ⌟

Proof: Cf.[Conrad L18 P4].**?** □

Cor. (8.4.1.35) [Compatibility of $\varphi_{\mathcal{F}}$ with Proper Pushforward]. If $X \to S$ is a separated morphism of f.t. between k-schemes and $\mathcal{F}$ is a torsion Abelian sheaf on $X_{\text{ét}}$, then the morphism

$$\varphi_{r,S}^* R^i f_!\mathcal{F} \to R^i f_!\varphi_{r,X}^*\mathcal{F} \xrightarrow{R^i f_!(\varphi_{\mathcal{F}})} R^i f_!\mathcal{F}$$

is just $\varphi_{R^i f_!\mathcal{F}}$. ⌟

Proof: Choose a compactification, the $j_!$ doesn't matter, so we finish by(8.4.1.34). □

Def. (8.4.1.36) [Frobenius Action on Compact Cohomology]. Let $k \cong \mathbb{F}_{p^r} \in$ p-$\mathtt{Field}$, $X_0 \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,ft}}/k, \mathcal{F}_0 \in \mathcal{S}\mathrm{h}((X_0)_{\text{ét}})$, $X = X_0 \times_k \overline{k}$, $\mathcal{F} = \mathcal{F}_0 \times_k \overline{k}$,

- As Fr_X is finite, by(8.4.5.4) it induces a pullback map $H^i_{\text{ét},c}(X, \mathcal{F}) \to H^i_{\text{ét},c}(X, \mathrm{Fr}_X^* \mathcal{F})$, which by composing with the natural isomorphism

$$\mathrm{Fr}_{\mathcal{F}} : \mathrm{Fr}_X^* \mathcal{F} = \mathrm{Fr}^*(X \to X_0)^*\mathcal{F}_0 = (X \to X_0)^*(\varphi_{r,X})^*\mathcal{F}_0 \overset{\varphi_{\mathcal{F}_0}(8.4.1.32)}{\cong} (X \to X_0)^*\mathcal{F}_0 = \mathcal{F}$$

  gives an endomorphism $\mathrm{Fr}_{\mathcal{F}}^* : H^i_{\text{ét},c}(X, \mathcal{F}) \to H^i_{\text{ét},c}(X, \mathcal{F})$, called the **geometric Frobenius action on the étale cohomology**.

- Similarly, there are natural isomorphisms

$$F_{\mathcal{F}} : F_X^*\mathcal{F} = F_X^*(X \to X_0)^*\mathcal{F}_0 \cong ((X \to X_0) \circ F_X)^*\mathcal{F}_0 = \mathcal{F},$$

  so we can define the action F_X^* on $H^i_{\text{ét},c}(X, \mathcal{F})$, called the **arithmetic Frobenius action on the étale cohomology**.

- Similarly, the natural isomorphisms $\varphi_{\mathcal{F}} : \varphi_{r,X}^*\mathcal{F} \cong \mathcal{F}$(8.4.1.32) defines an action $\varphi_{r,X}^*$ on $H^i_{\text{ét},c}(X, \mathcal{F})$, called the **absolute Frobenius action on the étale cohomology**.

⌟

Lemma (8.4.1.37). Situation as in(8.4.1.36), $\mathrm{Fr}_X^* \mathcal{F} = \varphi_{r,X}^* F_X^* \mathcal{F} \cong \varphi_{r,X}^*\mathcal{F} \xrightarrow{\varphi_{\mathcal{F}}} \mathcal{F}$ is just $\mathrm{Fr}_{\mathcal{F}}$, by(6.2.10.2). ⌟

Prop. (8.4.1.38) [Frobenius Actions are Compatible]. Situation as in(8.4.1.36), $\varphi_{r,X}^* = \mathrm{id}$ on $H^i_{\text{ét},c}(X, \mathcal{F})$.

In particular, (8.4.1.37) shows $\mathrm{Fr}_X^* = \varphi_{r,X}^* \circ F_X^*$ on $H^i_{\text{ét},c}(X, \mathcal{G})$, so F_X^* agrees with Fr_X^* on $H^i_{\text{ét},c}(X, \mathcal{F})$, which is $\overline{k}$-linear. We can calculate with either one of them, and denote it by F_X^*., called the **Frobenius action on compact étale cohomologies**. ⌟

Proof: Choose an injective resolution $\mathcal{F} \to \mathcal{I}^\bullet$, it suffices to show that

$$\Gamma(X, \mathcal{I}^\bullet) \to \Gamma(X, \varphi_*\varphi^*\mathcal{I}^\bullet) \xrightarrow{\varphi_{\mathcal{F}}} \Gamma(X, \varphi_*\mathcal{I}^\bullet)$$

is the identity. But notice by definition $\mathcal{I}^\bullet \to \varphi_*\varphi^*\mathcal{I}^\bullet \xrightarrow{\varphi_{\mathcal{F}}} \varphi_*\mathcal{I}^\bullet$ is the inverse of the isomorphism in(8.4.1.32). □

Kummer Theory

Prop. (8.4.1.39) [Kummer Sequence]. For $X \in \mathcal{S}\mathrm{ch}/\mathbb{Z}[\frac{1}{n}]$, there is an exact sequence in $\mathcal{S}\mathrm{h}(X_{\text{ét}})$:

$$0 \to \mu_{n,X} \to \mathbb{G}_{m,X} \xrightarrow{n} \mathbb{G}_{m,X} \to 0$$

⌟

Proof: The proof is similar to that of Artin-Schreier sequence(8.4.1.45), noticing that $A \to A[T]/(T^n - s)$ is an étale map. □

Cor. (8.4.1.40). For $X \in \mathcal{S}\mathrm{ch}/\mathbb{Z}[\frac{1}{n}]$, by(6.7.1.14), there is an exact sequence

$$0 \to H^0(X, \mathcal{O}_X^*)/nH^0(X, \mathcal{O}_X^*) \to H^1(X, \mu_n) \to \mathrm{Pic}(X)[n] \to 0$$

⌟

Cor. (8.4.1.41). If $X = \mathrm{Spec}\, A$ where A is a local ring and n is invertible in A, then $H^1(X, \mu_n) \cong A^*/(A^*)^n$.**?** ⌟

Proof: Cf.[Tamme, P110]. □

Cor. (8.4.1.42). If $k \in \texttt{Field}$, $k = k^{\text{sep}}$, $X \in \mathcal{S}\mathrm{ch}^{proper}_{\text{red}}/k$, and $n \in \mathbb{Z} \cap k^\times$, then $\mathrm{H}^1_{\text{ét}}(X, \mu_n) \cong \mathrm{Pic}(X)[n]$, by(6.11.1.12). ⌟

Artin-Schreier Theory

Prop. (8.4.1.43) [Characters of Finite Fields]. Any character $\psi : \mathbb{F}_q \to \overline{\mathbb{Q}}_\ell^\times$ can be extended to $\mathbb{F}_{q^n}$ by
$$\mathbb{F}_{q^n} \xrightarrow{\mathrm{tr}} \mathbb{F}_q \xrightarrow{\psi} \overline{\mathbb{Q}}_\ell^\times,$$
also denoted by ψ. ⌟

Def. (8.4.1.44) [Artin-Schreier Covering]. The **Artin-Schreier cover** of $\mathbb{A}^1$ is defined to be the finite Galois cover
$$\varphi : \mathbb{A}^1_{\mathbb{F}_q} \to \mathbb{A}^1_{\mathbb{F}_q} : x \mapsto x^q - x,$$
with the Galois group isomorphic to $\mathbb{F}_q$ via $a \mapsto (x \mapsto x + a)$. ⌟

Prop. (8.4.1.45) [Artin-Schreier Sequence]. For $X \in \mathcal{S}\mathrm{ch}/\mathbb{F}_p$, let $P = \mathrm{id} - \mathrm{Frob}$, then there is an **Artin-Schreier exact sequence** of étale sheaves
$$0 \to (\underline{\mathbb{Z}/(p)})_X \to (\mathbb{G}_a)_X \xrightarrow{P} (\mathbb{G}_a)_X \to 0$$
⌟

Proof: If $s \in \mathcal{O}_{X'}$ is in the kernel, then $s = s^p$, so it is locally constant and comes from the map $\mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_{X'}$. Conversely, for any $s \in \mathcal{O}_{X'}$, it suffices to find an étale cover that s is a p-th power in $\mathcal{O}_{X'_i}$. For this, it suffices to notice that for any p-ring A, $A[t]/(t^p - t - s)$ is free of rank p and étale over A. □

Cor. (8.4.1.46). If X has char p, then by the long exact sequence and (8.4.1.22), there is an exact sequence
$$0 \to H^0(X, \mathcal{O}_X)/P(H^0(X, \mathcal{O}_X)) \to H^1(X, (\mathbb{Z}/p\mathbb{Z})) \to H^1(X, \mathcal{O}_X)^F \to 0$$
where the last one is the fixed elements. ⌟

Cor. (8.4.1.47). If $X = \operatorname{Spec} A$ and $pA = 0$, then $\mathrm{H}^q_{\text{ét}}(X, \mathbb{Z}/p\mathbb{Z}) = \begin{cases} A/\operatorname{Im}((\mathrm{Frob} - \mathbf{1})|_A) & , q = 0 \\ 0 & , q \geq 1 \end{cases}$. ⌟

Cor. (8.4.1.48). if $k \in$ p-`Field`, $k = k^{\mathrm{sep}}$ and X is a reduced proper k-scheme, then $H^1(X, \mathbb{Z}/p\mathbb{Z}) = (H^1(X, \mathcal{O}_X))^F$. ⌟

2 Constructible Sheaves

Torsion Sheaves

Def. (8.4.2.1) [Torsion Sheaves]. For $\mathcal{C} \in \mathcal{S}\mathrm{ite}$, $\mathcal{F} \in \mathcal{S}\mathrm{h}(\mathcal{C}; \mathcal{S}\mathrm{et})$ is called a **torsion sheaf** iff it is associated to a presheaf of torsion Abelian groups. Equivalently, the canonical morphism $\varinjlim_n \mathcal{F}[n] \to \mathcal{F}$ is an isomorphism. The category of torsion sheaves on $\mathcal{C}$ is denoted by $\mathcal{S}\mathrm{h}_{\mathrm{tor}}(\mathcal{C})$. ⌟

Proof: It $\mathcal{F} = P^\sharp$, then consider $0 \to P[n] \to P \xrightarrow{n} P \to 0$. Because $\sharp$ is exact, $\mathcal{F}[n] = (P[n])^\sharp$. Then because $\sharp$ commutes with inductive limits and $P = \varinjlim_n P[n]$, it follows $\mathcal{F} = \varinjlim_n \mathcal{F}[n]$.

Conversely, if $\mathcal{F} = \varinjlim_n \mathcal{F}[n]$, then $\mathcal{F} = \varinjlim_n (\mathcal{F}^{\mathcal{PS}\mathrm{h}}[n])^\sharp = (\varinjlim_n \mathcal{F}[n])^\sharp$, and $\varinjlim_n \mathcal{F}^{\mathcal{PS}\mathrm{h}}[n]$ is presheaf of torsion Abelian groups. □

Remark (8.4.2.2). WARNING: For a torsion sheaf, $\mathcal{F}(U)$ need not be torsion Abelian, but this is the case if U is quasi-compact, Cf.[Tamme P146]. ⌟

Prop. (8.4.2.3) [Being Torsion is Local]. $\mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\text{ét}})$ is a torsion sheaf iff all stalks $\mathcal{F}_x$ are torsion. ⌟

Proof: By definition $\mathcal{F}$ is torsion iff $\varinjlim_n \mathcal{F}[n] \to \mathcal{F}$ is an isomorphism. Then use the fact isomorphisms are checked on stalks(8.4.1.17) and stalk maps are exact(8.4.1.13). □

Prop. (8.4.2.4). Let $f : X \to Y \in \mathcal{S}\mathrm{ch}$.

- If $\mathcal{F}$ is a torsion sheaf on Y, then $f^*\mathcal{F}$ is torsion sheaf on X.
- If f is qcqs and $\mathcal{F}$ is a torsion sheaf on X, then $R^q f_*\mathcal{F}$ are torsion sheaves on Y.

In particular, if X is qcqs and $\mathcal{F}$ is a torsion sheaf on X, then $\mathrm{H}^q_{\text{ét}}(X, F)$ are torsion for all q. ⌟

Proof: 1: This follows immediately from(8.4.2.3) and(8.4.1.13).

2: For any $y \in Y$, $(R^q f_* F)_{\overline{y}} \cong H^q(\overline{X}, \overline{F})$, where $\overline{X} = X \otimes_Y \overline{Y}$ and $\overline{Y}$ is the strict localization of Y in $\overline{y}$ by**?**. Now $\overline{F}$ is torsion sheaf by item1, and $\overline{X} \to \overline{Y}$ is also qcqs with $\overline{Y}$ being affine, so $H^q(\overline{X}, \overline{F})$ is torsion by item3, so $R^q f_* F$ is torsion by(8.4.2.3). □

Prop. (8.4.2.5). Let $X \in \mathrm{N}\,\mathcal{S}\mathrm{ch}_{\mathrm{qc}}$ and $x \subset X$, then

- for any torsion sheaf $\mathcal{F} \in \mathcal{S}\mathrm{h}(\mathrm{Spec}(\kappa(x))_{\text{ét}})$, the sheaves $R^p i_* \mathcal{F}$ are torsion sheaf for $p > 0$.
- $\mathrm{H}^p_{\text{ét}}(X, i_*\mathcal{F})$ are torsion for all $p > 0$.

⌟

Proof: 1: Cf.[Tamme P148]. Uses strict Henselization.

2: Consider the Leray spectral sequence $\mathrm{H}^p_{\text{ét}}(X, R^q i_* F) \Longrightarrow H^{p+q}_{\text{ét}}(\mathrm{Spec}(k(x)), F)$, the left term vanishes for $p \geq 0, q > 0$ by item1 and(8.4.2.4), and the right hand side vanish for $p + q > 0$ by(8.4.2.4), then it can be checked that $\mathrm{H}^p_{\text{ét}}(X, i_* F)$ are torsion for $p > 0$. □

Prop. (8.4.2.6). For a closed subscheme $i : Y \subset X$, $R^p i^!$ preserves torsion sheaves. ⌟

Proof: Cf.[Tamme P148]. □

Prop. (8.4.2.7). For a regular Noetherian scheme X, $\mathrm{H}^q_{\text{ét}}(X, \mathbb{G}_m)$ are torsion for $q \geq 2$. ⌟

Proof: Cf.[Tamme P149]. □

Prop. (8.4.2.8). For a torsion sheaf F, define $F(\ell) = \varinjlim_n F[\ell^n]$, so it is an ℓ-torsion sheaf, and in fact

$$\bigoplus_{\ell \in \mathbf{P}} F(\ell) = F$$

this is because this is true at the stalks, because stalks is exact and commutes with colimits(8.4.1.13).

So if X is qcqs, then $H^p(X, F) \cong H^p(X, F(l))$, which is the primary decomposition of $H^p(X, F)$. ⌟

Proof: □

Def. (8.4.2.9) [Cohomological Dimension]. If $X \in \mathcal{S}\mathrm{ch}_{\mathrm{qcqs}}/k$, $\ell \in \mathbf{P}$, define the **ℓ-adic cohomological dimension** of X as the smallest number $\mathrm{cd}_\ell(X) = n$ that $H^p(X, \mathcal{F})[\frac{1}{\ell}] = 0$ for all $p > n$ and $\mathcal{F} \in \mathcal{S}\mathrm{h}^{\mathrm{tor}}(X_{\text{ét}})$, and define the **cohomological dimension** $\mathrm{cd}(X)$ of X as the smallest number n that $H^p(X, F) = 0$ for all $p > n$ and $\mathcal{F} \in \mathcal{S}\mathrm{h}_{\mathrm{tor}}(X_{\text{ét}})$. Equivalently, $\mathrm{cd}(X) = \sup_{\ell \in \mathbf{P}}\{\mathrm{cd}_\ell(X)\}$. ⌟

Prop. (8.4.2.10). If $k \in \texttt{Field}$ and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}}/k$, then

$$\mathrm{cd}_\ell(X) \leq \begin{cases} 2\dim X + \mathrm{cd}_\ell(k) & \ell \neq \mathrm{char}\, k \\ \dim X + 1 & \ell = \mathrm{char}\, k \end{cases}.$$

⌟

Proof: □

Cor. (8.4.2.11). If $k \in \texttt{Field}, k = k^s$, then $\mathrm{cd}(X) \leq 2\dim X$. ⌟

Proof: □

Thm. (8.4.2.12) [Artin Vanishing]. If $k \in \texttt{Field}, k = k^{\mathrm{sep}}$ and $X \in \mathcal{A}\mathrm{ff}^{\mathrm{ft}}/k$, then $\mathrm{cd}(X) \leq \dim X$. ⌟

Proof: Cf.[Mil13b]P105.**?** □

Prop. (8.4.2.13) [Arc Descent for Étale Cohomology]. Let R be a ring and $\mathcal{G} \in \mathcal{S}\mathrm{h}^{\mathrm{tor}}_{\text{ét}}(\mathrm{Spec}\, R)$, and $\mathcal{F} : (\mathcal{S}\mathrm{ch}_{\mathrm{qcqs}}/R)^{\mathrm{op}} \to D^{\geq 0}(\Lambda)$ be the functor $(f : X \to \mathrm{Spec}\, R) \mapsto R\Gamma(X_{\text{ét}}, f^*\mathcal{G})$, then $\mathcal{F}$ satisfies arc-descent. ⌟

Proof: Cf.[Arc Topology, Bhatt, 5.4.] □

Constructible Sheaves

References are [Conrad notes, L3].

Prop. (8.4.2.14). If G is a commutative, finite and étale group scheme on X, the sheaf G_X represented by G is locally finite on $X_{\text{ét}}$.

Conversely, any locally constant sheaf on $X_{\text{ét}}$ is represented by a unique commutative étale group scheme over X, and it is finite if F has finite stalks. ⌟

Proof: Cf.[Tamme P152]. □

Def. (8.4.2.15)[Finite étale Sheaves]. For $X \in \mathcal{S}\mathrm{ch}$, a **finite étale sheaf** is a sheaf $\mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\text{ét}}; \mathcal{S}\mathrm{et})$ s.t. all its stalks are finite. ⌟

Def. (8.4.2.16) [Constructible étale Sheaves]. For $X \in \mathrm{N}\,\mathcal{S}\mathrm{ch}$, a **constructible étale sheaf** is a sheaf $\mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\text{ét}}; \mathcal{S}\mathrm{et})$ s.t. there is a stratification $\{X_i\}$ of X that $\mathcal{F}_{X_i}$ are all locally constant and finite(8.4.2.15). The category of constructible sheaves on X is denoted by $\mathcal{S}\mathrm{h}_{\mathrm{const}}(X_{\text{ét}}; \mathcal{S}\mathrm{et})$.

If moreover $\mathcal{F}$ is locally constant, i.e. $\mathcal{F}$ is locally constant and finite, then it is called a **lcc étale sheaf**. The category of lcc étale sheaves are denoted by $\mathcal{S}\mathrm{h}_{\mathrm{lcc}}(X_{\text{ét}}; \mathcal{S}\mathrm{et})$. ⌟

Prop. (8.4.2.17). $\mu_{n,X}$ is étale over X iff n is prime to the characteristic of all local residue fields of X. (Only unramifiedness is concerned, and it is fiberwise(5.4.6.6)). And we can compute the Kahler differential of $k[T]/(T^n - 1)$ vanish iff $n \neq 0$ in k.

In this case, μ_n is locally isomorphic to $(\mathbb{Z}/n\mathbb{Z})_X$, because for any affine open $U = \mathrm{Spec}\, A$, $U' = \mathrm{Spec}\, A[t]/(t^n - 1) \to U$ is étale and surjective(5.4.1.22) and U' has all n-th roots of unity, so $(\mu_n)_{\mathrm{Spec}\, U'} \cong (\mathbb{Z}/n\mathbb{Z})_{\mathrm{Spec}\, U'}$. ⌟

Example (8.4.2.18). For $n \in \mathbb{Z}_+$, $\mu_n \in \mathcal{S}\mathrm{h}_{\mathrm{const}}(\mathbb{Z}[\frac{1}{n}])$ but $\mu_n \notin \mathcal{S}\mathrm{h}_{\mathrm{lcc}}(\mathbb{Z}[\frac{1}{n}])$. ⌟

Proof: It is locally constant after the étale base change $\mathbb{Z}[\frac{1}{n}] \to \mathbb{Z}[\frac{1}{n}][\zeta_n]$. □

Prop. (8.4.2.19) [Properties of Constructible Sheaves].

- If $F \in \mathcal{S}\mathrm{h}(X_{\text{ét}})$ and X has a finite decomposition into constructible reduced subschemes X_i that F/X_i are locally constant, then F is constructible. The converse is also true if X is qcqs.
- Constructibility is a local property.
- Constructibility is stable under pullback, pushout and finite direct limits.
- Constructibility is stable $j_!$ for j qc étale.
- Subsheaves of a constructible sheaf are constructible.

⌟

Proof: Cf.[Tamme P155]. [Conrad L3 P2], [Étale Cohomology and Weil Conjecture P42]**?** □

Prop. (8.4.2.20) [Lcc Sheaves and Finite Étale Schemes]. The functor $X \mapsto \mathrm{Hom}_S(-, X)$ defines an equivalence of categories

$$\mathcal{S}\mathrm{ch}^{\text{fét}}/S \cong \mathcal{S}\mathrm{h}_{\mathrm{lcc}}(S_{\text{ét}}; \mathcal{S}\mathrm{et}).$$

⌟

Proof: The Yoneda functor is fully faithful, thus we need to show the essentially surjectivity. Notice first $\mathrm{Hom}_S(-, X)$ is locally constant finite: we can restrict to an open subset of S that the fiber are of fixed order n, and $X \to X \times_S X$ is étale and a closed immersion, thus $X \times_S X = X \coprod Y$, and Y is finite étale over X through π_1. Now by induction on the order of the fiber, $Y = X \otimes \Sigma'$ locally. So $X = S \times \Sigma$ locally, which means X represents the constant sheaf $\underline{\Sigma}$ locally.

To show that every locally constant finite étale sheaf is represented by a finite étale scheme, Cf.[Conrad Etale coh, P19]**?**. □

Prop. (8.4.2.21). If G is a commutative étale group scheme over X, then the sheaf G_X represented by G is constructible iff G is f.p. over X. ⌟

Proof: □

Prop. (8.4.2.22) [Locally Constancy and Specializations]. For $S \in \mathrm{N}\mathcal{S}\mathrm{ch}$ and $\mathcal{F} \in \mathcal{S}\mathrm{h}_{\mathrm{const}}(S_{\text{ét}})$, $\mathcal{F}$ is locally constant iff all the specialization maps for geometric points $\mathcal{F}_{\overline{s}} \to \mathcal{F}_{\overline{\eta}}$ are bijective. ⌟

Proof: If $\mathcal{F}$ is locally constant, because the conclusion is local, we may assume $\mathcal{F}$ is constant, then $\mathcal{F}_{\overline{s}} \to \mathcal{F}_\eta$ are all identities.

Conversely, for any geometric point s, $\Sigma = \mathcal{F}_s$ is finite by definition, thus there is an étale nbhd U of s that the map $\underline{\Sigma} \to \mathcal{F}$ induces an isomorphism on s-stalks, so this is an isomorphism for any geometric point linked to s by specialization, in particular the generic point of the irreducible component containing s and all the points in this irreducible component, thus $\mathcal{F}$ is constant on an open nbhd of s(because X is Noetherian thus has f.m. irreducible components), so $\mathcal{F}$ is locally constant because X is Noetherian. □

Prop. (8.4.2.23) [Constructible Sheaves are Noetherian]. $\mathcal{S}\mathrm{h}_{\mathrm{const}}(X_{\text{ét}})$ are exactly the Noetherian objects in $\mathcal{S}\mathrm{h}_{\mathrm{tor}}(X_{\text{ét}})$. ⌟

Proof: □

3 Base Changes

Prop. (8.4.3.1) [Proper Base Change]. If there is a Cartesian diagram

$$\begin{array}{ccc} X' & \xrightarrow{g'} & Y' \\ \downarrow{f'} & & \downarrow{f} \\ X & \xrightarrow{g} & Y \end{array}$$

that f is proper, then for any torsion sheaf $\mathcal{F}$ on Y', the base change maps(6.3.3.18)

$$g^* R^q f_* \mathcal{F} \to R^q f'_*(g'^* \mathcal{F})$$

are isomorphisms. ⌟

Proof: Cf.[Conrad L6]. □

Prop. (8.4.3.2) [Smooth Base Change]. If there is a Cartesian diagram

$$\begin{array}{ccc} X' & \xrightarrow{g'} & Y' \\ \downarrow{f'} & & \downarrow{f} \\ X & \xrightarrow{g} & Y \end{array}$$

that f is smooth, then for any $\mathcal{K}^\bullet \in D^+(X, \mathbb{Z}/(n))$, the base change map(6.3.3.18)

$$f^* R g_* \mathcal{K}^\bullet \to R g'_* f'^* \mathcal{K}^\bullet$$

is an isomorphism. ⌟

Proof: Cf.[Lei Fu, P391]. □

4 Lower Shriek Functor

5 Cohomology with Compact Support

Cf.[Weil1, P18].

Lemma (8.4.5.1). Extension by 0 commutes with pullback Cf.[KF Lemma4.9]. ⌟

Def. (8.4.5.2) [Higher Direct Images with Compact Support]. Let $Y \in \mathcal{S}\mathrm{ch}_{\mathrm{qcqs}}, f : X \to Y \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,ft}}/Y, \mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\text{ét}})$, then f factors as $f : X \overset{j}{\hookrightarrow} \overline{X} \xrightarrow{\overline{f}} Y$ where $j : X \to \overline{X}$ is an open dense subscheme and $\overline{f}$ is proper, by Nagata compactification(6.8.3.2), then we define the **higher direct image with compact support** as

$$R f_! = R\overline{f}_* j_! : D^+(X, \mathrm{tor}) \to D^+(Y, \mathrm{tor}).$$

Then this notion is well-defined.

And if $Y = \operatorname{Spec} k$, define $H^i_{\text{ét},c}(X, \mathcal{F}) = H^i(\operatorname{Spec} k, R f_! \mathcal{F})$, called the **étale cohomology with compact support**. ⌟

Proof: To show it is well-defined, notice for any two compactification, we can find a common compactification that dominates them both**?**, so using lemma(8.4.5.3), we easily show they are isomorphic. □

Lemma (8.4.5.3) [$i_!$ and Higher Pushforward]. If there is a commutative diagram

$$\begin{array}{ccc} X & \xhookrightarrow{i} & \overline{X} \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \overline{f}} \\ Y & \xhookrightarrow{j} & \overline{Y} \end{array}$$

where i, j are open immersion and $f, \overline{f}$ are proper, then there is a natural transformation $j_! f_* \to \overline{f}_* i_!$ that induces a natural transformation

$$j_! R f_* \to R\overline{f}_* i_!,$$

which is an isomorphism iff $\overline{f}$ is proper. ⌟

Proof: If this is a Cartesian diagram, then the natural transformation is give by

$$j_! f_* \to \overline{f}_* \overline{f}^* j_! f_* \cong \overline{f}_* i_! f^* f_* \to \overline{f}_* i_!.$$

(the second isomorphism is by(8.4.5.1)). The rest is by proper base change Cf.[KF P88].

The general case is also easily reduced to the Cartesian case.? □

Prop. (8.4.5.4) [Proper Map Induces Map on Proper Pushforward]. If $g : Y \to X, f : X \to S$ is a proper morphism between schemes separated of f.t. over a Noetherian scheme S, then for any étale Abelian sheaf $\mathcal{F}$ on X, there is a canonical mop

$$g : Rf_!(\mathcal{F}) \to R(f \circ g)_!(\mathcal{F})$$

⌟

Proof: Choose a compactification $X_2 \xrightarrow{j} \overline{X}_2$, then choose a compactification $X_1 \xrightarrow{i} \overline{X}_1$ of $i \circ g$, now Cf.https://math.stackexchange.com/questions/3120833/proper-morphism-induces-a-map-between-co
?. □

Prop. (8.4.5.5) [Properties of Compact Pushforwards].

- (Base Change) If there is a Cartesian diagram

$$\begin{array}{ccc} X' & \xrightarrow{h} & X \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} \\ S' & \xrightarrow{g} & S \end{array}$$

  that f is separated of f.t., then there is a natural isomorphism

$$g^* R f_! \cong R f'_! h^*$$

- (Composition) For two separated morphisms of f.t, $R(f_1 \circ f_2)_! = R(f_1)_! R(f_2)_!$, which induces a Leray spectral sequence.
- (Excision) Let $f : X \to S$ be a separated morphism of f.t, and $\mathcal{F} \in D^+_{\text{tor}}(X)$. Let $Z \subset X$ be a closed subscheme and $U = X \backslash Z$, then there is a long exact sequence

$$\cdots \to R^p(f_U)_!(\mathcal{F}|_U) \to R^p f_! \mathcal{F} \to R^p(f_Z)_!(\mathcal{F}|_Z) \to R^{p+1}(f_U)_!(\mathcal{F}|_U) \to \cdots$$

⌟

Proof: 1: Choose a compactification of f, then it suffices to show Rf^c_* and $j_!$ both commutes with base change, which is by proper base change(8.4.3.1) and(8.4.5.1).

2: Two compactification can be splinted, and use(8.4.5.3).

3: Use the long exact sequence applied to the exact sequence(checked on stalks(8.4.1.17))

$$0 \to j_! j^* F \to \mathcal{F} \to i_* i^* \mathcal{F} \to 0$$

□

Prop. (8.4.5.6)[Proper Pushforward to Direct Image]. There is a natural map from $R^i f_! \to R^i f_*$, which is induced by

$$R^i f_! = R^i \overline{f}_* j_! \to R^i \overline{f}_* j_* \to R^i f_*$$

where the second one is edge map of Leray spectral sequence.

In particular, there is a map $H^i_{\text{ét},c}(X, \mathcal{F}) \to \mathrm{H}^i_{\text{ét}}(X, \mathcal{F})$. ⌟

Prop. (8.4.5.7) [Vanishing Result]. If $f: X \to S \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,ft}}/S$ and let $d = \sup_{s\in S} \dim X_s$, then if $\mathcal{F} \in D(X, \mathrm{tor})$ satisfies $H^p(\mathcal{F})[p] = 0$ for $p \geq r$, then

$$R^p f_! \mathcal{F} = 0, \quad p \geq r + 2d.$$

⌟

Proof: Cf.[Conrad L10 P4]. □

Thm. (8.4.5.8) [Projection Formula]. If $f: X \to S$ is a quasi-projective morphism, $\mathcal{F} \in D^-(S)$ and $\mathcal{G} \in D(X)$, then we have a natural isomorphism

$$\mathcal{F} \otimes^L_S Rf_! \mathcal{G} \cong Rf_!(f^* \mathcal{F} \otimes^{\mathrm{L}}_X \mathcal{G})$$

⌟

Proof: We may pass to the compactification, as $j_!$ commutes with f^***?**. □

6 Torsion Cohomology

Finiteness Theorems

Prop. (8.4.6.1). If $S \in \mathcal{S}\mathrm{ch}$ is Noetherian, $f: X \to S \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,ft}}/S$, and $\mathcal{F} \in \mathcal{S}\mathrm{h}_{\mathrm{const}}(X_{\text{ét}})$ whose torsion order is invertible in S, then $R^p f_! \mathcal{F}$ are all constructible on Y. ⌟

Proof: Cf.[Conrad L10 P5]. □

Cor. (8.4.6.2). If X is a proper scheme over a separably closed field k and $\mathcal{F}$ is a constructible sheaf on $X_{\text{ét}}$, then $\mathrm{H}^p_{\text{ét}}(X, \mathcal{F})$ are finite for all $p \geq 0$. ⌟

Proof: □

Lemma (8.4.6.3). If $X \to S$ is smooth and proper, and F is a locally constant finite Abelian sheaf with torsion order invertible on S, suppose S is Noetherian, then all specialization maps for $R^p f_* \mathcal{F}$ are isomorphisms. ⌟

Proof: Cf.[Conrad L10 P5]. □

Prop. (8.4.6.4) [Proper Smooth Higher Direct Image of Lcc Sheaves]. If $X \to S$ is smooth and proper, and F is a lcc Abelian sheaf(8.4.2.15) with torsion order invertible on S, then $R^p f_* \mathcal{F}$ are locally constant finite sheaves for any $p \geq 0$. ⌟

Proof: By(8.4.2.20), we may assume $\mathcal{F} = \underline{X'}$ for some finite étale scheme $X' \to X$. By Noetherian descent**?** together with proper base change, we may reduce to the case S is Noetherian. Thus by(8.4.6.1), $R^p f_* \mathcal{F} = R^p f_! \mathcal{F}$ are constructible, and(8.4.6.3) shows that the stalk maps are isomorphisms. So(8.4.2.22) shows that $R^p f_* \mathcal{F}$ are locally constant finite. □

7 ℓ-adic Étale Cohomologies

Notation (8.4.7.1).

- Fix a CDVR $(\Lambda, \mathfrak{m}, K, \kappa)$ of mixed characteristic $(0, p)$ and suppose $\# \kappa < \infty$.
- Fix $S \in \mathcal{S}\mathrm{ch}$.
- Let $\Lambda_n = \Lambda / \mathfrak{m}^n$.

⌟

Artin-Rees Formalism

Def. (8.4.7.2). The **pre Artin-Rees category** of A-modules has objects $M_\bullet = (M_n)_{n \in \mathbb{Z}}$ which are projective systems of A-modules with $M_n = 0$ for $n << 0$, and the morphisms in this category are the elements of the set

$$\mathrm{Hom}_{\text{A-R}}(M_\bullet, N_\bullet) = \varinjlim \mathrm{Hom}(M_\bullet[d], N_\bullet)$$

An object $M^\bullet$ in the Artin-Rees category is called a **null system** if for some ≥ 0 the map $M_{n+} \to M_n$ vanishes for all n. ⌟

Prop. (8.4.7.3) [Artin-Rees Category]. The pre Artin-Rees category is an Abelian category, and the null systems form a Weak Serre subcategory. Then we define the **Arin-Rees category** as the quotient category. ⌟

Proof: □

Prop. (8.4.7.4). If the kernel and cokernel of two systems are all null systems, then they induce isomorphism on inverse limit. ⌟

Proof: Cf.[Conrad L15, P5]. □

Def. (8.4.7.5). An object $M^\bullet$ in the A-R category is called **Artin-Rees I-adic** if it is represented by a system M_n that $M_n = 0$ for $n < 0$ and M_n is finite over A_n, $M_{n+1} \otimes_{A_{n+1}} A_n \to M_n$ is an isomorphism for $n \geq 0$. ⌟

Prop. (8.4.7.6). The full subcategory of Artin-Rees I-adic modules is an Abelian category, and it is equivalent to the category of finite A-modules by the stalk functor. ⌟

Prop. (8.4.7.7). The category $\mathcal{S}\mathrm{h}_{\Lambda\text{-lcc}}(S_{\text{ét}})$ is equivalent to the full subcategory of $\mathcal{S}\mathrm{h}_{\mathfrak{m}}(S_{\text{ét}})$ consisting of objects with Artin-Rees property and that the terminal stable image is constructible. ⌟

Proof: □

Def. (8.4.7.8) [Strictly $\mathfrak{m}$-adic Sheaves]. The category $\mathcal{S}\mathrm{h}_{\mathfrak{m}\text{-strict}}(S_{\text{ét}})$ of **strict $\mathfrak{m}$-adic sheaves** are defined as before. ⌟

Prop. (8.4.7.9). We can strictify any $\mathfrak{m}$-adic sheaf, Cf.[Conrad, Etale Coh]. ⌟

Constructible and Lisse $\mathfrak{m}$-adic Sheaves

Def. (8.4.7.10) [Lisse Adic Sheaves]. For $S \in \mathcal{S}\mathrm{ch}$, $\mathcal{F} \in \mathcal{S}\mathrm{h}_{\mathfrak{m}}(S)$ is called **constructible $\mathfrak{m}$-adic sheaf** if it is isomorphic to a strict system $\{\mathcal{F}_n\}$ that $\mathcal{F}_n \in \mathcal{S}\mathrm{h}_{\Lambda_n\text{-const}}(S_{\text{ét}})$. The subcategory of constructible $\mathfrak{m}$-adic sheaves is denoted by $\mathcal{S}\mathrm{h}_{\mathfrak{m}\text{-const}}(S)$.

$\mathcal{F} \in \mathcal{S}\mathrm{h}_{\mathfrak{m}}(S)$ is called a **lisse $\mathfrak{m}$-adic sheaf** if it is isomorphic to a strict system $\{\mathcal{F}_n\}$ s.t. $\mathcal{F}_n \in \mathcal{S}\mathrm{h}_{\Lambda_n\text{-lcc}}(S_{\text{ét}})$. ⌟

Def. (8.4.7.11) [Tate Twist Sheaves]. The **Tate twist sheaf** $\Lambda(1)$ is defined to be**?**. It is invertible, thus we denote its dual by $\Lambda(-1)$. Then $\Lambda(r) \in \mathcal{S}\mathrm{h}_{\Lambda\text{-lcc}}(X_{\text{ét}})$ if p is invertible on X.

For any $\mathfrak{m}$-adic sheaf $\mathcal{F}$, denote $\mathcal{F}(1)$ to be the sheaf $\mathcal{F} \otimes \Lambda(1)$. Also denote $\Lambda(r) = \Lambda(1)^{\otimes r}$. ⌟

Def. (8.4.7.12) [Stalk Maps]. Let $s \to S$ be a arithmetic point, then there is a **stalk map**

$$\mathcal{S}\mathrm{h}_{\mathfrak{m}\text{-const}}(S) \to \mathcal{M}\mathrm{od}_{\Lambda}^{\mathrm{fin}} : \mathcal{F}_\bullet \mapsto \varprojlim_n (\mathcal{F}_n)_s.$$

It is well-defined by [Conrad, Etale Coh]P72. ⌟

Prop. (8.4.7.13). Constructibility/lisse are étale-local and stratification-local properties for $\mathcal{F} \in \mathcal{S}\mathrm{h}_{\mathfrak{m}}(S_{\text{ét}})$. ⌟

Proof: Cf.[Conrad, Etale Coh]P71. □

Prop. (8.4.7.14). The full subcategory $\mathcal{S}\mathrm{h}_{\mathfrak{m}\text{-lcc}}(S_{\text{ét}}) \subset \mathcal{S}\mathrm{h}_{\mathfrak{m}}(S_{\text{ét}})$ is stable under taking kernels and cokernels. ⌟

Prop. (8.4.7.15) [Constructible and Lisse $\mathfrak{m}$-adic Sheaves]. Let $S \in \mathrm{N}\,\mathcal{S}\mathrm{ch}$ and $\mathcal{F} \in \mathcal{S}\mathrm{h}_{\mathfrak{m}\text{-const}}(S_{\text{ét}})$, then there is a stratification of X that $\mathcal{F}$ is locally constant finite on each stratum. ⌟

Proof: Cf.[Conrad, Etale Coh]P73**?**.

By the stalk criterion of locally constant finite(8.4.2.22), a constructible extension of locally constant finite sheaves is also locally constant finite. So by the exact sequence $1 \to \ell^{n-1}\mathcal{F}_n \to \mathcal{F}_n \to \mathcal{F}_{n-1} \to 1$, iff we show there is a stratification that all $\ell^{n-1}\mathcal{F}_n$ are locally constant finite, then by induction all $\mathcal{F}_n$ are locally constant finite. But then $\ell^{n-1}\mathcal{F}_n$ is a descending chain of quotients of $\mathcal{F}_1$, thus the kernel is ascending thus stablizes because $\mathcal{F}_1$ is constructible(8.4.2.23), so there are only f.m. such $l^n\mathcal{F}_n$, so there is a common stratification. □

Cor. (8.4.7.16). Exactness/Isomorphism between constructible sheaves can be checked at stalks. ⌟

Def. (8.4.7.17) [Constructible K-Sheaves]. The category $\mathcal{S}\mathrm{h}_{K\text{-const}}(X_{\text{ét}})$ of **constructible K-sheaves** has the same object as $\mathcal{S}\mathrm{h}_{\mathfrak{m}\text{-const}}(X_{\text{ét}})$ but with the homomorphism groups

$$\mathrm{Hom}_{\mathcal{S}\mathrm{h}_{K\text{-const}}(S_{\text{ét}})}(\mathcal{F}, \mathcal{G}) = \mathrm{Hom}_{\mathcal{S}\mathrm{h}_{\mathfrak{m}\text{-const}}(S_{\text{ét}})}(\mathcal{F}, \mathcal{G}) \otimes_\Lambda K.$$

And there is a natural functor

$$K \otimes - : \mathcal{S}\mathrm{h}_{\mathfrak{m}\text{-const}}(X_{\text{ét}}) \to \mathcal{S}\mathrm{h}_{K\text{-const}}(X_{\text{ét}}).$$

Then a **lisse K-sheaf** is the image of a lisse $\mathfrak{m}$-adic sheaf. ⌟

Def. (8.4.7.18) [Tate Twist Sheaves]. Denote $K(r) = \Lambda(r) \otimes_\Lambda K$, also called the **Tate twist sheaf**. ⌟

Prop. (8.4.7.19) [Lisse K-Sheaves and $\pi_1(S,\overline{x})$-Representations]. Assume S is connected, then for an arithmetic point $\overline{s}$ of S, the stalk map $\mathcal{F} \to \mathcal{F}_{\overline{x}}$ induces equivalences:

$$\mathcal{S}\mathrm{h}_{\Lambda\text{-const}}(X_{\text{ét}}) \cong \mathrm{Rep}_\Lambda(\pi_1(S,\overline{s})), \quad \mathcal{S}\mathrm{h}_{K\text{-const}}(X_{\text{ét}}) \cong \mathrm{Rep}_K^{\mathrm{fd}}(\pi_1(S,\overline{s})).$$

⌟

Proof: The point is that by(18.3.1.3), any representation of $\pi_1(S,\overline{s})$ stabilizes some Λ-lattice. So by the equivalence(8.3.2.5)(8.4.2.20) and taking limit using(8.4.7.6), we get the result about $\mathcal{O}_E$-sheaves and representations of $\pi_1(X_0,\overline{s})$ over $\mathcal{O}_E$. □

Prop. (8.4.7.20) [Lisse and Specializations]. For $S \in \mathrm{N}\,\mathcal{S}\mathrm{ch}$ and $\mathcal{F} \in \mathcal{S}\mathrm{h}_{\mathfrak{m}\text{-const}}(S_{\text{ét}})$, then $\mathcal{F}$ is lisse iff all the specialization maps for geometric points $\mathcal{F}_{\overline{s}} \to \mathcal{F}_{\overline{\eta}}$ are bijective.

And if S is moreover normal, then the same holds for $\mathcal{F} \in \mathcal{S}\mathrm{h}_{K\text{-const}}(S_{\text{ét}})$. ⌟

Proof: We can assume $\mathcal{F}$ is strictly $\mathfrak{m}$-adic(8.4.7.10) and then use(8.4.2.22) on each $\mathcal{F}_n$.

For the second assertion, Cf.[Conrad, Etale Coh]P77. □

Cor. (8.4.7.21) [Étale Descent for Lisse K-Sheaves]. If S is Noetherian and normal, then étale descent holds for lisse K-sheaves. ⌟

Proof: ? □

Prop. (8.4.7.22). Constructible $\mathfrak{m}$-adic sheaves are Noetherian: Ascending chain of subsheaves stablizes. ⌟

Proof: Cf.[Conrad L16 P3]. □

Prop. (8.4.7.23). For any $\mathcal{F} \in \mathcal{S}\mathrm{h}_{\mathfrak{m}\text{-const}}(S_{\text{ét}})$, there exists some $\mathcal{G} \in \mathcal{S}\mathrm{h}_{\Lambda\text{-const}}(S_{\text{ét}})$ s.t. $\mathcal{G} \subset \mathcal{F}$ and $\mathcal{F}/\mathcal{G}$ has Λ-flat stalks.

In particular, any $\mathcal{F} \in \mathcal{S}\mathrm{h}_{K\text{-const}}(S_{\text{ét}})$ is K-isomorphic to some $K \otimes \mathcal{F}'$ where $\mathcal{F}'$ has Λ-flat stalks. ⌟

Proof: Cf.[Conrad Etale Coh]P75.? □

Def. (8.4.7.24) [Extensions]. Let Λ'/Λ be an extension, then we can define extension functors

$$\Lambda' \otimes_\Lambda - : \mathcal{S}\mathrm{h}_{\Lambda\text{-const}}(X_{\text{ét}}) \to \mathcal{S}\mathrm{h}_{\Lambda'\text{-const}}(X_{\text{ét}}), \quad K' \otimes_K - : \mathcal{S}\mathrm{h}_{K\text{-const}}(X_{\text{ét}}) \to \mathcal{S}\mathrm{h}_{K'\text{-const}}(X_{\text{ét}}).$$

? ⌟

$\mathfrak{m}$-adic Cohomologies

Prop. (8.4.7.25) [Direct Pushforward of $\mathfrak{m}$-adic Sheaves]. For a constructible $\mathfrak{m}$-adic sheaf $\mathcal{F}$ and a compatifiable morphism $X_0 \to S_0$, we can define $R^i f_*$ and $R^i f_!$ termwisely, and we have $R^i f_* \mathcal{F}$ is a constructible sheaf, hence so is $R^i f_!$. ⌟

Proof: Cf.[Weil Conjecture and Étale sheaves, P128]. □

Constructible and Lisse $\overline{\mathbb{Q}}_\ell$-Sheaves

Def. (8.4.7.26)[E-Sheaves]. The category $\mathcal{S}\mathrm{h}_{\overline{\mathbb{Q}}_\ell\text{-const}}(X_{\text{ét}})$ of **constructible $\overline{\mathbb{Q}}_\ell$-sheaves** are the direct limit of categories of $\mathcal{S}\mathrm{h}_{E\text{-const}}(X_{\text{ét}})$ for $E \in p$-`NField`.

The category $\mathcal{S}\mathrm{h}_{\overline{\mathbb{Q}}_\ell\text{-lcc}}(X_{\text{ét}})$ of **lisse $\overline{\mathbb{Q}}_\ell$-sheaves** are the direct limit of categories of $\mathcal{S}\mathrm{h}_{E\text{-lcc}}(X_{\text{ét}})$ for $E \in p$-`NField`. ⌟

Prop. (8.4.7.27) [Lisse $\overline{\mathbb{Q}}_\ell$-Sheaves and $\pi_1(S,\overline{x})$-Representations]. Assume S is connected, then for an arithmetic point $\overline{s}$ of S, the stalk map $\mathcal{F} \to \mathcal{F}_{\overline{s}}$ induces equivalences:

$$\mathcal{S}\mathrm{h}_{\overline{\mathbb{Q}}_\ell\text{-const}}(X_{\text{ét}}) \cong \mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(\pi_1(S,\overline{s})), \quad \mathcal{S}\mathrm{h}_{\Lambda\text{-const}}(X_{\text{ét}}) \cong \mathrm{Rep}^{\mathrm{fd}}_\Lambda(\pi_1(S,\overline{s}))$$

⌟

Proof: This follows from(8.4.7.19) and(18.3.1.3) by taking direct limit. □

Cor. (8.4.7.28) [Irreducible/Semisimple Lisse Sheaves]. $\mathcal{F} \in \mathcal{S}\mathrm{h}_{\overline{\mathbb{Q}}_\ell-\mathrm{lcc}}(S_{\text{ét}})$ is called an **irreducible/semisimple lisse sheaf** if its corresponding representation(8.4.7.27) is. It is called **geometrically irreducible/semisimple** if $\mathcal{F}_{k^s} \in \mathcal{S}\mathrm{h}_{\overline{\mathbb{Q}}_\ell\text{-lcc}}((S_{k^s})_{\text{ét}})$ is irreducible/semisimple, or equivalently, its corresponding representation is irreducible/semisimple as a $\pi_1(S_{k^s},\overline{x})$-representation. ⌟

Def. (8.4.7.29) [p-adic étale Cohomologies]. For $X \in \mathcal{S}\mathrm{ch}$, $p \in \mathbf{P}$, define

$$\mathrm{H}^i_{\text{ét}}(X,\mathbb{Q}_p) = \Big(\varprojlim_n H^i(X,\mathbb{Z}/(p^n))\Big)[\frac{1}{p}].$$

⌟

Artin-Schreier Sheaves

Def. (8.4.7.30) [Artin-Schreier Sheaves]. The Artin-Schreier cover(8.4.1.44) gives a map $\pi_1(\mathbb{A}^1_{\mathbb{F}_q},\overline{s}) \to \mathbb{F}_q$, when composed with any character $\psi : \mathbb{F}_q \to \overline{\mathbb{Q}_\ell}^\times$, we get a rank1 ℓ-adic étale sheaf $\mathcal{L}(\psi)$ via(8.4.7.19), called an **Artin-Schreier sheaf** on $\mathbb{A}^1_{\mathbb{F}_q}$.

Moreover, if we extend ψ to $\mathbb{F}_{q^n}$ by $\psi_n = \psi \circ \mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$, then the definition of $\mathcal{L}(\psi)$ or even $\mathcal{L}(\psi_x)$ is compatible with base change.(where $\psi_x(y) = \psi(xy)$.) ⌟

Proof: This is because over a base change field $\mathbb{F}_{q^n}$, there is a map of Galois coverings:

$$\wp^{(n)} = \wp \circ \mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{A}^1_{\mathbb{F}_{q^n}} \to \mathbb{A}^1_{\mathbb{F}_{q^n}},$$

so by a minute's thought, their corresponding maps $\pi_1(\mathbb{A}^1_{\mathbb{F}_{q^n}},\overline{s}) \to \overline{\mathbb{Q}_\ell}^\times$ are the same. Thus $\mathcal{L}(\psi_n) \cong \mathcal{L}(\psi)$ over $\mathbb{F}_{q^n}$.

For ψ_x, just notice if $x \in \mathbb{F}_q$, $\psi_x \circ \mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} = (\psi_n)_x$. □

Prop. (8.4.7.31). For $\psi \neq \mathbf{1} \in \chi(\mathbb{F}_q)$ and $x \in \mathbb{F}_q$, denote $\psi_x \in \chi(\mathbb{F}_q) : y \mapsto \psi(xy)$, then

$$\wp_*(\overline{\mathbb{Q}_\ell}) = \bigoplus_{x\in\mathbb{F}_q} \mathcal{L}(\psi_x).$$

⌟

Proof: Cf.[K-W01]P39. □

Prop. (8.4.7.32)[Frobenius Action on Artin-Schreier Sheaves]. Situation as in(8.4.7.30), for any $x \in \mathbb{A}^1(\mathbb{F}_{q^n})$, $\mathrm{Frob}_{\overline{x}}^{-1}$ acts on the stalk $\mathcal{L}(\psi^{-1})_{\overline{x}}$ via multiplication by $\psi(\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^n}}(x))$. ⌟

Proof: By(8.4.7.30), we may base change to $\mathbb{F}_{q^n}$. Let $\alpha \in \mathbb{A}^1(\overline{\mathbb{F}_q})$ s.t. $\alpha^{q^n} - \alpha = x$, then the arithmetic Frobenius at x maps α to $\alpha^{q^n} = \alpha + x$. So by the definition of fundamental group(8.3.2.5), (17.2.1.4) and the definition of the Artin-Schreier sheaf(8.4.7.30), $\mathrm{Frob}_{\overline{x}}^{-1}$ acts via multiplication by $\psi(\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^n}}(x))$. □

Analytification

Comparison Theorems

Thm. (8.4.7.33) [Topological Comparison, Artin]. Let $f : X \to S \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}}/\mathbb{C}$ be separable of f.t., then

- If $\mathcal{F} \in \mathcal{S}\mathrm{ch}_{\mathrm{tor}}(S_{\text{ét}})$, then the comparison morphism for $R^\bullet f_!$ is an isomorphism.
- If $\mathcal{C} \in \mathcal{S}\mathrm{ch}_{\mathrm{const}}(S_{\text{ét}})$, then the comparison morphism for $R^\bullet f_*$ is an isomorphism.

⌟

Proof: [Conrad, Etale Coh]**?** □

Cor. (8.4.7.34) [Comparison with Betti Cohomology]. For $X \in \mathcal{S}\mathrm{ch}^{\mathrm{ft,sep}}/\mathbb{C}$, $A \in \mathcal{A}\mathrm{b}^{\mathrm{fin}}$, there is a canonical isomorphism

$$\mathrm{H}^q_{\text{ét}}(X, \underline{A}_X) \cong H^q_{\mathrm{Betti}}(X; A).$$

⌟

Cor. (8.4.7.35). Let $F \in \mathtt{NField}, p \in \mathbf{P}$ and $v \in \Sigma_F^p$. For $\mathcal{X} \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}/\mathcal{O}_{F_v}$, let $X = \mathcal{X}_{\kappa(v)}$ and $\overline{X} = X_{\overline{\kappa(v)}}$, then for $\ell \neq p$, then

$$\mathrm{H}^i_{\text{ét}}(\overline{X}; \mathbb{Q}_\ell) \cong H^i(\mathcal{X}_{\overline{\eta}}; \mathbb{Q}_\ell) \cong H^i_{\mathrm{Betti}}(\mathcal{X}_{\mathbb{C}})_{\mathbb{Q}_\ell}.$$

⌟

Proof: Let $\mathrm{Spec}\,\mathcal{O}_{F_v} = \{s, \eta\}$, where s is the special point and η the generic point. Let $\overline{\eta}, \overline{s}$ be arithmetic points mapping to η, s resp. By proper base change(8.4.3.1), The stalk of higher direct image of $X \to \mathcal{O}_{F_v}$ along $\overline{s}, \overline{\eta}$ are $\mathrm{H}^i_{\text{ét}}(\overline{X}, \mathbb{Q}_\ell)$ and $H^i(\mathcal{X}_{\overline{\eta}}, \mathbb{Q}_\ell)$ resp., and they are the same by(8.4.6.4). And $H^i(\mathcal{X}_{\overline{\eta}}, \mathbb{Q}_\ell) \cong H^i_{\mathrm{Betti}}(X, \mathbb{Q}_\ell)$ by(8.4.7.34) and the fact $\overline{\mathbb{Q}}_\ell$ is isomorphic to $\mathbb{C}$. □

Cor. (8.4.7.36) [Good Reduction implies Unramifiedness]. If $K \in p\text{-}\mathtt{LField}$ and X is a scheme over K with good reduction, then $\mathrm{H}^i_{\text{ét}}(X, G)$ is an unramified representation of Gal_K. ⌟

Prop. (8.4.7.37) [Étale and Fppf Comparison]. Let $X \in \mathcal{S}\mathrm{ch}$ and G a smooth commutative group scheme over X, then there are natural isomorphisms

$$\mathrm{H}^*_{\text{ét}}(X; G) \cong H^*_{\mathrm{fppf}}(X; G).$$

⌟

Proof: Cf.[Mil80Etale Cohomologies, Prop. III.3]. □

$\mathbf{A}^f$-Cohomologies

Def. (8.4.7.38) [$\mathbf{A}^f$-Cohomologies]. For $X \in \mathcal{S}\mathrm{ch}$, define

$$\mathrm{H}^n_{\text{ét}}(X; \mathbf{A}^f) = (\varprojlim_m \mathrm{H}^n_{\text{ét}}(X, \mathbb{Z}/(m))) \otimes \mathbb{Q}.$$

Then if X is a smooth complete variety over $\mathbb{C}$, then by(8.4.7.34), there is a canonical isomorphism

$$H^n_{\text{Betti}}(X) \otimes \mathbf{A}^f \cong H^n_{\mathbf{A}^f}(X).$$

Thus $H^n_{\text{Betti}}(X) \otimes \mathbf{A}^f$ is intrinsic in X and $H^n_{\mathbf{A}^f}(X)$ free over $\mathbf{A}^f$. ⌟

Conjectures

Conj. (8.4.7.39) [Grothenfieck-Serre]. For $F \in \texttt{NField}$ and $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}/F$, the representation $\mathrm{H}^i_{\text{ét}}(X, \mathbb{Q}_p)$ of Gal_F is semistable. ⌟

Conj. (8.4.7.40) [Semisimplicity of Frobenius]. For X ⌟

Curves

Prop. (8.4.7.41). If $k \in \texttt{Field}, k = k^s, X \in \mathcal{S}\mathrm{ch}^{\text{sep,ft,dim=1}}/k$, and $\mathcal{F} \in \mathcal{S}\mathrm{h}^{\text{tor}}(X_{\text{ét}})$, then $\mathrm{H}^i_{\text{ét}}(X, \mathcal{F}) = 0$ for $i > 2$, and if $\mathcal{F}$ is constructible, then $\mathrm{H}^i_{\text{ét}}(X, \mathcal{F})$ are finite.

Moreover if X is affine and $\mathcal{F}$ is locally killed by n not divisible by $\mathrm{char} k$ or X is proper and sections of $\mathcal{F}$ are locally p-torsions with $p = \mathrm{char}\, k > 0$, then $H^2_{\text{ét}}(X, \mathcal{F}) = 0$. ⌟

Proof: Cf.[Conrad L4 P4] and [Tamme]. □

Lemma (8.4.7.42) [Smooth Complete Curves]. If $k \in \texttt{Field}, k = k^s$, X/k is a non-singular complete curve of genus g and $n \in \mathbb{Z} \cap k^*$, then there are canonical identifications

$$\mathrm{H}^q_{\text{ét}}(X, \mu_n) = \begin{cases} \mu_n(k) & , q = 0 \\ \mathrm{Pic}^0(X)[n] & , q = 1 \\ \mathbb{Z}/n\mathbb{Z} & , q = 2 \\ 0 & , q \geq 3 \end{cases}, \quad \#\mathrm{H}^q_{\text{ét}}(X, \mu_n) = \begin{cases} n & , q = 0 \\ n^{2g} & , q = 1 \\ n & , q = 2 \\ 0 & , q \geq 3 \end{cases}$$

In particular, because $\underline{\mathbb{Z}/(n)} \cong \mu_n$, we can get the corresponding cohomologies. ⌟

Proof: Cf.[Sta]03RQ. □

Prop. (8.4.7.43) [Torsion-Freeness]. Let $k \in \texttt{Field}$, $L \in \ell\text{-}\texttt{NField}$, X a non-singular curve over k, then $H^i_{\text{ét},c}(X, \mathcal{O}_L)$ are torsion-free. ⌟

Proof: Cf. [SGA4$\frac{1}{2}$, Chap3.3].**?** □

Prop. (8.4.7.44) [Curve and Jacobians]. For a smooth complete curve C, its first ℓ-adic étale cohomology group equals that of its Jacobian variety. ⌟

Proof: □

Prop. (8.4.7.45) [Non-Complete Curves]. If $k \in \texttt{Field}, k = k^s, \ell \in \mathbf{P} \backslash \mathrm{char}\, k$, then

$$H^i_{\text{ét},c}(\mathbb{A}^1_k, \mathbb{Q}_\ell) = \begin{cases} \mathbb{Q}_\ell & , i = 2 \\ 0 & , \text{otherwise} \end{cases}, \quad H^i_{\text{ét},c}(\mathbb{A}^1_k \backslash \{0\}, \mathbb{Q}_\ell) = \begin{cases} \mathbb{Q}_\ell & , i = 1, 2 \\ 0 & , \text{otherwise} \end{cases}$$

⌟

Proof: These follow from(8.4.7.42) by excision and(8.4.2.12). □

Weil Axioms

Prop. (8.4.7.46) [Compact ℓ-adic Étale Cohomologies]. Let $k \in \mathtt{Field}, k = k^s, X \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,ft,dim}=d}/k$, $\Lambda \in \mathcal{A}\mathrm{b}^{\mathrm{tor}}$ with torsion orders prime to $\mathrm{char}\, k$, then

1. $H^i_{\text{ét},c}(X, \underline{\Lambda})$ are finite Λ-modules.
2. $H^i_{\text{ét},c}(X, \underline{\Lambda}) = 0$ if $i < 0$ or $i > 2d$. And if X is affine, then $H^i_{\text{ét},c}(X, \underline{\Lambda}) = 0$ if $i < 0$ or $i > d$.
3. There is a natural isomorphism $H^{2d}_{\text{ét},c}(X, \underline{\Lambda}) \cong \Lambda[S]$, where S is the set of irreducible components of X of dimension d.
4. there is a long exact sequence
$$\cdots \to H^p_{\text{ét},c}(U, \underline{\Lambda}) \to H^p_{\text{ét},c}(X, \underline{\Lambda}) \to H^p_{\text{ét},c}(Z, \underline{\Lambda}) \to H^{p+1}_{\text{ét},c}(U, \underline{\Lambda}) \to \cdots$$
5. $H^i_{\text{ét},c}(\mathbb{A}^d_k, \underline{\Lambda}) = \begin{cases} \Lambda & i = 2d \\ 0 & \text{otherwise} \end{cases}.$
6. If G is a connected algebraic scheme over k acting regularly on X, then $G(k)$ acts trivially on $H^i_{\text{ét},c}(X, \underline{\Lambda})$.

⌟

Proof: 1 follows from(8.4.6.1). 4 follows from excision(8.4.5.5).
2 follows from(8.4.2.11) and(8.4.2.12).
3: By item2 and item4, it suffices to show for X irreducible.**?**
5: This follows from Künneth formula(8.4.7.49) and(8.4.7.45).
6: Cf.[Deligne-Lustig]Prop6.4**?**. □

Def. (8.4.7.47) [Cup Product]. ⌟

Cor. (8.4.7.48) [Homotopy Axiom]. Two maps $\varphi, \varphi' : X \to Y \in \mathcal{S}\mathrm{ch}$ induce the same map on the ℓ-adic cohomology if their graphs are rationally equivalent. ⌟

Proof: This is because the maps on cohomology depends only on the rational equivalence classes of the graph.**?** □

Prop. (8.4.7.49) [Künneth Formula]. Let X, Y be complete varieties over k, then there is a natural isomorphism
$$\mathrm{H}^*_{\text{ét}}(X, \mathbb{Q}_\ell) \otimes \mathrm{H}^*_{\text{ét}}(Y, \mathbb{Q}_\ell) \cong \mathrm{H}^*_{\text{ét}}(X \times Y, \mathbb{Q}_\ell).$$
⌟

Proof: **?** □

Lemma (8.4.7.50) [Torsion Poincaré Duality]. ⌟

Prop. (8.4.7.51) [Poincaré Duality]. If $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k, d = \dim X$, $\mathcal{F}$ is a lisse sheaf on X, then there is a natural isomorphism $H^{2d}_{\text{ét},c}(X_{k^s}, \mathbb{Q}_\ell(d)) \xrightarrow{\mathrm{tr}_X} \mathbb{Q}_\ell$ and a perfect pairing
$$\mathrm{H}^n_{\text{ét}}(X_{k^s}, \mathcal{F}) \times H^{2d-n}_{\text{ét},c}(X_{k^s}, \mathcal{F}^\vee(d)) \xrightarrow{\cup} H^{2d}_{\text{ét},c}(X_{k^s}, \mathbb{Q}_\ell(d)) \xrightarrow{\mathrm{tr}_X} \mathbb{Q}_\ell$$
compatible with action of Gal_k. ⌟

Proof: Cf.[Conrad L12-13], [Weil 2Bhatt P5].**?**. □

Def. (8.4.7.52) [Cycle Maps]. For $X \in \mathcal{S}m\mathcal{P}rpr/k$, there exists a **cycle map**

$$\mathrm{cyl}_\ell : \mathrm{CH}^j(X) \to \mathrm{H}^{2j}_{\text{ét}}(X_{k^s}, \mathbb{Q}_\ell)(j)$$

s.t.

$$x \cdot y = \mathrm{tr}_X(\mathrm{cyl}_\ell(x) \cup \mathrm{cyl}_\ell(y)).$$

⌟

Proof:

□

Trace Formulae

Def. (8.4.7.53) [Lefschetz Numbers]. Let $k \in \texttt{Field}, k = k^{\text{sep}}$, $X \in \mathcal{S}\mathrm{ch}^{\text{sep,ft}}/k$, $\mathcal{F}$ a constructible $\mathbb{Q}_\ell$-sheaf on X, then for any $g \in \mathrm{Aut}(X)$, define the **alternating cohomology group**

$$H_{\text{ét},c}(X, \mathcal{F}) = \sum_{i \geq 0} (-1)^i H^i_{\text{ét},c}(X, \mathcal{F}).$$

and the **Lefschetz number** to be

$$\mathrm{tr}(g, X, \mathcal{F}) = \mathrm{tr}(g | H_{\text{ét},c}(X, \mathcal{F})) = \sum_{i \geq 0} (-1)^i \,\mathrm{tr}(g | H^i_{\text{ét},c}(X, \mathcal{F})).$$

⌟

Prop. (8.4.7.54). Let $k \in \texttt{Field}, k = k^s$, $X, C' \in \mathcal{S}\mathrm{ch}^{\text{sep,ft}}/k, g, h \in \mathrm{Aut}(X), g' \in \mathrm{Aut}(X')$, then

1. $\mathrm{tr}(g, X, \cdot)$ is additive.
2. If $Z \subset X$ is a closed subscheme and $U = X \backslash Z$, then $\mathrm{tr}(g, X, \mathcal{F}) = \mathrm{tr}(g, U, \mathcal{F}) + \mathrm{tr}(g, Z, \mathcal{F})$.
3. $\mathrm{tr}(g \times g, X \times X', \mathcal{F} \times \mathcal{F}') = \mathrm{tr}(g, X, \mathcal{F})\,\mathrm{tr}(g', X', \mathcal{F}')$.
4. If g, h commute, then $\mathrm{tr}(gh, X, \mathcal{F}) = \mathrm{tr}(g, X^h, \mathcal{F})$.
5. If T is a tori acting on X, then $\mathrm{tr}(g, X, \mathcal{F}) = \mathrm{tr}(g, X^S, \mathcal{F})$.

⌟

Proof: $1, 2, 3$ follow from(8.4.7.46).
$4, 5$: [Deligne-Lustig, Thm3.2] and [Digne and Michel, Prop10.15].**?** □

Prop. (8.4.7.55). Cf.[Representations of Finite Groups of Lie type, Digne and Michel]. ⌟

Cor. (8.4.7.56). The Lefschetz number is independent of ℓ. ⌟

8.5 Pro-Étale Cohomology

Main references are [B-S14] and [Sta]Chap56.

1 Introduction

In his second paper on the Weil conjectures ([Del80]), Deligne introduced a derived category of l-adic sheaves as a certain 2-limit of categories of complexes of sheaves of $\mathbb{Z}/l^n\mathbb{Z}$-modules on the étalesite of a scheme X. This approach is used in the paper by Beilinson, Bernstein, and Deligne ([BBD82]) as the basis for their beautiful theory of perverse sheaves. In a paper entitled "Continuous ÉtaleCohomology"([Jan88]) Uwe Jannsen discusses an important variant of the cohomology of a l-adic sheaf on a variety over a field. His paper is followed up by a paper of Torsten Ekedahl ([Eke90]) who discusses the adic formalism needed to work comfortably with derived categories defined as limits.

2 Ring-Theoretical Stuff

Def. (8.5.2.1) [étaleLocal Isomorphism]. A ring map $A \to B$ is called a **local isomorphism** if for every prime $\mathfrak{q} \in \operatorname{Spec} B$, there is a nbhd $\operatorname{Spec} B_g$ that $\operatorname{Spec} B_g \to \operatorname{Spec} A$ is an open immersion. ⌟

Prop. (8.5.2.2). The class of local isomorphisms is stable under base change and compositions. (This follows from(6.4.4.60)).

Moreover, if $A \to B \to C$ are ring maps that $A \to B, A \to C$ are both local isomorphisms, then $B \to C$ is also a local isomorphism. ⌟

Def. (8.5.2.3) [w-Local Rings]. A ring A is called **w-local** if $\operatorname{Spec} A$ is w-local(4.12.4.17). it is called **strictly w-local** if it is w-local and every f.f. étale map $A \to B$ has a section. A map of rings is called **w-local** if it induces a w-local map(4.12.4.17) on the Spec. ⌟

Prop. (8.5.2.4). A w-local ring A is strictly w-local iff all local rings of A at closed pts are strictly Henselian. ⌟

Proof: Cf.[Pro-Etale Cohomology, Scholze, P10]. □

Ind-Zariski Algebra

Def. (8.5.2.5) [Ind-Zariski Algebra]. A ring map $A \to B$ is called **ind-Zariski/smooth/étale** if B is a filtered colimit of local isomorphisms/smooth ring maps/étale ring maps $A \to B_i$. ⌟

Prop. (8.5.2.6) [Properties of Ind-Zariski Algebras]. Ind-Zariski ring maps are stable under base change and composition, by(8.5.2.2).**?**

If $A \to B \to C$ are ring maps that $A \to B, A \to C$ are both ind-Zariski, then $B \to C$ is also ind-Zariski.

$A \to B$ be ind-Zariski, then it identifies local rings. ⌟

Proof: □

Def. (8.5.2.7) [Ind-(Zariski Localization)]. A ring map $A \to B$ is called a **Zariski localization** if $B = \prod_i^n A_{f_i}$. An **ind-(Zariski localization)** of A is a colimit of Zariski localizations of A. ⌟

Ind-Smooth Algebra

Ind-Étale Algebra

8.6 Perverse Sheaves

References are [Perverse Sheaves, Beilinson-Bernsterin-Deligne], [D-modules, perverse sheaves, and representation theory], [K-W01].

Notation (8.6.0.1).

- Let $k \in \texttt{Field}$ s.t. $\#k < \infty$ or $k = \overline{k}$.
- Let $\ell \in \mathbf{P} \setminus \{\operatorname{char} k\}$.

$\lrcorner$

8.7 Profinite Cohomology

Reference are [Neu15] and the giant book [Neukirch Cohomology of Number Fields].

1 Group Cohomology

Let G be a finite group.

Def. (8.7.1.1) [Group Cohomologies]. For $G \in \mathcal{G}\mathrm{rp}^{\mathrm{fin}}$, the **group cohomology** $H^n(G, A)$ is the derived functor of the left exact functor

$$\mathcal{M}\mathrm{od}_G \to \mathcal{A}\mathrm{b} : H^0(G, A) = A^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A),$$

so $H^n(G, A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$.

The **group homology** $H_n(G, A)$ is the left derived functor of the right exact functor

$$\mathcal{M}\mathrm{od}_G \to \mathcal{A}\mathrm{b} : H_0(G, A) = A_G = \mathbb{Z} \otimes_{\mathbb{Z}[G]} A,$$

so $H_n(G, A) = \mathrm{Tor}_n^{\mathbb{Z}[G]}(\mathbb{Z}, A)$。 ⌟

Prop. (8.7.1.2). For a normal subgroup H of G, $A \mapsto A^H$ is left exact from G-mod to G/H-mod and preserves injectives **??** because it is right adjoint to the exact inclusion functor as $\mathrm{Hom}_G(B, A) = \mathrm{Hom}_{G/H}(B, A^H)$. Dually for A_H. ⌟

Prop. (8.7.1.3). For $G = \mathbb{Z}$, we have a free resolution $0 \to Z[t, t^{-1}] \xrightarrow{1-t} Z[t, t^{-1}] \to Z \to 0$. In particular, thus $H_n(\mathbb{Z}, \mathbb{Z}) = \mathbb{Z}$ iff $n = 0, 1$ and vanish otherwise. ⌟

Prop. (8.7.1.4) [Tate Cohomology]. There is a standard resolution of the $\mathbb{Z}[G]$-module $\mathbb{Z}$:

$$\cdots \longleftarrow X_{-2} \longleftarrow X_{-1} \xleftarrow{\mu\circ\varepsilon} X_0 \longleftarrow X_1 \longleftarrow \cdots$$

that $X_q = X_{-q-1}$ are $\mathbb{Z}[G]$-module generated by q-cells $(\sigma_1, \ldots, \sigma_q)$, $X_0 = X_{-1} = \mathbb{Z}[G]$.

It then can be verified that for $G \in \mathcal{A}\mathrm{b}^{\mathrm{fin}}$, Hom from this resolution gives out the Tate cohomology

$$H^n_T(G, A) = \begin{cases} H^n(G, A) & n \geq 1 \\ A^G / \mathrm{tr}_G A & n = 0 \\ {}_{\mathrm{tr}_G}A / I_G A & n = -1 \\ H_{-1-n}(G, A) & n \leq -2 \end{cases}$$

and H^n_T is a long exact sequence.

In particular, the Hom complex looks like:

$$\cdots \to A_{-2} \xrightarrow{\partial_{-1}} A_{-1} \xrightarrow{\partial_0} A_0 \xrightarrow{\partial_1} A_1 \xrightarrow{\partial_2} A_2 \to \cdots$$

where $A_{-1} = A_0 = A$ and $\partial_0 x = \mathrm{tr}_G x$, $(\partial_1 x)(\sigma) = \sigma x - x$,

$\partial_2(x)(\sigma_1, \sigma_2) = \sigma_1 x(\sigma_2) - x(\sigma_1\sigma_2) + x(\sigma_1)$. ⌟

Proof: Cf.[Neukirch CFT P13]**?** □

Remark (8.7.1.5). From now on, consider only Tate cohomology. ⌟

Prop. (8.7.1.6).

$$H^{-2}(G,\mathbb{Z})=G^{ab},\quad H^{-1}(G,\mathbb{Z})=0,\quad H^0(G,\mathbb{Z})=\mathbb{Z}/|G|\mathbb{Z},\quad H^1(G,\mathbb{Z})=0,\quad H^2(G,\mathbb{Z})=\chi(G).$$

⌟

Proof: H^0 is trivial and $H^1(G,\mathbb{Z})=H^0(G,\mathbb{Q}/\mathbb{Z})=0$, $H^2(G,\mathbb{Z})=H^1(G,\mathbb{Q}/\mathbb{Z})=\mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$. $H^{-1}(G,\mathbb{Z})={}_{N_G}\mathbb{Z}/I_GA=0$.

For $H^{-2}(G,\mathbb{Z})$, use the dimension shifting $0\to I_G\to\mathbb{Z}[G]\to\mathbb{Z}\to 0$, $=H^{-1}(G,I_G)=I_G/I_G^2$. And $G^{ab}\cong I_G/I_G^2$ by $\sigma\mapsto\sigma-1$. □

Prop. (8.7.1.7) [Group Cohomologies are Torsion]. For $G\in\mathcal{A}\mathrm{b}^{\mathrm{fin}}$, $\#G\cdot H^n(G,A)=0$ for any $A\in\mathcal{M}\mathrm{od}_G$. (True for H^0 and use dimension shifting). In particular, a divisible G-module A has trivial cohomology. ⌟

Operations

Prop. (8.7.1.8)[Dimension Shifting]. There are fundamental split exact sequence $0\to I_G\to\mathbb{Z}[G]\to\mathbb{Z}\to 0$ and $0\to\mathbb{Z}\to\mathbb{Z}[G]\to J_G\to 0$, thus $A_G=A/I_GA$. This can be used to tensor with A and define natural dimension shifting of cohomology δ. ⌟

Lemma (8.7.1.9). If H is a subgroup of G, then by Grothendieck spectral sequence applied to $\mathcal{M}\mathrm{od}_G\xrightarrow{\mathrm{res}}\mathcal{M}\mathrm{od}_H\xrightarrow{(\cdot)^H}\mathcal{A}\mathrm{b}$ shows that for $A\in\mathcal{M}\mathrm{od}_G$, $H^*(H,A)$ is the same as the right derived functor of the functor $(\cdot)^H$ on $\mathcal{M}\mathrm{od}_G$. ⌟

Def. (8.7.1.10) [Restrictions, Corestrictions and Inflations]. Let H be a subgroup of G,

- The **inflation** is the δ-morphism $H^*(G/H,A)\to H^*(G,A)$ on $\mathcal{M}\mathrm{od}_{G/H}$ induced by the natural transformation**?** How to define it**?**
- The **restriction** are the δ-morphisms $H^*(G,A)\to H^*(H,A)$ on $\mathcal{M}\mathrm{od}_G$ induced by the natural transformation $A^G\to A^H$.
- The **corestriciton** are the δ-morphisms $H^*(H,A)\to H^*(G,A)$ on $\mathcal{M}\mathrm{od}_G$ induced by the natural transformation $A^H\to A^G: a\mapsto N_{G/H}a$.

⌟

Proof: These exist by(4.10.3.5) and(8.7.1.9). □

Cor. (8.7.1.11). Let H be a subgroup of G, then $\mathrm{cor}\circ\mathrm{res}=[G:H]\,\mathrm{id}$. ⌟

Prop. (8.7.1.12) [Kernel of Restriction]. If G is a finite group and H_1,H_2 are conjugate subgroups of G and $M\in\mathcal{M}\mathrm{od}_G$, then the kernel of the restriction maps $H^1(G,M)\to H^1(H_i,M)$ are identical. ⌟

Proof: If a 1-cycle $\sigma\mapsto f(\sigma)$ is a cocycle, then it is a boundary when restricted to H_1 iff $f(\sigma)=\sigma(a)-a$ for some $a\in M$ for any $\sigma\in H_1$. Thus

$$f(x^{-1}\sigma x)=f(x^{-1})+x^{-1}f(\sigma x)=-x^{-1}f(x)+x^{-1}f(\sigma)+x^{-1}\sigma f(x)=x^{-1}(\sigma(f(x)+a)-(f(x)+a))$$

is also boundary when restricted to $x^{-1}H_1x$. □

Prop. (8.7.1.13)[Serre-Hochschild Spectral Sequence]. If H is a normal subgroup of a finite group G, by Grothendieck spectral sequence, the relation $A^G = (A^H)^{G/H}$ gives us a spectral sequence E that

$$E_2^{p,q} = H^p(G/H, H^q(H, A)) \Longrightarrow E^n = H^n(G, A).$$

The edge morphisms are:

- inflation maps $H^k(G/H, A^H) \xrightarrow{\text{inf}} H^k(G, A)$.
- restriction maps $H^k(G, A) \xrightarrow{\text{res}} H^k(H, A)^{G/H}$.

And the lower parts give us:

$$0 \to H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A)^{G/H} \xrightarrow{transgression} H^2(G/H, A^H) \xrightarrow{inf} H^2(G, A).$$

dually for homology group.

Moreover if $H^k(H, A) = 0$ for $k = 1, \ldots, n-1$, then the rows are blank, thus the above lower part can change to dimension n. ⌟

Proof: Prove the compatibility of inflation, restriction with the definition given in(8.7.1.10).**??** □

Cor. (8.7.1.14) [Hopf]. If $G = F/R$, F is free, then use the homology spectral sequence, $H_2(G, \mathbb{Z}) \cong \frac{R\cap[F,F]}{[F,R]}$. Cf.[Weibel P198]. ⌟

Prop. (8.7.1.15). For an isomorphism (σ^*, σ) of a group and its cochain map in the sense that $\sigma^*(g)(\sigma(a)) = g(a)$, we have an isomorphism of Conjugation acts trivially on the group cohomology, because it does on H^0 because $H^0 = A^G$ fixed by G, and it commutes with dimension shifting. (Warning, if you count directly $a(\sigma\tau\sigma^{-1}) - \sigma a(\tau)$, you won't get 0, but a 1-coboundary). ⌟

Prop. (8.7.1.16)[Cup Products]. The cup product is defined by $C^p(X, A) \times C^q(X, B) \to C^{p+q}(X, A\otimes B)$:

$$(a \smile b)(\sigma_1, \ldots, \sigma_{p+q}) = a(\sigma_1, \ldots, \sigma_p) \otimes \sigma_1 \ldots \sigma_p b(\sigma_{p+1}, \ldots, \sigma_{p+q}).$$

It satisfies $\partial(a \smile b) = \partial(a) \smile b + (-1)^p a \smile \partial(b)$, thus defines a:

$$\smile : H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B)$$

for $p, q \geq 0$. And in negative dimension this is also definable but not computable, Cf.[Neukirch Cohomology of Number Fields P42] or [Neukirch Class Field Theory 2015 P45].

- $a \smile b = a \otimes b$ for $a \in H^0(G, A), b \in H^0(G, B)$.
- $\delta(a \smile b) = \delta a \smile b, \delta(a \smile b) = (-1)^p(a \smile \delta b)$ for $a \in H^p(G, A)$.
- $\smile$ is associative and skew-symmetric (follows from dimension shifting and the last one.)

⌟

Proof: □

Prop. (8.7.1.17) [Duality and Cup Product]. Let $0 \to A' \xrightarrow{i} A \xrightarrow{j} A'' \to 0$ and $0 \to B' \xrightarrow{u} B \xrightarrow{v} B'' \to 0$ be exact and there is a pairing $\varphi : A \times B \to C$ that $\varphi(A' \times A') = 0$ hence induce a compatible pairing on $A' \times B''$ and $A'' \times B'$, then we have

$$\delta(\alpha) \smile \beta + (-1)^p \alpha \smile \delta(\beta) = 0$$

for $\alpha \in H^p(G, A'')$ and $\beta \in H^q(G, B'')$. ⌟

Proof: Use the definition of δ, let a, b be the preimage of α, β in A and B, and $ia' = \partial a, ub' = \partial b$, then $\delta(\alpha) \smile \beta + (-1)^p \alpha \smile \delta(\beta) = a' \smile vb + (-1)^p ja \smile b' = \partial a \smile b + (-1)^p a \smile \partial b = \partial(a \smile b)$ is a boundary. □

Prop. (8.7.1.18) [Naturality of Cup Products].

$$\mathrm{res}(a \smile b) = \mathrm{res}(a) \smile \mathrm{res}(b), \quad \inf(a \cup b) = \inf(a) \cup \inf(b), \quad \mathrm{cor}(\mathrm{res}\, a \smile b) = a \smile \mathrm{cor}\, b.$$

⌟

Proof: Cf.[Neukirch CFT P48] or [Central Simple Algebras]P100.**?** □

Prop. (8.7.1.19). Let $\sigma \in G^{ab} = H^{-2}(G, \mathbb{Z})$ and $a_1 \in H^1(G, A), a_2 \in H^2(G, A)$, then

$$a_1 \smile \sigma = a_1(\sigma), \quad a_2(\sigma) = \sum_{\tau} a_2(\tau, \sigma).$$

Cf.[Neukirch CFT P50,P51]. ⌟

Prop. (8.7.1.20) [Cyclic Group Cohomologies]. For cyclic group, the Tate cohomology is 2-cyclic.

In particular, if σ be a generator for $\mathbb{Z}/(n)$, then $H^p(\mathbb{Z}/(n), A) = A^G/\mathrm{tr}(A)$ for p even and $H^p(\mathbb{Z}/(n), A) = {}_{\mathrm{tr}}A/(\sigma - 1)A$ for p odd. ⌟

Proof: There is an exact sequence $0 \to \mathbb{Z} \to \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \to \mathbb{Z} \to 0$, and this defines an isomorphism $\delta^2 : H^0(G, \mathbb{Z}) \cong H^2(G, \mathbb{Z})$. And this is also true for any A when tensored with it. The isomorphism is $a \mapsto \delta^2 a = \delta^2(1) \smile a$. □

Prop. (8.7.1.21) [Duality]. The cup product induces an isomorphism $H^i(G, A^\vee) \cong (H^{-i-1}(G, A))^\vee$, i.e, $H^n(G, A^\vee)$ and $H_n(G, A)$ are dual to each other when $n > 0$, where $A^\vee = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$. ⌟

Proof: We only need to verify $A^{*G}/N_G A^* \cong ({}_{N_G}A/I_G A)^*$ and use dimension shifting. Should use the injectivity of $\mathbb{Q}/\mathbb{Z}$ and the compatibility of cup product with dual. □

Cor. (8.7.1.22). When A is $\mathbb{Z}$-free, the cup product also induce an isomorphism $H^i(G, \mathrm{Hom}(A, \mathbb{Z})) \cong H^{-i}(G, A)^\vee$. ⌟

Prop. (8.7.1.23) [Theorem of Cohomological Triviality]. For a G-module A, if there is a q s.t. $H^q(g, A) = H^{q+1}(g, A) = 0$ for all subgroups of G, then $H^p(g, A) = 0$ for any p and subgroup g. Cf.[Neukirch CFT P57]. ⌟

Prop. (8.7.1.24) [Tate's Theorem]. Assume A is a G-module that $H^1(G, A) = 0$ and $H^2(g, A)$ is cyclic of order $|g|$ for any subgroup g of G, then for a generator a of $H^2(G, A)$, there is an isomorphism

$$a \smile : H^q(G, \mathbb{Z}) \cong H^{q+2}(G, A).$$

Cf.[Neikirch CFT P79]. ⌟

Cor. (8.7.1.25). In particular, by dimension shifting, if A is a G-module that $H^1(G, A) = 0$ and $H^2(g, A)$ is cyclic of order $|g|$ for any subgroup g of G this gives an isomorphism:

$$a \smile : H^q(G, \mathbb{Z}) \cong H^{q+2}(G, A).$$

for a generator a of $H^2(G, A)$, because cup product commutes with dimension shifting. ⌟

Miscellaneous

Prop. (8.7.1.26) [H^2 and Extensions, Schreier]. For a G-module A, there is a correspondence of equivalence classes of extension of G over A that are compatible with the G action and $H^2(G,A)$. ⌟

Proof: Cf.[Weibel P183]. In fact there are also interpretations of $H^3(G,A)$ as $0\to A\to N\to E\to G$ under some equivalences. □

Prop. (8.7.1.27) [Herbrand Quotients for Cyclic Groups]. When G is a cyclic group and A is a G-module, let $f=\sigma-1$, $g=1+\sigma+\ldots+\sigma^{n-1}$, then we can form a cyclic complex of order 2 and compute the Herbrand quotient(4.8.7.7). In this case, $g_{f,g}$ is just $|H^0(G,A)|/|H^{-1}(G,A)|$. And by(4.8.7.9), if a G-morphism $A\to B$ has finite kernel and cokernel, then they have the same Herbrand quotient. ⌟

2 Cohomology of Profinite Groups

Prop. (8.7.2.1) [Abelian Sheaves on T_G]. For $G\in\mathcal{P}\mathrm{rof}$, the category of Abelian sheaves on the canonical topology(6.1.2.4) T_G of G-sets is equivalent to the the category $\mathcal{M}\mathrm{od}_G^{\mathrm{alg}}$, by $Z\mapsto\mathrm{Hom}(-,Z)$. The inverse map is given by $F\mapsto\varinjlim F(G/H)$. ⌟

Proof: The task is to prove $F\cong h_{\varinjlim F(G/H)}$. Cf.[Tamme P29].

The inverse of the Yoneda functor is the functor $F\mapsto F(G)$ as a left G-set where $gs=F(\cdot g)s$. The task is to show that $F\cong h_{F(G)}$. For this, for any U we consider the covering $\{G\xrightarrow{\varphi_u}U$ where $\varphi_U(g)=gu$. Sheaf condition says

$$F(U)\to\prod_{u\in U}F(G)\rightrightarrows F(G\times_U G)$$

is exact, in other words, $F(U)\cong\mathrm{Hom}_G(U,F(G))$. □

Prop. (8.7.2.2) [Profinite Cohomologies]. The **profinite cohomology** is the derived functor of $A\to A^G$ on the Abelian category $\mathcal{M}\mathrm{od}_G^{\mathrm{alg}}$(8.7.2.1)(It has enough injectives by(18.1.2.1)). It satisfies

$$H^*(G,A)\cong H^*(C^\bullet(G,A))\cong\varinjlim H^*(G/U,A^U)$$

where $C^\bullet(G,A)$ is the set of continuous cochain complex of morphisms from G to A and the colimit is taken over the transition maps defined by inflations. Moreover, for the same reason, when $G=\varprojlim G_i$, and $A=\varinjlim A_i$, then

$$H^*(G,A)\cong\varinjlim H^*(G_i,A_i).$$

⌟

Proof: The second is an isomorphism because $C^n(G,A)=\varinjlim C^n(G/U,A^U)$ and direct limit is exact.

For the first, the H^0 obviously coincide, so it suffice to prove $H^*(C(G,A))$ form a universal δ-functor. It is effaceable because $(-)^U$ preserves injective modules(8.7.1.2).

For the last one, we need to check $C^n(G,A)=\varinjlim C^n(G_i,A_i)$. Notice G has the profinite topology, thus must factor through some G_i, and the right through some A_i because the image of a morphism from G^n to A has finite image. Thus the result follows. □

Prop. (8.7.2.3) [Cohomology Groups are Torsion]. For $G\in\mathcal{P}\mathrm{rof}$, $M\in\mathcal{M}\mathrm{od}_G^{\mathrm{alg}}$, $i\in\mathbb{N}$, $H^i(G,M)$ are torsion Abelian groups. And if G is a pro-p-group, then $H^i(G,M)$ are p-primary torsion subgroups. ⌟

Proof: Notice if $M \in \mathcal{M}od_G^{alg}$, this follows from(8.7.2.2) and(8.7.1.7). The last assertion is similar. □

Def. (8.7.2.4) [Restrictions, Corestrictions and Inflations]. Let $G \in \mathcal{P}rof$ and $H < G$ be a closed subgroup, for any $A \in \mathcal{M}od_G^{alg}$, taking colimits over all open subgroup U_α of G of the restriction maps

$$\mathrm{res} : H^i(G/U_\alpha, A^{U_\alpha}) \to H^i(H/(H \cap U_\alpha), A^{U_\alpha}) \to H^i(H/H \cap U_\alpha, A^{H \cap U_\alpha}),$$

by(3.1.13.6), we get a restriction map

$$\mathrm{res} : H^i(G, A) \to H^i(H, A).$$

Similarly, if H is open in G, we can define a corestriction map

$$H^i(H, A) \to H^i(G, A).$$

And if $H \lhd G$ is normal, we can define an inflation map

$$H^i(G/H, A^H) \to H^i(G, A).$$

as the colimit of the inflation maps

$$H^i(G/HU_\alpha, A^{HU_\alpha}) \to H^i(G/H, A^{U_\alpha}).$$

⌟

Prop. (8.7.2.5). $\mathrm{cor} \circ \mathrm{res} = [G : H]$ for a subgroup H is also true for profinite cohomology(8.7.1.11), if H is an open subgroup of G. This is because of(8.7.2.2). ⌟

Prop. (8.7.2.6). If H is a closed subgroup of a profinite group G, $p \in \mathbf{P}$ s.t. $p \nmid [G : H]$, then for any $A \in \mathcal{M}od_G^{alg}, i \in \mathbb{N}$, $\mathrm{res} : H^i(G, A) \to H^i(H, A)$ is injective on the p-primary part of $H^i(G, A)$. ⌟

Proof: This follows from(8.7.2.5) and(8.7.2.4) by taking filtered colimits. □

Lemma (8.7.2.7) [Shapiro].

$$H_*(G, \mathrm{Ind}_H^G(A)) \cong H_*(H, A), \quad H^*(G, \mathrm{ind}_H^G(A)) \cong H^*(H, A)$$

because (co)induction is adjoint to exact functors, so it preserves injectives(projectives) and it is exact because $\mathbb{Z}[G]$ is free $\mathbb{Z}[H]$-module.

And in the finite case, this is also true for Tate cohomology using dimension shifting. ⌟

Prop. (8.7.2.8) [Serre-Hochschild Spectral sequence]. The same spectral sequence as in the finite case(8.7.1.13) also applies to profinite cohomology with H closed normal in G. ⌟

Def. (8.7.2.9) [Cup Products]. For any $U < G$ open and $A, B \in \mathcal{M}od_G^{alg}$, there are natural cup product maps

$$H^*(G/U, A^U) \times H^*(G/U, B^U) \to H^*(G/U, A^U \otimes B^U) \to H^*(G/U, (A \otimes B)^U).$$

Then by the naturality of inflation and the fact inflation commutes with cup product(8.7.1.18), we get a natural cup product map

$$H^*(G, A) \times H^*(G, B) \to H^*(G, A \otimes B).$$

⌟

Prop. (8.7.2.10). The cup products for profinite groups(8.7.2.9) is associative, graded-commutative, and commutes with inflations, restrictions and corestrictions as in(8.7.1.18). ⌟

Proof: □

Cohomological Dimensions

Def. (8.7.2.11) [Cohomological Dimensions]. The ***p*-cohomological dimension** $cd_p(G)$ of a profinite group G is defined as the smallest integer n that $H^i(G,A)[p^\infty]=0$ for any torsion G-module A. The **strict *p*-cohomological dimension** $scd_p(G)$ of a profinite group G is defined as the smallest integer n that the $H^i(G,A)[p^\infty]=0$ for any G-module A.

The **cohomological dimension** $cd(G)$ is defined to be $cd(G)=\sup_p(cd_p(G))$. The **strict cohomological dimension** $scd(G)$ is defined to be $\sup_p(scd_p(G))$. ⌟

Prop. (8.7.2.12). For $G\in\mathcal{P}\mathrm{rof}$, the following are equivalent:

- $cd_p(G)\le n$.
- $H^i(G,A)=0$ for any $i>n$ and any p-torsion G-module A.
- $H^{n+1}(G,A)=0$ for any simple p-torsion G-module A.

And if G is pro-p, then it suffice to check $H^{n+1}(G,\mathbb{Z}/p\mathbb{Z})=0$ ⌟

Proof: For any torsion G-module A, $A=\oplus_p A(p)$, so $H^i(G,A(p))$ is the p-primary part of $H^i(G,A)$, so $1\iff 2$. For $3\to 1$: use the fact cohomology commutes with colimits(8.7.2.2), reduce to the case of A finite, and then use use the quotient tower.

The last assertion is by(3.1.13.15). □

Prop. (8.7.2.13). For any $G\in\mathcal{P}\mathrm{rof}$, $cd_p(G)\le scd_p(G)\le cd_p(G)+1$. ⌟

Proof: Let $A_p=\ker(p:A\to A)$. There are exact sequences $0\to A_p\to A\xrightarrow{p} pA\to 0$ and $0\to pA\to A\to A/pA\to 0$. A_p and A/pA are p-torsion G-modules, so if $i>cd_p(G)+1$, then $H^i(G,A_p)$ and $H^{i-1}(G,A/pA)$ vanish. so $H^i(G,A)\xrightarrow{p} H^i(G<pA)$ and $H^i(G,pA)\to H^i(G,A)$ are injections, so their composition $H^i(G,A)\xrightarrow{p} H^i(G,A)$ is injective, showing $(H^i(G,A))_p=0$, so $scd_p(G)\le cd_p(G)+1$. □

Prop. (8.7.2.14). For a closed subgroup H of a profinite group G, $cd_p(H)\le cd_p(G)$ and $scd_p(H)\le scd_p(G)$, and if $[G:H]$ is relatively prime to p, then equality holds. ⌟

Proof: The first is because of Shapiro's lemma(8.7.2.7). For the equality, use(8.7.2.6). □

Cor. (8.7.2.15). $cd_p(G)=cd_p(G_p)=cd(G_p)$, $scd_p(G)=scd_p(G_p)=scd(G_p)$. ⌟

Prop. (8.7.2.16). If H is a closed normal subgroup of G, then $cd_p(G)\le cd_p(H)+cd_p(G/H)$, by Hochschild-Serre spectral sequence. ⌟

Prop. (8.7.2.17). If K is a field of char p, then $cd_p(\mathrm{Gal}_K)=0$.

If $H^2(G(K_s/L),K_s^*)=0$ for all L/K separable, then $cd(G(K_s/K))\le 1$. In particular $H^i(G(K_s/K),K_s^*)=0$ for $i\ge 1$. ⌟

Proof: Let G_p be the Sylow p-subgroup of $G(K_s/K)$ and $M=K_s^{G_p}$. There is an exact sequence $0\to\mu_p\to K_s\xrightarrow{x^p-x} K_s\to 0$, and combined with the fact that $H^i(G_p,K_s)=H^i(G(K_s/M),K_s)=0$ for $i\ge 1$(8.7.3.1), so $H^i(G_p,\mathbb{Z}/p\mathbb{Z})=0$ for $i\ge 2$. Thus by(8.7.2.12) and(8.7.2.15), $cd_p(G(K_s/K))\le 1$.

For the second assertion, similarly, for $l\ne p$, consider the kernel of x^l, μ_l of l-th roots of unity in K_s, and $H^2(G_l,\mu_l(K_s))=\varinjlim_L H^2(G(K_s/L),\mu_l(K_s))=0$, so $cd_l(G(K_s/K))\le 1$. Then $cd(G(K_s/K))\le 1$, and $scd(G(K_s/K))\le 2$, so $H^i(G(K_s/K),K_s^*)=0$ for $i\ge 1$. □

Prop. (8.7.2.18). For L/K field extension, $cd_p(\mathrm{Gal}_L)\le cd_p(\mathrm{Gal}_K)+\mathrm{tr.deg}(L/K)$. ⌟

Proof: Cf.[Etale Cohomology Fulei P169]. □

Cor. (8.7.2.19). If $k=k^s$ and K be a function field over k, then $cd(\mathrm{Gal}_K)\le 1$.
And if K is of char $p>0$, $H^2(G(K_s/K),K_s^*)$ is a p-torsion group. ⌟

Proof: Th first one is clear, for the second, for any $l\neq p$, use the exact sequence $\mu_l(K_s)\to K_s^*\xrightarrow{x\to x^l}K_s^*\to 0$, then $H^2(G(K_s/K),\mu_l(K_s))=0$, and $H^2(G(K_s/K),K_s^*)\xrightarrow{l}H^2(G(K_s/K),K_s^*)$ is injective. l is arbitrary, so $H^2(G(K_s/K),K_s^*)$ must be a p-torsion group. □

3 Galois Cohomology

References are [Neukirch, Cohomology of Number Fields]Chap6. Should include [Galois Cohomology Serre].

Prop. (8.7.3.1) [Hilbert's Additive Satz 90]. For $K\in\texttt{Field}$, if L/K is a Galois extension, then $H^n(\mathrm{Gal}(L/K),L)=0$ for $n>0$, where L is equipped with the discrete topology. ⌟

Proof: Form the normal basis theorem**??**, for finite Galois extension L/K, L is an induced module over K, thus $H^*(G,L)=H_*(G,L)=0$ for $*\neq 0$ and $H_T^*(G,L)=0$ by(8.7.2.7).

Hence the same is true, for arbitrary Galois extension, when L is equipped with the discrete topology, the same as in the proof of(8.7.3.16). □

Prop. (8.7.3.2)[Hilbert's Multiplicative Satz 90]. $H^1(\mathrm{Gal}(L/K),L^\times)=0$ for any Galois extension L/K, where L is equipped with the discrete topology. ⌟

Proof: This follows from(8.7.3.16). □

Prop. (8.7.3.3)[Generalized Hilbert's Additive Satz 90]. For L/K a Galois extension and $k\in\mathbb{Z}_+$, $H^1(\mathrm{Gal}(L/K),W_{p,k}^+(L))=0$. ⌟

Proof: By linear independence of characters, if L/K is finite, then there is some $x_0\in L$ s.t. $\mathrm{tr}_{L/K}(x_0)\neq 0$. Then by(5.5.3.17), $x=(x_0,0,\dots,0)$ is a unit in $W_{p,k}^+(L)$. Given any cocycle $\mu:\sigma\mapsto\mu_\sigma$, let

$$\theta=\mathrm{tr}_{L/K}(x)^{-1}\sum_{\sigma\in\mathrm{Gal}(L/K)}\mu_\sigma\sigma(x),$$

then for $\tau\in\mathrm{Gal}(L/K)$,

$$\theta-\tau(\theta)=\mathrm{tr}_{L/K}(x)^{-1}\sum_{\sigma\in\mathrm{Gal}(L/K)}[\mu_{\tau\sigma}(\tau\sigma)(x)-\tau(\mu_\sigma)(\tau\sigma)(x)]=\mathrm{tr}_{L/K}(x)^{-1}\mu_\tau\sum_{\sigma\in\mathrm{Gal}(L/K)}(\tau\sigma)(x)=\mu_\tau.$$

Thus μ is a coboundary.

Hence the same is true, for arbitrary Galois extension, when L is equipped with the discrete topology, the same as in the proof of(8.7.3.16). □

Def. (8.7.3.4)[Galois Cohomologies]. For $k\in\texttt{Field}$, for any $M\in\mathcal{M}\mathrm{od}^{\mathrm{alg}}(\mathrm{Gal}_k)$, denote $H^i(k,M)=H^i(\mathrm{Gal}_k,M)$. ⌟

Prop. (8.7.3.5). $\mathrm{Br}(\mathbb{R})=\mathbb{Z}/(2)$. ⌟

Proof: By(8.7.1.20) and(8.7.1.4), $H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}),\mathbb{C}^\times)\cong\{u\in\mathbb{C}^\times|\overline{u}=u\}/\{|u|^2,u\in\mathbb{C}^\times\}\cong\mathbb{Z}/(2)$. □

Prop. (8.7.3.6) [Kummer Cohomology]. For L/K a Galois extension and $\mathrm{char}\,k=p\in\mathbf{P},r\in\mathbb{Z}_+$, then there exists an isomorphism

$$k^\times/(k^\times)^m\xrightarrow{\partial,\cong}H^1(k,\mathbb{Z}/(p^r)).$$

⌟

Proof: This follows from the Kummer exact sequence and Hilbert's theorem90(8.7.3.2). □

Prop. (8.7.3.7) [Restrictions and Corestrictions on H^0]. Let K/k be a separable field extension, then

$$\mathrm{res}_k^K=i:k\to K,\quad \mathrm{cor}_k^K=\mathrm{Nm}_{K/k}:K\to k$$

⌟

Proof: This follows from the definition(8.7.1.10). □

Cor. (8.7.3.8)[Change of Fields and Kummer Cohomology]. Let K/k be a separable field extension and $m\in\mathbb{Z}\cap k^\times$, then there are commutative diagrams

$$\begin{array}{ccc} k^\times & \xrightarrow{\partial} & H^1(k,\mu_m)\\ \downarrow & & \downarrow\mathrm{res}\\ K^\times & \xrightarrow{\partial} & H^1(K,\mu_m)\end{array}\qquad\begin{array}{ccc} K^\times & \xrightarrow{\partial} & H^1(K,\mu_m)\\ \downarrow\mathrm{Nm}_{K/k} & & \downarrow\mathrm{cor}\\ k^\times & \xrightarrow{\partial} & H^1(k,\mu_m)\end{array}$$

⌟

Proof: Cf.[Central Simple Algebras]P131.**?** □

Prop. (8.7.3.9) [Artin-Schreier Cohomology]. Let $k\in\mathtt{Field},m\in\mathbb{Z}\cap k^\times$, then there exists an isomorphism

$$W_{p,r}(k)^+/(\mathrm{Frob}-\mathrm{id})W_{p,r}(k)^+\cong H^1(k,\mu_m).$$

⌟

Proof: This follows from the Artin-Schreier exact sequence(8.7.3.3) and Hilbert's theorem90(8.7.3.3). □

Prop. (8.7.3.10)[Unramified Classes]. Let F be a global field and $G=\mathrm{Gal}_F$, then for a Gal_F-module M, is called a **unramified class** at a place $v\in\Sigma_F$ if it is trivial when restricted to $H^k(I_v,M)$, where I_v is the inertia group at v, which is defined only up to conjugacy, but this notion is well-defined by(8.7.1.12). ⌟

Prop. (8.7.3.11)[Unramified Classes are Rare]. Let C be a proper Dedekind domain or a complete non-singular curve over a field k with fraction field F and $G=\mathrm{Gal}_F$, then for any finite G_F-module M, if S is a finite set of places in F and $H^1(\mathrm{Gal}_F,M,S)$ the set of elements of $H^1(\mathrm{Gal}_F,M,S)$ that is unramified outside S, then $\#H^1(G_F,M,S)<\infty$. ⌟

Proof: By the inflation restriction exact sequence(8.7.1.13), we can reduce G to a subgroup of finite index. And because M is a finite G-module, there is a finite index subgroup of G that acts trivially on M. Thus we can assume M is G-trivial. But then if $m>0$ s.t. $mM=0$, then the assertion follows from the fact the maximal Abelian extension of exponent m unramified outside S is finite over K(14.6.4.4). □

Non-Abelian Cohomology

Def. (8.7.3.12) [Non-Abelian Cohomology]. Let G, M be topological groups, with a continuous action of G on M, then we define $H^0(G,M) = M^G$.

We define $Z^1(G,M)$=continuous maps $x : G \to M$ that

$$\sigma_1(x(\sigma_2))x(\sigma_1\sigma_2)^{-1}x(\sigma_1) = 1, \quad \text{i.e.} \quad x(gh) = x(g)g(x(h))$$

If $x \in Z^1(G,M)$, then $x_m : \sigma \to m^{-1}x(\sigma)\sigma(m) \in Z^1(G,M)$ too. This defines an equivalence relation on $Z^1(G,M)$, the equivalence classes are called $H^1(G,M)$. This is compatible with the commutative case. ⌟

Prop. (8.7.3.13). Restriction map and inflation map is definable for H^0 and H^1, and $H^1(H,M)$ is a G/H-set where G acts on $H^1(H,M)$ by $g(c)(h) = g(c(g^{-1}hg))$. ⌟

Prop. (8.7.3.14). There is an exact sequence of pointed sets:

$$0 \to H^1(G/H, M^H) \xrightarrow{\text{inf}} H^1(G,M) \xrightarrow{\text{res}} H^1(H,M)^{G/H}.$$

⌟

Proof: First $\text{res}(H^1(G,M)) \subset H^1(H,M)^{G/H}$ because $g(c)(h) = c(g)^{-1}c(h)h(c(g))$ is checked so $g(c)$ is cohomologous to c.

$\text{res} \circ inf = 0$ is easy, if $\text{res}(c) = 0$, then c is trivial on H, hence $c(gh) = c(g)$ and $h(c(g)) = c(hg) = c(g \cdot g^{-1}hg) = c(g)$, so c is inflated from $H^1(G/H, M^H)$.

For the injectivity of inf. If $c(\overline{g}) = g^{-1}g(a)$, then $a \in M^H$, so it is a coboundary in $H^1(G/H, M^H)$. □

Prop. (8.7.3.15). Let $1 \to A \to B \to C \to 1$ be an exact sequence of G-groups, then there is a long exact sequence of pointed sets

$$1 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G,A) \to H^1(G,B) \to H^1(G,C) \xrightarrow{\Delta} H^2(G,A)$$

the last term is defined only when A is in the center of B.

Where δ is defined as follows: for $c \in C^G$, let b be an inverse image of c in B, then $a_\sigma = b^{-1}\sigma(b) \in A$, and it defines a cocycle in $H^1(G,A)$, different choice differ by a coboundary, so it is well-defined.

Δ is defines as: for c_σ a cocycle in $H^1(G,C)$, choose b_s inverse images of c_s, then $a_{\sigma,\tau} = b_\sigma\sigma(b_\tau)b_{\sigma\tau}^{-1}$ is a cocycle in $H^2(G,A)$. ⌟

Proof: Similar to (6.3.2.19), but need to show continuity**?** □

Prop. (8.7.3.16) [Hilbert's Theorem 90]. For $L/K \in \text{Gal}$, $H^1(\text{Gal}(L/K), \text{GL}_n(L)) = 1$, where L is equipped with the discrete topology. ⌟

Proof: We prove any cocycle is a coboundary, for this, notice any cocycle factor through a finite quotient, and the images of it is contained in a finite extension of K, hence it reduce to the case of L/K finite.

By definition, this is equivalent to any B-semi-linear representation of G free of finite rank is trivial, which is by(18.1.1.14). □

Cor. (8.7.3.17). $H^1(G(L/K), \text{SL}_n(L)) = 1$. This is seen from the exact sequence $1 \to \text{SL}(n,L) \to \text{GL}(n,L) \to L^\times \to 1$. ⌟

Interpretation of H^1 and Torsors

Def. (8.7.3.18) [A-Torsors]. A G-set X is a discrete set with a continuous G-action on X. Let A be a G-group, an **A-torsor** is a G-set with a right A-action that is simply transitive and semi-linear in G. ⌟

Prop. (8.7.3.19) [H^1 and Torsors]. We have a canonical bijection of pointed sets: $H^1(G, A) \cong TORS(A)$. ⌟

Proof: Let X be an A-torsor, choose $x \in X$, then $\sigma(x) = xa_\sigma$ for $a_\sigma \in A$. Now that $\sigma \mapsto a(\sigma)$ is checked to be a cocycle, and change of x changes to $\sigma \mapsto b^{-1}a_\sigma\sigma(b)$. Conversely, for an $a \in H^1(G, A)$, we let $X = A$ be a right A-module, and let $\sigma'(x) = a_\sigma\sigma(x)$, i.e. regarding coming from $x = 1$, then this is a inverse map. □

Prop. (8.7.3.20) [Extension of Rings]. ⌟

Prop. (8.7.3.21). There is an isomorphism of pointed sets $H^1(G, O(\varphi_L)) \cong E_\varphi(L/K)$. ⌟

Proof: Cf.[Neukirch Cohomology of Number Fields P346]. □

4 Continuous Cohomologies

In this subsubsection cohomology of G-modules with topology is studied. References are [Cohomology of Number Fields, Neukirch Chap 2.7].

Prop. (8.7.4.1). $H^*_{\text{cont}}(G, -)$ forms a long exact sequence for any $0 \to A \to B \to C \to 0$ of continuous G-modules. ⌟

Proof: ? □

Prop. (8.7.4.2). If A is a compact G-module which is an inverse limit of finite discrete G-modules A_n, then if $H^i(G, A_n)$ is finite for all n, then

$$H^{i+1}_{\text{cont}}(G, A) = \varprojlim_n H^{i+1}(G, A_n).$$

⌟

Proof: Cf.[Cohomology of Number Fields Neukirch P142]. □

Lemma (8.7.4.3). Let π be a topologically nilpotent element of A which is complete in the ϖ-adic topology and ϖ is not a zero-divisor, let $R = A/(\varpi)$ equipped with discrete topology. Let G be a group which acts continuously on A and fix π, then if $H^1(G, R)$ is trivial, then $H^1(G, A)$ is trivial, and if moreover $H^1(G, GL(n, R))$ is trivial, then $H^1(G, GL(n, A))$ is trivial. ⌟

Proof: Cf.[Galois Representations Berger P15]. □

Prop. (8.7.4.4) [Cyclic Case]. if G is a topological cyclic group $\overline{\langle g \rangle}$, then the map $H^1(G, M) \to M/(1-g)$ is well-defined and injective. And when M is profinite, p-adically complete, then the map is also surjective. ⌟

Proof: The surjection: there is only one choice: $c(g^i) = (1 + g + \ldots + g^{i-1})(m)$. And we need to verify that it is continuous. The case of p-adic can be deduced from profinite case, because $c(\gamma) \in p^{-k}M$ for some k, and $p^{-k}M$ is then profinite. For any finite quotient N of M, there is a k that $kM = 0$, and a n that $g^n = \text{id}$ on N, so $c(g^{rkn}) = 0$ on N, which shows c is continuous. □

Prop. (8.7.4.5) [Inf-Res Exact Sequence]. ⌟

Prop. (8.7.4.6) [Cohomology as Extensions]. Let G be a topological group acting on a field K and $W \in \mathrm{Rep}_K(G)$, there exists a bijection continuous extensions

$$0 \to W \to W' \to K \to 0$$

and $H^1_{\mathrm{cont}}(G, W)$ that is K-linear. ⌟

Proof: For any such extension, choose a K-linear splitting $W' \cong W \oplus K$, then

$$g(w, c) = (g(w) + g(c)\tau(g), g(c)),$$

where $\tau : G \to W$ is a continuous 1-coboundary in $H^1(G, W)$, and clearly changing a splitting changes this coboundary by a 1-cocycle, and it is clearly a bijection. □

8.8 Crystalline Cohomology

Main references are [Sta]and [Berthelot-Ogus, Notes on Crystalline Cohomology. Princeton University Press, 1978.]

1 PD-Schemes

Def. (8.8.1.1)[PD-Schemes]. A **pd-scheme** is a triple $(S, \mathcal{I}, \gamma)$ where S is a scheme, $\mathcal{I}$ is a Qco sheaf of ideals, and γ is a pd-structure on $\mathcal{I}$(5.6.0.1). A morphism of pd-schemes is a morphism that all the structure morphisms are morphisms of pd-structures. ⌟

Def. (8.8.1.2)[PD-Thickening]. A **pd-thickening** is a (U, T, δ) where T is a thickening of U(6.8.9.1) with sheaf of ideals $\mathcal{I}$(i.e. $U = \mathbf{Spec}(\mathcal{I})$) that $(T, \mathcal{I}, \delta)$ is a pd-structure. ⌟

Prop. (8.8.1.3). The fibered product of two morphisms in the category of pd-schemes exists if one of them is a pd-thickening. ⌟

Proof: Cf.[Sta]07ME. □

2 Crystalline Site

Def. (8.8.2.1)[Coverings]. A family of morphisms $\{(U_i, T_i, \delta_i) \to (U, T, \delta)\}$ of pd-thickenings is called a Zariski/smooth/étale/syntomic/fppf... iff

- $U_i = U \otimes_T T_i$,
- $\{T_i \to T\}$ is a Zariski/smooth/étale/syntomic/fppf... covering of T.

⌟

Def. (8.8.2.2)[Crystalline Sites]. Let p be a prime and $(S, \mathcal{I}, \gamma)$ be a pd-scheme over $\mathbb{Z}_{(p)}$, let $S_0 = V(\mathcal{I}) \subset S$, and $X \to S_0$ a morphism of schemes that p is nilpotent on X, then the **big-crystalline site** $(X/S)_{\mathrm{Crys}}$ consists of pd-thickenings(8.8.1.2) (U, T, δ) over $(S, \mathcal{I}, \delta)$ and a morphism of schemes $U \to X$, and the topology is the Zariski topology(8.8.2.1). In fact for any $(U, T, \delta) \in (X/S)_{\mathrm{Crys}}$, p is locally nilpotent in T, by(5.6.0.5).

The **crystalline site** $(X/S)_{\mathrm{crys}}$ is the strictly full subcategory consisting of objects that $U \to X$ is an open immersion.

Notice the structure sheaf that maps (U, T, δ) to $\Gamma(\mathcal{O}_U, U)$ is a sheaf of rings on $(X/S)_{\mathrm{crys}}$, called the **structure sheaf** $\mathcal{O}_{X/S}$. ⌟

Prop. (8.8.2.3)[Comparing with Zariski Site]. The functor

$$u_{X/S} : (X/S)_{\mathrm{crys}} \to X_{\mathrm{Zar}} : (U, T, \delta) \to U$$

is cocontinuous(easy to verify), thus defines a morphism of topoi $Sh((X/S)_{\mathrm{crys}}) \to Sh(X_{\mathrm{Zar}})$ by(6.1.2.21), which is functorial in X and S. ⌟

Prop. (8.8.2.4)[Finite Limits]. The category $(S/X)_{\mathrm{Crys}}$ has all finite limits, and the forgetful functor $(U, T, \delta) \to U$ preserves finite limits. ⌟

Proof: Cf.[[Sta]07I9].**?** □

Def. (8.8.2.5) [Affine Crystalline Site]. Let (A, I, γ) be a pd-structure that A is a $\mathbb{Z}_{(p)}$-algebra, and C is an A/I-algebra that p is nilpotent in C, then the crystalline site(8.8.2.2) $(C/A)_{\text{Crys}}$ is the site whose object are pd-structures (B, J, δ) over (A, I, γ) that p is nilpotent in B(5.6.0.5), together with a map of rings $C \to B/J$ over A/I, and $(C/A)_{\text{crys}}$ the full subcategory of objects B that $C \to B/J$ is an isomorphism.

Notice for any object (B, J, δ) in $(C/A)_{\text{Crys}}$, J is nilpotent, by(5.6.0.5). ⌟

Sheaf of Differentials

Def. (8.8.2.6) [S-Derivations]. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_{X/S}$-modules on $(X/S)_{\text{crys}}$, then an S-derivation $D : \mathcal{O}_{X/S} \to \mathcal{F}$ is a map of sheaves that for any object (U, T, δ) of $(X/S)_{\text{crys}}$, the map $D : \Gamma(T, \mathcal{O}_T) \to \Gamma(T, \mathcal{F})$ is a pd-derivation over $\Gamma(V, \mathcal{O}_V)$ for any open subset $V \subset S$ that $T \to S$ factors through V. ⌟

Prop. (8.8.2.7) [Sheaf of PD-Differentials]. Similar to the construction of sheaf of differentials(6.2.4.2), we can construct of sheaf of pd-differentials $\Omega_{X/S,\delta}$ on $(X/S)_{\text{crys}}$, which is a quotient of the sheaf of differentials $\Omega_{X/S}$. And similar to(6.2.4.3), for any $(U, T, \delta) \in (X/S)_{\text{crys}}$, $\Omega_{X/S,\delta}|_{(T/S)_{\text{crys}}} = \Omega_{T/S,\delta}$. ⌟

Prop. (8.8.2.8) [A First Order PD-Thickening]. Let $(U, T, \delta) \in (X/S)_{\text{crys}}$, $\mathcal{J}$ the ideal sheaf of U, we define a first order thickening T' of T: let $\mathcal{O}_{T'} = \mathcal{O}_T \oplus \Omega_{T/S,\delta}$ with the algebraic structure that $\Omega^2_{T/S,\delta} = 0$, and let $\mathcal{J}' = \mathcal{J} \otimes \Omega_{T/S,\delta}$, and define the pd-structure as

$$\delta'_n(f, \omega) = (\delta_n(f), \delta_{n-1}(f)\omega).$$

Then (U, T, δ') is a pd-thickening and $(U, T, \delta) \to (U, T', \delta')$ is a morphism in $(X/S)_{\text{crys}}$. Moreover, there are two ring maps

$$p_0, p_1 : \mathcal{O}_T \to \mathcal{O}_{T'} : p_0(f) = (f, 0), \quad p_1(f) = (f, d_{T/S,\delta}(f))$$

Then we get two contraction of the morphism $T \to T'$, and $p_0^* - p_1^*$ is the universal derivation $d_{T/S,\delta}$ included in $\mathcal{O}_{T'}$.

This construction is functorial in T/S by(8.8.2.7) and hence gives a functor of sites $(X/S)_{\text{crys}} \to (X/S)_{\text{crys}}$. ⌟

Proof: The verification of the pd-axioms in in [Sta]07HH. □

Prop. (8.8.2.9) [Second Order PD-Thickening]. There is a further thickening T'' of T', which is a second order thickening of T:

$$\Omega_{T''} = \mathcal{O}_T \oplus \Omega_{T/S,\delta} \oplus \Omega_{T/S,\delta} \oplus \Omega^2_{T/S,\delta}$$

with the algebra structure given by

$$(f, \omega_1, \omega_2, \eta)(f', \omega'_1, \omega'_2, \eta') = (ff', f\omega'_1 + f'\omega_1, f\omega'_2 + f'\omega_2, f\eta' + f'\eta + \omega_1 \wedge \omega'_2 + \omega'_1 \wedge \omega_2)$$

Let $\mathcal{J}'' = \mathcal{J} \oplus \Omega_{T/S,\delta} \oplus \Omega_{T/S,\delta} \oplus \Omega^2_{T/S,\delta}$, then there is a PD-structure on $\mathcal{J}''$ given by

$$\delta''_n(f, \omega_1, \omega_2, \eta)) = (\delta_n(f), \delta_{n-1}(f)\omega_1, \delta_{n-1}(f)\omega_2, \delta_{n-1}(f)\eta + \delta_{n-1}(f)\omega_1 \wedge \omega_2)$$

This construction is functorial in T/S by(8.8.2.7) and hence gives a functor of sites $(X/S)_{\text{crys}} \to (X/S)_{\text{crys}}$. ⌟

Proof: For the details, Cf.[Sta]07J3. □

3 Crystals

Def. (8.8.3.1) [Crystals]. In situation(8.8.2.2), for $\mathcal{F} \in \mathcal{M}od(X/S)_{\text{crys}}$, it restricts to a sheaf f_T on T for every object $(U,T,\delta) \in (X/S)_{\text{crys}}$. And it is functorial. Then $\mathcal{F}$ is called

- an $\mathcal{O}_{X/S}$-crystal if for any morphism $u : (U',T',\delta') \to (U,T,\delta)$ in $(X/S)_{\text{crys}}$, the morphism of $\mathcal{O}_{T'}$-modules $u^*\mathcal{F}_T \to F_{T'}$ is an isomorphism.
- **locally Qco** if $\mathcal{F}_T \in \mathcal{QC}oh(\mathcal{O}_T)$ for any $(U,T,\delta) \in (X/S)_{\text{crys}}$.
- **Qco** as defined in(6.2.2.25).

In particular, $\mathcal{O}_{X/S}$ is a crystal in $\mathcal{O}_{X/S}$-modules. ⌟

Def. (8.8.3.2). Is it true that if $X = S = \operatorname{Spec} R$ where R is a perfect ring, then a crystal is simply a module over $W(R)$**??** ⌟

Connections

Def. (8.8.3.3) [deRham Complexes for $(X/S)_{\text{crys}}$]. On a crystalline site $(X/S)_{\text{crys}}$, if we define $\Omega^i_{X/S,\delta} = \wedge^i \Omega_{X/S,\delta}$(8.8.2.7), then by(8.2.1.2), the universal S-derivative $d_{X/S}$ give rises to the **deRham complex**

$$\mathcal{O}_{X/S} \to \Omega^1_{X/S,\delta} \to \Omega^2_{X/S,\delta} \to \dots$$

as $\mathcal{O}_{X/S}$-modules on $(X/S)_{\text{crys}}$. ⌟

Proof: The verification of the condition for the quotient $\Omega_X \to \Omega_{X/S,\delta}$ is routine. □

Def. (8.8.3.4) [Connections on $(X/S)_{\text{crys}}$]. we define the notion of connection on $(X/S)_{\text{crys}}$ of an $\mathcal{O}_{X/S}$-module $\mathcal{F}$ on $(X/S)_{\text{crys}}$ w.r.t. the differential $\Omega_{X/S,\delta}$, as in(8.2.1.5). ⌟

Prop. (8.8.3.5) [Connections of Crystals]. Any $\mathcal{O}_{X/S}$-crystal $\mathcal{F}$ is equipped with a canonical integrable connection. ⌟

Proof: For any $(U,T,\delta) \in (X/S)_{\text{crys}}$, consider the first order thickening (U,T',δ') given in(8.8.2.8), then there are two projections $p_0, p_1 : T' \to T$ and a inclusion $i : T \to T'$, then by the property of crystals we get isomorphisms

$$p_0^*\mathcal{F}_T \xrightarrow{c_0} \mathcal{F}_{T'} \xleftarrow{c_1} p_1^*\mathcal{F}_T$$

then $\nabla(s) = p_1^*(s) - c_1^{-1}c_0(p_0^*(s))$ vanishes after pulling back to T via i^*, so it is in the kernel of i^*, which is

$$\mathcal{F}_T \otimes_{\mathcal{O}_T} \Omega_{T/S}$$

by the construction of T'(8.8.2.8). This ∇ is functorial in T as everything is functorial, hence gives a connection on $\mathcal{F}$.

For the integrability, Cf.[Sta]07J6.**?** □

Cor. (8.8.3.6). If $\mathcal{F}$ is a crystal in in Qco modules, then we can define a de Rham complex

$$\mathcal{F} \to \mathcal{F} \otimes_{\mathcal{O}_{X/S}} \Omega_{X/S,\delta} \to \mathcal{F} \otimes_{\mathcal{O}_{X/S,\delta}} \Omega^2_{X/S,\delta} \to \dots$$

⌟

Crystals in Qco modules

Def. (8.8.3.7) [Quasi-Coherent Crystals]. An $\mathcal{O}_X$-module $\mathcal{F}$ on $(X/S)_{\mathrm{crys}}$ is called a **quasi-coherent crystal** if it satisfies the following equivalent conditions:

- $\mathcal{F} \in \mathfrak{QCoh}(X/S)_{\mathrm{crys}}$.
- $\mathcal{F}$ is locally Qco(8.8.3.1) and it is a crystal in $\mathcal{O}_{X/S}$-modules.

Moreover, $\mathcal{F}$ is called a **crystal in finite locally free modules** if $\mathcal{F}$ is finite locally free. ⌟

Proof: Cf.[[Sta]07IT]. □

Def. (8.8.3.8) [Notations in Polynomial case]. If in situation(8.8.2.5), $S = \operatorname{Spec} A, X = \operatorname{Spec} C$, we let $P \to C$ be a surjection of A-algebras with $P = A[X_i]$, and the kernel is J. Set $D = D_{P,\gamma}(J)^\wedge$ be the p-adically completed pd-envelope, then $(D, \widehat{J}, \widehat{\gamma})$ admits a natural pd-structure, by(5.6.0.12). Let $D_e = D/p^e$ and J_e the image of $\widehat{J}$ in D_e. Denote

$$\Omega_D = (\Omega_{D/A,\gamma})^\wedge = (\Omega_{D_{P,\gamma}(J)/A,\overline{\gamma}})^\wedge = \lim_e \Omega_{D(n)_e/A,\overline{\gamma}}(5.6.1.4).$$

By(5.6.1.4), $\Omega_{D_{P,\gamma}(J)/A,\overline{\gamma}} = \Omega_{P/A} \otimes_P D_{P,\gamma}(J)$ which is free over $D_{P,\gamma}(J)$ on dx_i, so Ω_D is topologically free over D on dx_i, and there is a universal derivation $d : D \to \Omega_D$.

Now let $J(n) = \ker(P \otimes_A \otimes_A \ldots \otimes_A P \to C)$ where the tensor has $n+1$ factors, and

$$D(n) = (D_{P \otimes_A \otimes_A \ldots \otimes_A P/A,\gamma}(J(n)))^\wedge$$

with divided ideals $\widehat{J}(n)$, and also $D(n)_e = D(n)/p^e$, $T(n)_e = \operatorname{Spec} D(n)_e$, then $(X, T(n)_e, \overline{\gamma}(n))$ is a pd-thickening by(5.6.0.5) for e large(5.6.0.12), by(5.6.0.5) as p is nilpotent in X. And

$$\Omega_{D(n)} = (\Omega_{D(n)/A,\overline{\gamma}(n)})^\wedge.$$

Then $D(0) = D, D(1), \ldots$ form a cosimplicial pd-structures.

Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_{X/S}$-modules, denote

$$M(n) = \lim_e (\Gamma((X, T(n)_e, \overline{\gamma}(n)), \mathcal{F})).$$

⌟

Prop. (8.8.3.9). Notation as in(8.8.3.8), there is an isomorphism

$$D(n) \cong (D\langle \xi_i(j) \rangle)^\wedge$$

where $\xi_i(j) = X_i \otimes 1 \otimes \ldots 1 - 1 \otimes 1 \ldots X_i \otimes 1 \otimes \ldots 1$. ⌟

Proof: There is an isomorphism $P \otimes_A \ldots \otimes_A P \cong P[\xi_i(j)]$, and $J(n)$ is just generated by $JP \otimes_A \ldots \otimes_A P + (\xi_i(j))$, so this theorem follows from(5.6.0.17). □

Crystals and Connections

Lemma (8.8.3.10) [Crystals and Connections]. Notation as in(8.8.3.8), there is a functor from the category of crystals in Qco $\mathcal{O}_{X/S}$-modules to the category of pairs (M, ∇) that

- M is a p-adically complete D-module.
- $\nabla : M \to M \widehat{\otimes}_D \Omega_D$ is an integrable connection.

- ∇ is topological quasi-nilpotent: for any $m \in M$, there are only f.m. pairs (i,k) that $\nabla^k_{\partial/\partial x_i}(m) \in pM$.

⌟

Proof: For a crystal, we associate to it $M = M(0)$ defined in(8.8.3.8). let $\Gamma((X, T(0)_e, \overline{\gamma}(0)), \mathcal{F}) = M_e$, then because $\mathcal{F}$ is a crystal in qco sheaves, $\mathcal{F}_{T(0)_e} = \widetilde{M_e}$, and $M_e = M_{e+1}/p^e M_{e+1}$, thus $M_e = M/p^e M$ and M is p-adically complete by(5.2.3.6). By evaluating the natural connection defined in(8.8.3.6) on T_e and take limit, then we get an integral connection $\nabla : M \to M\widehat{\otimes}_D \Omega_D$.

To show this integral is topologically quasi-nilpotent, we can do the same thing for $M = M(n)$ for any n, and using the crystal property of $\mathcal{F}$ and take limits, we get isomorphisms

$$M\widehat{\otimes}_{D,p_0} D(1) \to M(1) \to M\widehat{\otimes}_{D,p_1} D(1)$$

For the rest, Cf.[Sta]07JG. □

Prop. (8.8.3.11). The functor defined in(8.8.3.10) is an equivalence of categories. ⌟

Proof: Cf.[Sta]07JH. □

Def. (8.8.3.12) [Notations in Smooth Case]. Situation as in(8.8.3.8), but this time we choose a smooth A-algebra P' and $A \to P' \to C$ with $\ker(P' \to C) = J'$ and do the same as(8.8.3.8) again, to get

$$D' = D_{P',\gamma}(J')^\wedge$$

and

$$\Omega_{D'} = (\Omega_{D'/A,\gamma})^\wedge = (\Omega_{D_{P',\gamma}(J)/A,\overline{\gamma}})^\wedge = \lim_e \Omega_{D'(n)_e/A,\overline{\gamma}}$$

⌟

Prop. (8.8.3.13)[Crystals and Connections in Smooth case]. Situation as in(8.8.3.8) and(8.8.3.8), then we can find a $P = A[X_i]$ that there are maps $a : D \to D', b : D' \to D$ between the completed pd-envelope of P, P' that $a \circ b = \mathrm{id}$ and compatible with the maps $D \to C$ and $D' \to C$, such that the base change along a, b induces an equivalence of categories between the categories of modules with an integrable connection over D as in(8.8.3.10) and the category of modules over D' with an integrable connection. ⌟

Proof: We con find P that $P \to C$ factors through a surjection $P \to P'$, hence we get a surjection $a : D \to D'$ the left adjointness of pd-envelope. Let e large that D'_e is a pd-thickening of C over A by(5.6.0.12)(5.6.0.5), then the kernel of $D_e \to D'_e$ is nilpotent by(5.6.0.5), hence by the strongly lifting property(5.4.5.16) of the smooth ring map $P \to P'$(5.4.5.21) w.r.t. the thickening $D_e \to D'_e$, we find a lift $P' \to D_e$.

Notice $D_{e+i+1} \to D_{e+i} \times_{D'_{e+i}} D'_{e+i+1}$ is surjective with nilpotent kernels(because $p^{e+i}D \to p^{e+i}D'$ is surjective), we can use the smooth of $A \to P$ to lift inductively the map $P' \to D_e$ to a map $P' \to D$, thus by universal property of completed pd-envelope extends to a map $b : D' \to D$. It is clear that $a \circ b = \mathrm{id}$.

For the equivalence of categories, Cf.[[Sta]07L5].**?** □

Remark (8.8.3.14). In fact this proposition holds with P' being any ring that $A \to P'$ satisfies the strong lifting property(5.4.5.16). In particular, this holds for ind-smooth A-algebras(8.5.2.5). ⌟

4 (F-)Isocrystals

References are [Slope Filtrations of F-Crystals, Katz].

Notation (8.8.4.1).
- Let $R \in \mathcal{CR}\mathrm{ing}/\mathbb{F}_p, S = \operatorname{Spec} R$.

⌟

Def. (8.8.4.2) [Crystals and Isocrystals]. A **locally free crystal over** S is simply a module over $W(R)$.

An **isocrystal on** S is an object in the category of locally free crystals on S up to isogeny, i.e. a module over $W(R)[\frac{1}{p}]$.

An **F-isocrystal on** S is a pair (M, φ) where M is an isocrystal over S and $\varphi : M^{(p)} \cong M$ is an isomorphism of isocrystals over S. The category of F-isocrystals over S is denoted by F-Isoc(S). ⌟

Over Perfect Fields

Notation (8.8.4.3).
- Let $k \in \mathtt{Field}^p$ be a perfect field.
- $K_0 = W(k)[\frac{1}{p}]$ its maximal unramified subextension.
- The Frobenius action on K_0 is denoted by σ.
- We abbreviate F-isocrystals to isocrystals.

⌟

Def. (8.8.4.4) [Isocrystals and φ-Modules]. An isocrystal over k is the same thing as a φ-module over (K_0, σ)(18.4.8.1). ⌟

Def. (8.8.4.5) [Hodge-Tate Weight]. For any complete $W(k)$-lattice M of D, let a_n be the maximum integer that $\varphi^n(M) \subset p^{a_n} M$, then we have $a_{m+n} \geq a_m + a_n$, thus by(2.6.1.1), we have a_n/n converges to $\sup a_n/n = \lambda$. λ doesn't depend on M because of the cofinality of lattices, and it is called the **Hodge-Tate weight** of D. ⌟

Lemma (8.8.4.6). Let M be a lattice of D that $\varphi^{h+1}(M) \subset p^{-1}M$, where h is the dimension of D, then D is effective. ⌟

Proof: Let $M_j = M + \varphi(M) + \ldots + \varphi^j(M)$, then $M_j/M \subset p^{-1}M/M$, which is a k-vector space of dimension h, then $M_j = M_{j+1}$ for some j, hence M_j is stable under φ. □

Prop. (8.8.4.7). $\lambda \geq 0$ iff D is effective(18.4.8.11). And $\lambda = s/r$, where $1 \leq r \leq h$. ⌟

Proof: If D is effective, then $a_n \geq 0$, conversely, if $a_n \geq 1$, then $M' = M + \varphi(M) + \ldots + \varphi^{n-1}(M)$ is stable under φ, so D is effective.

For the second assertion, we first notice, if $\lambda > 0$, then φ is nilpotent on M/pM, which is a k-vector space of dimension h, then $\varphi^h = 0$ on M/pM, so $\lambda \geq 1/h$.

Now we find s, r that $|r\lambda - s| \leq 1/(h+1)$, and $\widetilde{\varphi} = p^{-s}\varphi^r$ has $|\widetilde{\lambda}| \leq 1/(h+1)$, so(8.8.4.6) shows that $\widetilde{\varphi}$ is effective, hence $\widetilde{\varphi} \geq 0$, and by what we have proved, $\widetilde{\varphi} = 0$, hence it is $\lambda = s/r$. □

Lemma (8.8.4.8). For a φ-stable $W(k)$-lattice M of D, one has $M = M_0 \oplus M_{>0}$, where φ is bijection on M_0 and topologically nilpotent on $M_{>0}$. ⌟

Proof: We consider M/p^nM, then by(3.2.4.5) under slight modification, we have a decomposition for M/p^nM. This decompositions for different n are compatible, so taking an inverse limit gives a decomposition of M it self. ☐

Def. (8.8.4.9) [Isotypical φ-Modules]. $V \in \varphi\mathfrak{Mod}(K_0)$ is called **pure(isotypical) of slope** $\lambda = s/r \in \mathbb{Q}$ if V admits a lattice M on which $p^{-s}\varphi^r$ is a bijection. This is independent of V because λ is independent of V. ⌟

Prop. (8.8.4.10)[Dieudonné-Manin]. Any $V \in \varphi$-$\mathfrak{Mod}(K_0)$ is a finite sum of modules pure of slopes λ_i. This is called the **isocrystal decomposition** of V. ⌟

Proof: We use the $\widetilde{\varphi}$ as in the proof of(8.8.4.7), we see that M has a decomposition $M_0 \oplus M_{>0}$ by(8.8.4.8), and $M_0 \neq 0$ by definition. Then we use induction to get the result. ☐

Lemma (8.8.4.11). If k is a separably closed field and V is a φ-module with $a \geq 1$ of slope 0, then V has a basis of elements fixed by φ, and $1 - \varphi$ is a surjection.

If $A = W(k)$ is a ring with k a separably close field and V is a φ-module over A with $a \geq 1$ and slope 0, then V has a basis of elements fixed by φ, and $1 - \varphi$ is a surjection. ⌟

Proof: We choose a $e_0 \in V$, and set $e_i = \varphi^i(e_0)$, and suppose $e_d = a_0e_0 + \ldots + a_{d-1}e_{d-1}$, then if we consider the equation $\varphi(b_0e_0 + \ldots + b_{d-1}e_{d-1}) = b_0e_0 + \ldots + b_{d-1}e_{d-1}$, then we need to assure b_{d-1} is a zero of

$$x = a_0^{q^{d-1}}x^{q^d} + a_1^{q^{d-2}}x^{q^{d-1}} + \ldots + a_{d-1}x^q$$

which is separable, so it has a non-zero solution in k, so φ has a fixed point v. By induction, we have $V/k \cdot v$ admits a basis fixed by φ. We know that $1 - \varphi : k \cdot v \to k \cdot v : x \mapsto (x - x^q)$ is surjective, so we can adjust the coefficient of v to get a basis of V fixed by φ. And meanwhile we proved $1 - \varphi$ is surjective.

The second assertion follows from successive approximation, as $x^p - x - a$ always has a root in k. ☐

Def. (8.8.4.12). When k is alg.closed, for $\lambda = s/r$, we define a φ-module over $K = W(k)[1/p]$ $E_\lambda = \oplus_{i+0}^{r-1}Ke_i$ that $\varphi(e_i) = e_{i+1}$, and $\varphi(e_{r+1}) = p^se_0$. In this case, E_λ is irreducible. ⌟

Proof: If D is a $W(k)$-lattice stable under φ, then we may assume it is pure of slope d/h by(8.8.4.10), and then we find an element $y = \sum y_ie_i$ fixed by $p^{-d}\varphi^h$, then $p^{sh}\varphi^{rh}(y_i) = p^{rd}y_i$, which by valuation is only possible when $sh = rd$, so $h \geq r$, so D generate E_λ. ☐

Thm. (8.8.4.13) [Dieudonné-Manin]. If $k = \overline{k}$, then any $V \in \varphi$-$\mathfrak{Mod}(K_0)$ has a unique decomposition as sums of E_{λ_i}(8.8.4.12). ⌟

Proof: By(8.8.4.10) we assume D is pure, then by(8.8.4.11) we find a basis y_i that $\varphi^r(y_i) = p^sy_i$, then there is a map $E_\lambda \to D$. Since E_λ is irreducible, this is injective, and we consider all y_i until $E_\lambda^m \to V$ is surjective, then it is an isomorphism(this is like the case of simple modules). ☐

Def. (8.8.4.14) [Tate Twists]. The Tate object $\mathbb{1}(n), n \in \mathbb{Z}$ is the 1-dimensional isocrystal over K_0 that $\varphi = p^n\sigma$, so it is of slope n. And the **Tate twist isocrystal** is tensoring by $\mathbb{1}(n)$. It preserves rank and shifts Hodge-Tate weight by n. ⌟

5 Properties

Cf.[Sta]Chap55.24.

Def. (8.8.5.1) [Higher Direct Images]. Let p be a prime number, $(S,\mathcal{I},\gamma)\to(S',\mathcal{I}',\gamma')$ be a morphism of PD-schemes over $\mathbb{Z}_{(p)}$ and $f:X/S_0\to X'/S_0'$ be a morphism of schemes that p is locally nilpotent on X and X'. For the rest, Cf.[Sta]07MJ. ⌟

Def. (8.8.5.2) [F-Crystals]. In situation(8.8.2.2), let $S=\operatorname{Spec}A$ where (A,I,γ) is a divided power algebra with $p\in I$, and there is a Frobenius σ on A extending that of A/I. Since the absolute Frobenius on X and S_0 are compatible, thus there is a morphism of crystalline site $(F_X)_{\mathrm{crys}}:(X/S)_{\mathrm{crys}}\to(X/S)_{\mathrm{crys}}$.

Then an **F-crystal** on X/S relative to σ is a pair $(\mathcal{E},F_{\mathcal{E}})$ given by a crystal in finite locally free $\mathcal{O}_{X/S}$-modules(8.8.3.7) together with a map

$$F_{\mathcal{E}}:(F_X)^*_{\mathrm{crys}}\mathcal{E}\to\mathcal{E}.$$

A **non-degenerate F-crystal** is an F-crystal that there exists a map $V:\mathcal{E}\to(F_X)^*_{\mathrm{crys}}\mathcal{E}$ that $V\circ F_{\mathcal{E}}=p^i\,\mathrm{id}$ for $i\geq 0$. ⌟

6 Computations

Prop. (8.8.6.1) [Affine Thickening is Acyclic]. If T is a locally Qco sheaf of $\mathcal{O}_X$-modules on (X/S), then $H^p((U,T,\delta),\mathcal{F})=0$ for any $p>0$ and U or T affine. ⌟

Proof: Firstly notice U is affine iff T is affine, by(6.8.9.2), then we use(6.3.2.16) with $\mathfrak{G}$ being the affine thickenings and Cov the affine coverings of affine thickenings, then Cov is cofinal, and it suffices to check that $\check{H}^q(T,\mathcal{F})=0$ for an affine thickening T and $q>0$, and this is just the usual cohomology for Qco sheaves as the affine covering is cofinal, and it follows from(6.7.1.1). □

Lemma (8.8.6.2). Situation as in(8.8.3.8), then the morphism

$$(\operatorname{colim}_e h_{(X,T_e,\overline{\delta})})^\sharp\to *$$

of sheaves on $(X/S)_{\mathrm{crys}}$ is surjective. ⌟

Proof: We need to show that for any $(U,B,\delta)\in(X/A)_{Crys}$, there is an Zariski covering (U_i,B_i,δ) of it that there are maps $(U_i,B_i,\delta)\to(X,T_{e_i},\overline{\delta})$ that are compatible, But this is in fact equivalent to the existence of a morphism $(U,B,\delta)\to(X,\operatorname{Spec}D,\delta)$ of pd-structures. For this, notice the morphism $U\to X$ can be extended to a morphism $X\to\operatorname{Spec}P$ by strong lifting property(5.4.5.16) of smooth morphism(5.4.5.21), and this extends to the desired morphism by the universal property of pd-envelope and the fact p is locally nilpotent on B(8.8.2.2) thus B is locally p-complete. □

Lemma (8.8.6.3). Let $K'=(\operatorname{colim}_e h_{(X,T_e,\overline{\delta})})^\sharp$, then the product sheaf $(K')^n$ is in fact isomorphic to $(\operatorname{colim}_e h_{(X,T(n)_e,\overline{\delta})})^\sharp$ on $(X/S)_{\mathrm{crys}}$. ⌟

Proof: This follows from the definition and the universal properties of completion, pd-envelope and $P\otimes_A\otimes_A\ldots\otimes_A P$ is a coproduct. Compare with the proof of(8.8.6.2). □

Prop. (8.8.6.4). Situation as in(8.8.3.8), if $\mathcal{F}$ is locally Qco and satisfies: for any morphism $f : (U,T,\delta) \to (U',T',\delta') \in (X/S)_{\mathrm{crys}}$ that $f : T \to T'$ is a closed immersion the map $f^*\mathcal{F}_{T'} \to \mathcal{F}_T$ is surjective, then the complex

$$M(0) \to M(1) \to \dots$$

computes $R\Gamma((X/S)_{\mathrm{crys}}, \mathcal{F})$. Moreover,

$$R\Gamma((X/S)_{\mathrm{crys}}, \mathcal{F} \otimes_{\mathcal{O}_{X/S}} \Omega^i_{X/S,\delta}) = 0$$

for $i > 0$. ⌟

Proof: We use(6.3.1.19) for the presheaf $K' = \mathrm{colim}_e\, h_{(X,T_e,\overline{\delta})}$ and $K = *$, which satisfies the condition by(8.8.6.2). Then we get a spectral sequence

$$E_1^{p,q} = H^q(K'_p, \mathcal{F}) \Rightarrow H^{p+q}(K, \mathcal{F}).$$

Notice $K'_n = (\mathrm{colim}_e\, h_{(X,T(n)_e,\overline{\delta})})^\sharp$ by(8.8.6.3), so the cohomology

$$R\Gamma(K'_n, \mathcal{F}) = R\lim_e(\Gamma((X, T(n)_e, \overline{\gamma}(n)), \mathcal{F}))$$

Now the surjectivity $f^*\mathcal{F}_{T'} \to \mathcal{F}_T$ is equivalent to the surjectivity $\mathcal{F}_{T'} \to f_*\mathcal{F}_T$, so there is an exact sequence of Qco $\mathcal{T}'$-sheaves

$$0 \to \mathcal{K} \to \mathcal{F}_{T'} \to f_*\mathcal{F}_T \to 0$$

which implies that $\mathcal{F}((U',T',\delta')) \to \mathcal{F}((U,T,\delta))$ is surjective, by(6.7.4.2) and(6.7.1.3).

Then by(5.9.3.3),

$$R\Gamma(K'_n, \mathcal{F}) = R\lim_e(\Gamma((X, T(n)_e, \overline{\gamma}(n)), \mathcal{F})) = M(n)$$

thus we are done. □

Lemma (8.8.6.5). Situation as in(8.8.3.8), the complex $\Omega_{D(\bullet)}$ is homotopic to 0 as a $D(\bullet)$-cosimplicial module. ⌟

Proof: This complex is the p-adic completion of the base change of the cosimplicial module $M_\bullet = (\Omega_{P^{\otimes^\bullet_A}/A})$ under the cosimplicial ring map $P^{\otimes^\bullet_A} \to D(\bullet)$. Then it suffices to show $M_\bullet$ is homotopic to 0. For this, the whole thing can be written down clearly, Cf.[Sta]07LA. □

Lemma (8.8.6.6). In situation(8.8.3.8), for any cosimplicial module M_* over the cosimplicial ring $D(*)$ and $i > 0$, the cosimplicial module

$$M_0 \widehat{\otimes}_{D(0)} \Omega^i_{D(0)} \to M_1 \widehat{\otimes}_{D(1)} \Omega^i_{D(1)} \to \dots$$

is homotopic to 0. ⌟

Proof: □

Crystal Case

Prop. (8.8.6.7). Situation as in(8.8.3.8), and let $\mathcal{F}$ be a crystal in Qco modules, and let (M,∇) be the corresponding module with connection over D by(8.8.3.10), then the complex

$$M\widehat{\otimes}_D\Omega^\bullet_D$$

computes $R\Gamma((X/S)_{\mathrm{crys}},\mathcal{F})$. ⌟

Proof: Use the spectral sequence associated to the double complex

$$K^{a,b}=M\widehat{\otimes}_D\Omega^a_{D(b)}$$

Then the rows $K^{a,\bullet}$ is acyclic for $a>0$ by(8.8.6.6) and(5.8.2.21), and $K^{0,\bullet}$ is quasi-isomorphic to $R\Gamma((X/S)_{\mathrm{crys}},\mathcal{F})$ by(8.8.6.4). Now we look at the other direction, (5.6.1.7) and(8.8.3.9) show that each of the b maps $D\to D(b)$ determines the same quasi-isomorphism

$$M\widehat{\otimes}_D\Omega^*_D\cong M\widehat{\otimes}_{D(b)}\Omega^*_{D(b)}$$

as their inverse is given by the same $D(b)\to D$. Then it is clear that the E_2 page in this direction is $H^a(M\widehat{\otimes}_D\Omega^*_D)$ in the zero-th row and vanish otherwise, so we get the desired isomorphism by edge morphisms. □

Prop. (8.8.6.8) [de Rham Comparison for Crystalline Cohomology]. In situation(8.8.3.12), let $\mathcal{F}$ be a crystal in Qco modules, and let (M',∇') be the corresponding module with connection over D' by(8.8.3.13), then the complex

$$M\widehat{\otimes}_{D'}\Omega^\bullet_{D'}$$

computes $R\Gamma((X/S)_{\mathrm{crys}},\mathcal{F})$. ⌟

Proof: Let $b:D'\to D, a:D\to D'$ be the maps defined in(8.8.3.13), then by(8.8.6.7), it suffices to prove the base change along a,b induces quasi-isomorphisms

$$M\widehat{\otimes}_D\Omega^\bullet_D\cong M\widehat{\otimes}_{D'}\Omega^\bullet_{D'}.$$

$a\circ b$ is trivial, thus it suffices to prove that $b\circ a$ induces anautomorphism of $M\widehat{\otimes}_D\Omega^\bullet_D$. In fact, this is true for any morphism $\rho:D\to D$ of pd-algebras over A compatible with the map $D\to C$:

Write $\rho(x_i)=x_i+z_i$, where $z_i\in J$ because ρ is compatible with $D\to C$. Then we can factor ρ as

$$D\xrightarrow{\sigma}D\langle\xi_i\rangle^\wedge\xrightarrow{\tau}C$$

where $\sigma(x_i)=x_i+\xi_i$ and $\tau(\xi_i)=z_i$.

Notice that there exists an automorphism α of $D\langle x_i\rangle^\wedge$ that maps x_i to $x_i-\xi_i$ and ξ_i to ξ_i. (Such a map exists because by universal property, it suffices to give a map of pairs

$$(P,J)\to D_{P,\gamma}(J)\langle\xi_i\rangle=D_{P[\xi_i],\gamma}(JP[\xi_i]+(\xi_i))$$

by(5.6.0.17), and we surely have.

Now α is an automorphism, we have a quasi-isomorphism

$$M\widehat{\otimes}_D\Omega^*_D\cong M\widehat{\otimes}_{D,\sigma}\Omega^*_{\widehat{D\langle\xi_i\rangle}}$$

by(5.6.1.7). Also τ induces an isomorphism because it has a right inverse, which is an isomorphism by(5.6.1.7) again, so ρ induces an isomorphism. □

Cor. (8.8.6.9) [Crystalline-de Rham Comparison modulo p]. In situation(8.8.3.12), if R is a smooth A/p-algebra, then there is a natural quasi-isomorphism

$$R\Gamma_{\text{crys}}(R/A)\otimes^L_A A/p\cong\Omega^\bullet_{R/(A/p)}$$

of commutative algebra objects. ⌟

Proof: we choose P to be a smooth lift of R**?** to A, then $J=IP$, and by(5.6.0.11), the pd-structure extends to P, thus $D_{P/A,\gamma}=P$, and notice $\Omega^i_{P/A}$ is finite projective hence flat, so $\Omega^\bullet_{P/A}$ is K-flat(6.3.3.2), and the left side of is just $\widehat{\Omega}^\bullet_{P/A}\otimes_A A/p=\widehat{\Omega}^\bullet_{R/(A/p)}$ by(8.8.6.8)(5.6.1.2) and(5.4.3.6). □

8.9 Prismatic Cohomology(Bhatt-Scholze)

Main references are [Sta], [Prisms and Prismatic Cohomology, Bhatt-Scholze], [Notes on Prismatic Cohomology, Bhatt], [Prismatic Cohomology notes, Kedlaya].

1 Prisms

Def. (8.9.1.1) [Prisms]. A **prism** is a pair (A, I) where A is a δ-ring A and $I \in \mathrm{Ideal}(A)$, s.t.

- $V(I) \subset \operatorname{Spec} A$ is a Cartier divisor,
- A is derived (p, I)-complete, and
- $p \in I + \varphi(I)A$.

A prism (A, I) is called **perfect prism** if A is a perfect δ-ring(5.5.4.25). it is called **bounded prism** if A/I has bounded p^∞-torsion. It is called **crystalline prism** if $I = (p)$. It is called **orientable** if I is principal. It is called **oriented** if $I = (d)$ for some $d \in A^\times$.

A map of primes $f : (A, I) \to (B, J)$ is called **(faithfully)flat** iff the map $A \to B$ is (p, I)-completely (faithfully)flat(5.9.7.1). ⌟

Lemma (8.9.1.2). Let A be a δ-ring and I be a locally principal ideal contained in $\mathrm{rad}(A)$ that $(p, I) \subset \operatorname{rad} A$, then the following are equivalent:

- $p \in I^p + \varphi(I)A$.
- $p \in I + \varphi(I)A$.
- There is a f.f. morphism of δ-rings $A \to A'$ where A' is a finite product of localizations of A φ-stable multiplicative subsets that IA' is generated by a distinguished element d and $d, p \in \mathrm{rad}(A')$.

⌟

Proof: $1 \to 2$ is trivial, for $2 \to 3$: Choose $(g_1, \ldots, g_r) = A$ that $IA_{g_{r_i}}$ is principal. Let $B = \prod_{i=1}^r A_{g_i}$, so $A \to B$ is f.f. and $IB = (f)$ is principal. Lt A' be the localization of B along the ideal (p, f)(5.1.1.32), then $p, f \in \operatorname{rad} A'$. Then $A \to A'$ is still f.f., because it is flat hence the image is stable under generalization by(5.4.1.19), so it must be all of $\operatorname{Spec} A$ because it contains (p, I) by construction, and $(p, I) \in \operatorname{rad} A$ by hypothesis.

Now because $p \in \operatorname{rad} A$, each localization of A has a compatible δ-structure, and $\widetilde{A}$ is a finite product of localizations of A, thus it has a δ-structure, and d is distinguished by(5.5.4.23).

$3 \to 1$: We need to check that $p = 0$ in $A/(I^p + \varphi(I)A)$, but this can be checked after base change to A', which is $p = 0 \in A'/(d^p, \varphi(d))$. This is true, because $d^p = d^p + p\delta(d)$ and $\delta(d)$ is a unit. □

Remark (8.9.1.3) [Examples of Prisms].

- If A is a p-torsionfree and p-adically complete δ-ring A, the pair $(A, (p))$ is a bounded crystalline prism.
- q-de Rham cohomology(5.5.4.24) determines a bounded prism. (completeness and boundedness is clear, and $p \in (d, \varphi(d))$ because**?**)
- Breuil-Kisin cohomology(5.5.4.24) determines a bounded prism. (boundedness is clear, and**?**)
- A_{inf}-cohomolgoy(5.5.4.24) detemines a bounded prism. (The same reason as item2).

⌟

Prop. (8.9.1.4) [Universal Oriented Prism]. Let $A_0 = \mathbb{Z}_{(p)}\{d, \delta(d)^{-1}\}$ be the localization δ-ring(5.5.4.15) of the free $\mathbb{Z}_{(p)}$-δ-ring on the variable d, and let A be the derived (p, d)-completion of A_0(it is discrete by(5.9.7.7)), and let $I = (d)$, then (A, I) is a bounded oriented prism, and it is the initial object in the category of bounded oriented prisms.

Moreover, the sequence (p, d) is regular and the Frobenius $\varphi : A/p \to A/p$ is d-completely flat. ⌟

Proof: It is clearly a prism and universal. For the assertions, firstly we show $A/(p, d) = A_0/(p, d)$: notice $A \otimes^L_{A_0} A_0/(p, d) = A_0/(p, d)$ by(5.9.7.4), so we can replace $\otimes^L$ with $\otimes$. Similarly for $A/(p, d^p)$ because A is (p, d^p)-complete. Now this map is .

(p, d) is regular by(5.9.7.7) applied to $(\mathbb{Z}_{(p)}[d], A)$**?**, for the last assertion, it suffices to show $A/(p, d) \xrightarrow{\text{Frob}} A/(p, d^p)$ is f.f.. □

Prop. (8.9.1.5). Let $(A, (d))$ be the universal prism(8.9.1.4) and let $B = A\{\frac{\varphi(d)}{p}\}^\wedge$(derived (p, d)-completion), then B is (p, d)-complete, p-torsionfree and it equals the derived (p, d)-completion of the pd-envelope $D_{A,\delta}((d))$ of $(A, (d))$. In particular, $(B, (p))$ is a crystalline prism, by(5.5.4.18). ⌟

Proof: B is p-complete by(5.9.6.16), as A is p-torsionfree. Also $d^p = p(\frac{\varphi(d)}{p} - \delta(d))$, so B is also (p, d)-complete. The last assertion follows from(5.6.0.21) and(8.9.1.4). □

Cor. (8.9.1.6) [Connection with Crystalline Prism]. In the above situation, B is also a δ-ring by(5.5.4.17), and both $\varphi(d), p$ are distinguished in B and $\varphi(d)$ divides p in B, so by(5.5.4.22) $(\varphi(d)) = (p)$.

Now the composition of maps of δ-rings(5.5.4.5) $\alpha : A \xrightarrow{\varphi} A \to B$ promotes to a morphism of prisms(8.9.1.5) $(A, (d)) \to (B, (p))$ which decompose as

$$(A, (d)) \xrightarrow{\varphi} (A, \varphi(d)) \to (B, (\varphi(d))) = (B, (p))$$

⌟

Prop. (8.9.1.7) [Rigidity of Maps]. If $(A, I) \to (B, J)$ is a morphism of prisms, then $I \otimes_A B = J$, in particular, $IB = J$. Conversely, if B is a derived (p, I)-complete δ-A-algebra, then (B, IB) is a prism iff $B[I] = 0$. ⌟

Proof: For the first assertion, it suffices to show that $I \otimes_A B \to J$ is surjective, because they are both invertible sheaves on B. Choose f.f. ring morphisms $A \to A', B \to B'$ as in(8.9.1.2) and there is a morphism $A' \to B'$ extending $A \to B$, (by taking B as the localization of $A' \times_A B$ along (p, J) and do the construction again). Then $IB' \subset JB'$ are an inclusion of principal ideals generated by distinguished elements, thus they are equal, by(5.5.4.22), finally we use faithfully flatness.

For the second assertion, notice $B[I] = 0$ iff $I \otimes_A B \to IB$ is an isomorphism. If (B, IB) is a prism, then clearly $I \otimes_A B \to IB$ is an isomorphism, because they are both invertible sheaves. The converse is also trivial. □

Prop. (8.9.1.8)[Prism is Nearly Principal]. Let (A, I) be a prism, then the ideal $\varphi(I)A$ is a principal ideal, and any generator is a distinguished element. In particular, if it is a perfect prism, then $I = (f)$ where f is a distinguished element. ⌟

Proof: It suffices to prove $\varphi(I)A$ is generated by a single distinguished element, and then use(5.5.4.21). By(8.9.1.2), we can assume $p = a + b$ where $a \in I^p, b \in \varphi(I)A$. Now we show b generate $\varphi(I)A$: choose a f.f. map as in(8.9.1.2), and then it suffices to check that $b : A' \to \varphi(I)A'$

is surjective. Now $\varphi(I)A' = (d), a = xd^p, b = y\varphi(d)$, so it suffices to show y is a unit in A'. Now $(p, d) \in \mathrm{rad}\, A'$, it suffices to show $A'/(p, f, y) = 0$. If not, we localize along (p, f, y), then we may assume $(p, f, y) \in \mathrm{rad}\, A'$.

The equation $p = a + b$ implies $p(1 - y\delta(d)) = d^p(x + y)$, and the left side is distinguished because p does and $1 - y\delta(d)$ is a unit, by(5.5.4.21). Then(5.5.4.22) shows $d^{p-1}(x + y)$ is a unit, then so does d, contradicting $d \in \mathrm{rad}\, A'$. □

Remark (8.9.1.9). Notice the proof goes through even I is only a locally principal ideal of A. ⌟

Cor. (8.9.1.10). If (A, I) is a prism, the invertible A-modules $\varphi^*(I) = I \otimes_{A,\varphi} A$ and I^p are trivial. ⌟

Proof: Cf.[Prisms, Scholze, P25]. □

Prop. (8.9.1.11) [Properties of Bounded Prisms]. Let (A, I) be a bounded prism, then

1. Any derived (p, I)-complete and (p, I)-completely flat A-complex $M \in D(A)$ is discrete and (p, I)-complete. For any $n \geq 0$, we have $M[I^n] = 0$ and M/I^nM has bounded p^∞-torsion.
2. A is (p, I)-complete, A/I is p-adically complete, $A[I^n] = 0$ and A/I^n has bounded p^∞-torsions.
3. The category of (faithfully)flat prisms over (A, I) identifies with the category of (p, I)-completely (faithfully)flat δ-A-algebras B by the bijection $B \leftrightarrow (B, IB)$.
4. (Bounded Prisms are fpqc-Locally Orientable)There is a (p, I)-completely faithfully flat δ-A-algebra B that $IB = (d)$, where d is distinguished and determines a nonzero divisor of B. Also (B, IB) is bounded.

⌟

Proof: 1: By(5.9.7.7).

2 follows from1. For A/I, it is derived p-complete by(5.9.6.8), then it is p-adically complete by(5.9.6.16).

3: By definition, a (faithfully)flat (A, I)-prism is (p, I)-completely (faithfully)flat(5.9.7.1). Conversely, by(8.9.1.7), it suffices to show that $B[I] = 0$, and this follows from item1.

4: We may choose B to be the derived (p, I)-completion of the f.f. δ-ring defined in(8.9.1.2), then it is also (p, I)-completely faithfully flat(5.9.7.4), and by item2 and3 it determines a bounded prism (B, IB). □

Prop. (8.9.1.12) [The Site of Bounded Prisms]. The prismatic site is the opposite category of the category of bounded prisms where the covers are determined by f.f. map of prisms.

Then the functors that maps (A, I) to A or A/I are sheaves on this cohomology with vanishing higher cohomologies. ⌟

Proof: To show this is a site, we need to check the base change of covers. If $(C, IC) \xleftarrow{c} (A, IA) \xrightarrow{b} (B, IB)$ is a diagram that b is f.f., then we let D be the derived (p, I)-completion of $B \otimes^L_A C$, then $C \to D$ is also (p, I)-completely f.f. by(5.9.7.5), so by(8.9.1.11) and(8.9.1.7) D is discrete and (D, ID) is a bounded prism over (A, IA). It is clear this is a base change in the category of bounded prisms.

The assertion about cohomology follows from [Scholze, Prism, 3.12]. □

Prismatic Envelopes

Prop. (8.9.1.13) [Prismatic Envelopes]. Let (A, I) be a prism, then the forgetful functor from the prisms over (A, I) to δ-pairs over (A, I) admits a left adjoint, called the **prismatic envelope** which maps (B, J) to $B\{\frac{J}{I}\}^\wedge$. ⌟

Proof: If we can construct this locally, then we can construct it globally by gluing and the universal property, so we can localize and assume $I = (d)$ where d is distinguished. Let B' be the free δ-ring over A generated by $\{x/d | x \in J\}$(5.5.4.10) and B_1 the derived (p, d)-completion module of B which is a δ-algebra by(5.5.4.18).

If d is torsion-free in B_1, then $(B_1, (d))$ is a prism that satisfies the universal property. Otherwise we choose the maximal d-torsion-free quotient(5.1.1.15)(5.5.4.14) and taking the derived (p, d)-completion module, and we can do this to $\aleph_0$, where we take the filleted colimit, then it is d-torsion-free and (p, d)-complete, by(5.9.6.5) and any prism over A map factors through this chain. □

Cor. (8.9.1.14). In the above situation, if (B, J) is (p, I)-completely flat over A, and $J = (I, x_1, \ldots, x_n)$ where $(x_1, \ldots, x_n)$ is a (p, I)-completely regular sequence w.r.t. A, then the prismatic envelope of $(B\{\frac{J}{I}\}^\wedge, IB\{\frac{J}{I}\}^\wedge)$ is flat over (A, I)(8.9.1.1).

Moreover, It is compatible with completed derived base change on (A, I), by universal properties and the fact the completed derived base change of it is discrete(5.9.7.5). Also, it is compatible with completed derived base change along a (p, I)-completely flat map $(B, J) \to (B', J')$. ⌟

Proof: It suffices to check locally for $I = (d)$ that $B_1 = (B\{\frac{x_1}{d}, \ldots, \frac{x_n}{d}\})^\wedge$ as a simplicial δ-ring is (p, I)-completely flat over A, then it is discrete and is torsionfree by(8.9.1.11), thus it is a prism over $(A, (d))$ by(8.9.1.7). And for the flat localization, notice the image of $x_1, \ldots, x_n$ is also (p, I)-completely regular w.r.t. A.

Consider the following diagram of derived (p, d)-complete simplicial δ-rings:

$$\begin{array}{ccccccc}
\mathbb{Z}_p\{z\}^\wedge & \xrightarrow{z\mapsto d} & A & \longrightarrow & B & \longrightarrow & B\{\frac{x_1}{d}, \ldots, \frac{x_n}{d}\}^\wedge = C \\
\downarrow{\scriptstyle z\mapsto\varphi(y)} & & \downarrow & & \downarrow & & \downarrow \\
\mathbb{Z}_p\{y\}^\wedge & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & B'\{\frac{x_1}{\varphi(d)}, \ldots, \frac{x_n}{\varphi(d)}\}^\wedge = C' \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & D = A'\{\frac{\varphi(y)}{p}\}^\wedge & \longrightarrow & B'' & \longrightarrow & B''\{\frac{x_1}{p}, \ldots, \frac{x_n}{p}\} = C''
\end{array}$$

where each square is completed derived tensor product. Notice the lat term has denominator p because $\varphi(y)$ and p are both distinguished in $\pi_0(D)$, so by(5.5.4.22) $\frac{\varphi(y)}{p}$ is a unit in D.

The leftmost arrow is (p, z)-completely f.f. by(5.5.4.10)(5.9.7.4), so all the vertical arrow in the upper row is (p, z)-completely flat by(5.9.7.5). Now the map $D \to C''$ is (p, z)-completely flat by(5.6.0.24), noticing that the conditions holds, by(5.9.7.5).

Now by definition the (p, d)-completely flatness is defined by flatness after base change to $Kos(A, p, d)$(5.8.3.5), it suffices to show that there is a map $D \to Kos(A', p, d)$. To show this, it suffices to assume $A' = \mathbb{Z}_p\{y\} = \mathbb{Z}_p[y, y_1, \ldots, y_n, \ldots]$ and base change. In this case, p, y is a regular sequence, so by(5.6.0.21) D is the derived completion of $D_{\mathbb{Z}_p\{y\}}((y))$, and $Kos(A', p, y) = \mathbb{F}_p[y_1, \ldots, y_n]$, so $A' \to Kos(A', p, d)$ factors through D by universal property. □

2 Perfect Prisms

Prop. (8.9.2.1) [Properties of Perfect Prisms]. Let (A, I) be a perfect prism(8.9.1.1), then:

- $I = (d)$ where d is distinguished and is a nonzero-divisor.
- A is p-torsionfree and p-adically complete, hence there is a natural isomorphism $A \cong W(A/p)$ of δ-rings.

- $A/I[p^\infty] = A/I[p]$, and $A/p[I^\infty] = A/p[I]$. In particular, (A, I) is bounded.
- A is (p, I)-complete.

⌟

Proof: 1: I is principal by(8.9.1.8). d is distinguished by(5.5.4.23), it is nonzero-divisor by definition of prisms.

2: This is because A is p-torsionfree by (5.5.4.27) and thus p-adically complete by(5.9.6.16), then $A \cong W(A/p)$ by the equivalence in(5.5.4.28).

3: Use item2, then A/p is perfect by(5.5.4.28), thus $A/p[I^\infty] = A/p[I]$. $A/d[p^\infty] = A/d[p]$ follows from(5.5.4.30).

4: This follows from item3 and(8.9.1.11). □

Prop. (8.9.2.2) [Perfection of Prisms]. There is a **perfection of prisms** functor that maps a prism (A, I) to a perfect prism (A_∞, IA_∞) left adjoint to the inclusion functor. ⌟

Proof: Let $A'_\infty = A_{\text{perf}}$ be the perfection of A as a δ-ring(5.5.4.26), and A_∞ be the derived (p, I)-complete of A'_∞ as a δ-ring(5.5.4.18), then the universal property follows form that of derived completion and perfection once we proved that A_∞ is perfect and $IA_\infty = (d)$ where d is a nonzero-divisor.

A_∞ is perfect because the Frobenius is isomorphism on A_{perf} and derived (p, I)-completion and $(p, \varphi(I))$-completion coincide(they have the same radical(5.9.6.15)).

A_∞ is p-adically complete because it is p-torsionfree(5.5.4.27), and then use(5.9.6.16).

Now(8.9.1.9) and the fact A_∞ is perfect shows $IA_\infty = (d)$ where d is distinguished, and(5.5.4.30) shows d is a nonzero-divisor, so we are done. □

Prop. (8.9.2.3) [Perfect Prisms are Final]. Let (A, I) be a perfect prism, then for any prism (B, J), a map $A/I \to B/J$ will induce a map of prisms $(A, I) \to (B, J)$. ⌟

Proof: Cf.[B-S19]4.8.

This map will induce a map $A \cong W((A/I)^\flat) \to W((B/J)^\flat)$. And there is a Fontaine's functor $W((B/J)^\flat) \to B$(11.2.9.7) which is a δ-map. Thus we obtain a map $A \to B$. And this map can be seen to be lifting $A/I \to B/J$. □

3 Integral Perfectoid Rings

Def. (8.9.3.1) [Integral Perfectoid Rings]. A commutative ring R is called a **integral perfectoid ring** if it has the form A/I for a perfect prism (A, I). An equivalent definition of an integral perfectoid ring is given in(8.9.3.6). ⌟

Def. (8.9.3.2) [Special Fiber]. For an integral perfectoid ring R, then **special fiber** of R is defined to be $\overline{R} = R/\sqrt{pR}$. It is perfect, by(8.9.3.5). ⌟

Prop. (8.9.3.3) [Perfect Prisms and Integral Perfectoid Rings]. The mapping $(A, I) \to A/I$ defines an equivalence of categories between perfect prisms and integral perfectoid rings, where the converse is given by $R \mapsto (A_{\text{inf}}(R), \ker(A_{\text{inf}}(R) \to R))$(5.5.1.15). ⌟

Proof: To show $A \cong A_{\text{inf}}(A/I)$, by(5.5.4.28), it suffices to show there is a natural isomorphism $A/p \cong (A/I)^\flat$. By(5.5.1.18), $(A/I)^\flat$ identifies with d-adic completion of A/p. Then it suffices to show A/p is I-adically complete, which is by(5.9.6.16), as A/p is derived d-complete because A does(5.9.6.8).

Now we have the Fontaine's map $A = A_{\inf}(A/I) \to A/I$, this map is surjective because $\varphi : A/(p, I) \to A/(p, I)$ is surjective as A/p is perfect. Also this is just the quotient map $A \to A/I$ because they are equal when modulo p, and then use(5.5.4.28). □

Cor. (8.9.3.4). Any perfect $\mathbb{F}_p$-algebra is an integral perfectoid ring corresponding to a crystalline prism, by(5.5.4.28).

Any integral perfectoid ring is p-adically complete, by(8.9.1.11). ⌟

Prop. (8.9.3.5). If R is a perfectoid ring, then

- R is semiperfect.
- There exists an element $\varpi \in R$ that admits a compatible system ϖ^{1/p^n} of p-power roots s.t. $\varpi = pu$ for a unit u and the kernel of the Frobenius $\varphi : R/p \to R/p$ is generated by $\varpi^{1/p}$.
- $\sqrt{pR} = \cup_n(\varpi^{1/p^n})$, and it is flat.
- $R[p] = R[\sqrt{pR}]$.

⌟

Proof: 1: Let $R = A/d$ where $A = A_{\inf}(R)$, then $R/p = A/(p, d)$, so $\varphi_{R/p}$ is surjective, as $A/p = R^\flat$ is perfect.

2: Notice $d = [a_0] - pu$ for a unit $u \in A$ by(5.5.4.30), then we can take ϖ to be the image of $[a_0]$ in R, and then $\varpi^{1/p^n} = [a_0^{1/p^n}]$.

3: firstly the LHS contains the RHS, and $R/\cup_n(\varpi^{1/p^n})$ is perfect hence reduced, so the two sides are equal. To check it is flat, we need to check that $M\otimes^L_R \sqrt{pR}$ is discrete, or equivalently $M\otimes^L_R \overline{R} \in D^{\geq -1}$ where $\overline{R} = R/\sqrt{pR}$ is perfect. But there is a distinguished triangle $M\otimes^L_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p[-1] \to M \to M[\frac{1}{p}]$($\mathbb{Q}_p$ is $\mathbb{Z}_p$ flat(5.4.1.6)) and the fact $\overline{R}[\frac{1}{p}] = 0$, it suffices to prove $M\otimes^L_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p\otimes^L_R \overline{R} \in D^{\geq -2}(R)$. Now $M \otimes^L_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ has cohomology groups p^∞-torsion, so using canonical truncation, it suffices to show $M \otimes^L_R \overline{R} \in D^{\geq -1}$ for any p^∞-torsion M. Because tensoring commutes with filtered colimits, it suffices to show for M an R/p^n-module. Now using exact sequences like

$$0 \to M[p]/M[p^2] \to M/M[p^2] \to M[p]/M[p^2] \to 0,$$

we can reduce to the case M is a R/p-module.

Now there is a commutative diagram

$$\begin{array}{ccc} A_{\inf}(R) & \longrightarrow & R \\ \downarrow & & \downarrow \\ A_{\inf}(\overline{R}) & \longrightarrow & \overline{R} \end{array}$$

and d is p-torsionfree in both $A_{\inf}(R)$ and $A_{\inf}(\overline{R})$(5.5.4.30), and $d = [a_0] - pu = pu \in W(\overline{R})$(as $a_0 = 0 \in \overline{R}$), so $\overline{R} = W(\overline{R})/d$ and this is a Tor-independent pushout square. Thus $M \otimes^L_R \overline{R} \cong M \otimes^L_{W(R^\flat)} W(\overline{R})$. As p is nonzero divisor in both $A_{\inf}(R)$ and $A_{\inf}(\overline{R})$, and $pM = 0$, we have a similar diagram quotient by p, and by the same reason $M \otimes^L_{W(R^\flat)} W(\overline{R}) \cong M \otimes^L_{R^\flat} \overline{R}$. Now the kernel of $R^\flat \to \overline{R}$ is of the form (f^{1/p^∞}), where f corresponds to (ω^{1/p^n}), so the claim follows from(5.5.1.7).

4: notation as in the proof of item2, it suffices to show the A-module $R[p]$ is annihilated by $[a_0^{1/p^n}]$ for $n \geq 0$. But $R[p] = A/d[p] = A/p[d] = R^\flat[d]$, and $d = [a_0]$ on $R^\flat$, which is perfect, so we are done. □

Prop. (8.9.3.6) [Equivalent Definition of Integral Perfectoid Rings]. A commutative ring R is an integral perfectoid ring iff the following are satisfied:

- R is p-adically complete and R/p is semiperfect.
- The kernel of $\theta_R : A_{\text{inf}}(R) \to R$((5.5.1.15), notice R is p-adically complete) is principal.
- There exists some $\varpi \in R$ that $(\varpi^p) = (p)$.

And if R is p-torsionfree, the condition2 can be replaced by: R is p-normal**??**. ⌟

Proof: If R is an integral perfectoid ring, then these are true by(8.9.3.5). Now if these are satisfied, then firstly θ is surjective by(5.5.1.16). Next, let $d \in A_{\text{inf}}(R)$ be the generator of θ, we show $A_{\text{inf}}(R)$ is derived (p, d)-complete. it is derived p-complete by(5.9.6.16). Now $R^\flat$ is derived d-complete by(5.5.1.18). By induction and(5.9.6.8), $A_{\text{inf}}(R)/p^n$ are all derived d-complete, and also by induction $A_{\text{inf}}(R)/p^n$ has bounded d^∞-torsion, as $R^\flat$ is perfect. Then $A_{\text{inf}}(R)/p^n$ are all d-adically complete. Thus

$$A_{\text{inf}}(R) = \varprojlim_n A_{\text{inf}}(R)/p^n = \varprojlim_n \varprojlim_m A_{\text{inf}}(R)/(p^n, d^m),$$

which means $A_{\text{inf}}(R)$ is (p, d)-adically complete thus derived (p, d) adically complete.

Then it suffices to show d is distinguished, by(5.5.4.30). Let $\varpi^p = up$, and lift ϖ, u to $x, v \in A_{\text{inf}}(R)$. Since $A_{\text{inf}}(R)$ is d-adically complete, v is unit in $A_{\text{inf}}(R)$. Then $d | x^p - pv$ and $x^p - pv$ is distinguished(5.5.4.30). Now $d, p \in \text{rad}(A_{\text{inf}}(R))$ as $A_{\text{inf}}(R)$ is (d, p)-adically complete, so by(5.5.4.22), d is distinguished.

Now if R is a p-torsionfree integral perfectoid ring, if $x \in R[\frac{1}{p}]$ satisfies $x^p \in R$, let $n \geq 0$ minimal that $y = \varpi^n x \in R$, then we show $n = 0$: if $n > 0$, then $(\varpi^n x)^p = \varpi^{np} x^p \in \varpi^{np} R$. Then we get $\varpi^n x \in \varpi^n R$, and then $x \in R$ as R is p-torsionfree.

Conversely, we use condition$1, 2, 4$ to prove 3: We first show the kernel of $\varphi : R/p \to R/p$ is generated by ϖ as in condition4: if $x^p \in pR = \varpi^p y$, then $(x/\varpi)^p = y$, thus $x \in \varpi R$ by hypothesis. Since R/p is semiperfect, $\overline{\varpi}$ admits a compatible p^n-th roots $\{\overline{\varpi}^{1/p^n}\}$. It can be shown by induction that $\ker(\varphi^n) = (\overline{\varpi}^{1/p^n})$. This implies that the kernel of $\overline{\theta}_R : R^\flat \to R/p$ is generated by the element $\varpi^\flat$ determined by the system $\{\overline{\varpi}^{1/p^n}\}$. As $W(R^\flat)$ and R are both p-torsionfree and p-adically complete, they kernel of θ_R is generated by any element in the kernel that lifts $\varpi^\flat$. In particular, the kernel is principal. □

Prop. (8.9.3.7) [Pushout of Integral Perfectoid Rings]. Integral perfectoid rings are closed under pushouts in the category of derived p-complete rings: i.e. if $C \leftarrow A \to B$ are maps of integral perfectoid rings, then $B \widehat{\otimes}_A^L C$ is also an integral perfectoid ring. ⌟

Proof: Let $R = C^\flat \otimes_{A^\flat}^L B^\flat = C^\flat \otimes_{A^\flat} B^\flat$ which is a perfect ring, by(5.5.1.3) and(5.5.1.7). Then we have

$$W(R) = W(A^\flat) \widehat{\otimes}_{W(A^\flat)}^L W(B^\flat),$$

because this can be checked via derived Nakayama(5.9.6.10). Now use the fact $A = W(A^\flat)/d$ for some distinguished element d, and then $B = W(B^\flat)/d, C = W(C^\flat)/d$ by rigidity(8.9.1.7), and d is nonzero-divisor in $W(B^\flat), W(C^\flat), W(R)$ by(5.5.4.28), so taking derived base change along $W(A^\flat) \to A$, we get

$$D = W(R)/d = B \widehat{\otimes}_A^L C,$$

and $W(R)$ is a perfect prism, by(8.9.1.7), so $D = W(R)/d$ is an integral perfectoid ring and equals $B \widehat{\otimes}_A^L C$. □

Cor. (8.9.3.8). The category of integral perfectoid rings is closed under arbitrary colimits and products in the category of derived p-complete rings.

But it is not closed under equalizers: Notice by Ax-Sen-Tate, $(\mathcal{O}_{\mathbb{C}_p})^{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} = \mathbb{Z}_p$, but $\mathbb{Z}_p$ is not an integral perfectoid by(8.9.3.6). ⌟

Proof: It suffices to show it is closed under products and sums**?**. □

Prop. (8.9.3.9) [Gluing]. Let R be an integral perfectoid ring, $\overline{R} = R/\sqrt{pR}, S = R/R[\sqrt{pR}], \overline{S} = S/\sqrt{pS}$, then $\overline{R}, S, \overline{S}$ are perfectoids, and the square

$$\begin{array}{ccc} R & \longrightarrow & S \\ \downarrow & & \downarrow \\ \overline{R} & \longrightarrow & \overline{S} \end{array}$$

is both a homotopy fiber square(5.9.1.2) and pullback square. Moreover,

- S is p-torsionfree.
- $\sqrt{pR}$ maps isomorphically onto $\sqrt{pS}$.
- $R[\sqrt{pR}]$ maps isomorphically to $\ker(\overline{R} \to \overline{S})$, thus $x \mapsto x^p$ is bijective on $R[\sqrt{pR}]$.

In particular, any integral perfectoid ring is a fiber product of integral rings that is either perfect or p-torsionfree. ⌟

Proof: By(8.9.3.5), $R[\sqrt{pR}] = R[p^\infty]$. In particular, S is p-torsionfree. Now if we know this is a homotopy fiber square, then we get $2, 3$ by comparing the kernel. And if we know the kernel, then this is a pushout square by(5.1.1.24). So it suffices to show this is a homotopy fiber square.

Let $d = [a_0] - pu$ for a distinguished element of $A = A_{\mathrm{inf}}(R)$ that $R = A/(d)$, and the ideal $I = (a_0^{1/p^\infty}) \subset R^\flat$ and $J = R^\flat[I]$. Then the square

$$\begin{array}{ccc} W(R^\flat) & \longrightarrow & W(R^\flat/J) \\ \downarrow & & \downarrow \\ W(R^\flat/I) & \longrightarrow & W(R^\flat/I+J) \end{array}$$

is a homotopy fiber square: all vertices are p-torsionfree and p-adically complete, and the square gives a fiber square when modulo p^n(use induction on n and(5.5.1.8)), and then take derived p-completions. Next we apply**?** □

Cor. (8.9.3.10). Integral perfectoid rings are reduced. ⌟

Proof: By(8.9.3.9), we may assume R is p-torsionfree or perfect. Thus it suffices to assume R is p-torsionfree. Let $\varpi \in R$ that $\varpi^p = pu$ as in(8.9.3.6). If $x^p = 0$, we show inductively that $x \in \varpi^n R$. If $x = \varpi^n y$, then $y^p = 0$ as R is p-torsionfree. Now the kernel of Frobenius $\varphi : R/p \to R/p$ is generated by ϖ, thus we have $y \in \varpi R$, so we can use induction. □

4 Prismatic Site

Remark (8.9.4.1). In this subsection, fix a bounded prism (A, I), all formal schemes over A are assumed to have the (p, I)-adic topology, and formal schemes over A/I are assumed to have the p-adic topology. ⌟

Def. (8.9.4.2) [Prismatic Site]. Let (A,I) be a bounded prism and X be a smooth p-adic formal scheme over A/I, let $(X/A)_{\Delta}$ be the site whose objects are bounded prisms (B,IB) over (A,I) together with a map $\mathrm{Spf}(B/IB)\to X$ over A/I. The morphisms are the natural one, and the coverings in $(X/A)_{\Delta}$ are f.f. maps of prisms $(B,IB)\to(C,IC)$. There are structure sheaves $\mathcal{O}_{\Delta}((B,IB))=B$ and $\overline{\mathcal{O}}((B,IB))=B/IB$. They are sheaves by(8.9.1.12).

Thus $\mathcal{O}_{\Delta}$ is valued in (p,I)-complete δ-A-algebras and $\overline{\mathcal{O}}_{\Delta}$ is valued over p-complete-algebras(5.9.6.16). ⌟

Def. (8.9.4.3) [Perfect Prismatic Site]. The **perfect prismatic site** $(X/A)_{\Delta}^{\mathrm{perf}}$ is the full subcategory of $(X/A)_{\Delta}$ consisting of perfect prisms. By(8.9.3.3), objects in this site are equivalent to the category of perfectoid rings R over A/I with a map $\mathrm{Spf}\,R\to X$. ⌟

Remark (8.9.4.4). If we further restrict to the site of perfect prisms (S,I) that S/I is integrally closed in $S/i[\frac{1}{p}]$, then we will get the notion of diamond of $(X[\frac{1}{p}],X)$, in sense of[Sch12]. ⌟

Def. (8.9.4.5) [Absolute Prismatic Site]. For a p-adic formal scheme X the **absolute prismatic site** consisting of bounded prisms (B,J) with a map $\mathrm{Spf}\,B/J\to X$. ⌟

Prop. (8.9.4.6) [Prismatic Site and Étale Site]. Let $\mathcal{FS}\mathrm{ch}\,/X$ be the category of p-adic formal schemes over X with the étaletopology, then there is a natural functor $\mu:(X/A)_{\Delta}\to\mathcal{FS}\mathrm{ch}\,/X$ sending (B,IB) over X to $\mathrm{Spf}\,B/IB\to X$.

This functor is cocontinuous: for any p-completely étalemap $B/IB\to C$, it is a derived p-completion of some étalemap $B/IB\to\overline{C}'$ by(5.9.7.9), and this can be lifted to a map $B\to S_C'$ by(8.9.1.11)(5.3.10.6) and(5.3.10.9), and we choose the (p,I)-completion of S_C, then it is a prism that lifts C. Thus by(6.1.2.21) defines a morphism of topoi:

$$\mu:\mathcal{S}\mathrm{h}((X/A)_{\Delta})\to\mathcal{S}\mathrm{h}(\mathcal{FS}\mathrm{ch}\,/X).$$

Also there is a natural map of topoi $\mathcal{S}\mathrm{h}(\mathcal{FS}\mathrm{ch}\,/X)\to\mathcal{S}\mathrm{h}(X_{\acute{e}t})$ by restriction, by(5.9.7.1). So we get a morphism of topoi

$$\nu:\mathcal{S}\mathrm{h}((X/A)_{\Delta})\to\mathcal{S}\mathrm{h}(X_{\acute{e}t}).$$

In particular, for any étaleformal scheme U over X, by definition of ${}_s\mu$(6.1.2.11), for any sheaf $\mathcal{F}$,

$$(\nu_*\mathcal{F})(U/X)=H^0((U/A)_{\Delta},\mathcal{F}|_{(U/A)_{\Delta}}).$$

⌟

Cor. (8.9.4.7)[Prismatic Complex and Hodge-Tate Complex]. In the above situation, we define **prismatic complexes**

$$\Delta_{X/A}=R\nu_*\mathcal{O}_{\Delta}\in D(X_{\acute{e}t},A)$$

and the **Hodge-Tate complex**

$$\overline{\Delta}_{X/A}=R\nu_*\overline{\mathcal{O}}_{\Delta}\in D(X_{\acute{e}t},\mathcal{O}_X).$$

The Frobenius action on $\mathcal{O}_{\Delta}$ induces a φ-semi-linear map $\Delta_{X/A}\to\Delta_{X/A}$. And there is a relation

$$\overline{\Delta}_{X/A}\cong\Delta_{X/A}\otimes_A^L A/I\in D(X_{\acute{e}t},A/I)$$

by the Grothendieck spectral sequences associated to the diagram of functors:

$$\begin{array}{ccc} \mathcal{M}\mathrm{od}((X/A)_{\Delta}, \mathcal{O}_{\Delta}) & \xrightarrow{-\otimes_{\mathcal{O}_{\Delta}}\overline{\mathcal{O}}_{\Delta}} & \mathcal{M}\mathrm{od}((X/A)_{\Delta}, \overline{\mathcal{O}}_{\Delta}) \\ \downarrow{\scriptstyle \Gamma((X/A)_{\Delta},-)} & & \downarrow{\scriptstyle \Gamma((X/A)_{\Delta},-)} \\ \mathcal{M}\mathrm{od}(X_{\text{ét}}, A) & \longrightarrow & \mathcal{M}\mathrm{od}(X_{\text{ét}}, A/I) \end{array}$$

⌟

Affine Case

Def. (8.9.4.8) [Situation]. In this subsubsection, fix a bounded prism (A, I) and a p-completely smooth(5.9.7.1) A/I-algebra R (or equivalently the p-adic completion of an étale$A$-algebra, by(5.9.7.9) and(5.9.6.16), and they define the same site by the universal property of completion). ⌟

Prop. (8.9.4.9) [Prismatic Site over Affine Formal Scheme]. The **prismatic site** of R relative to A, denoted by $(R/A)_{\Delta}$ is the site whose objects are bounded prisms over (A, I) together with an A/I-algebra map $R \to B/IB$. And it is endowed with the indiscrete topology(6.1.1.2), so sheaves on this site is just presheaves.

There are two natural sheaves on this site, $\mathcal{O}_{\Delta}$ maps a prism (B, IB) to B which is valued in (p, I)-complete δ-A-algebras, and $\overline{\mathcal{O}}_{\Delta}$ which maps a prism (B, IB) to B/IB which is valued in p-complete R-algebras(5.9.6.16) ⌟

Prop. (8.9.4.10) [Compare with Indiscrete Topology]. If $(X/A)'_{\Delta} \subset (X/A)_{\Delta}$ is a continuous map of sites that the former is endowed with the indiscrete topology, then it is a morphism of sites, by(6.1.2.14), so this induces a morphism of topoi

$$\mathcal{S}\mathrm{h}((X/A)_{\Delta}) \to \mathcal{S}\mathrm{h}((X/A)'_{\Delta})$$

by(6.1.2.20), then we have the Leray spectral sequence(6.3.1.9)

$$E_2^{p,q} = H^p(\mathcal{C}', R^q f_*(\mathcal{F}^\bullet)) \Rightarrow H^{p+q}(\mathcal{C}, \mathcal{F}^\bullet).$$

and by(6.3.1.7)(6.3.1.6) and(8.9.1.12), we have a natural isomorphism

$$R\Gamma((X/A)'_{\Delta}, \mathcal{F}) \to R\Gamma((X/A)_{\Delta}, \mathcal{F})$$

for $\mathcal{F} = \mathcal{O}_{\Delta}$ or $\overline{\mathcal{O}}_{\Delta}$. ⌟

How to Compute the Prismatic Complex in the Affine Case

Lemma (8.9.4.11) [Weakly Final Object]. Let (A, I) be a prism and let R be a p-completely smooth A/I-algebra, then the category $(R/A)_{\Delta}$ admits a weakly final object. Moreover, we can choose it to be flat over (A, I). ⌟

Proof: Let F_0 be the derived (p, I)-completion of a free δ-ring over A on the set R, then there is a surjection of A-algebras $F_0 \to R$, with kernel J derived (p, I)-complete**?**. Then(8.9.1.13) applied to the δ-ring (F_0, J) gives a prism (F, IF) over (A, I), and by construction it is an object of $(R/A)_{\Delta}$. And it is weakly final because of the universal properties of F_0(5.5.4.10) and F(8.9.1.13).

For the flatness, we temporarily call a δ-pair (B, J) **good** if

- B is (p,I)-completely flat over A and J is (p,I)-complete.
- the prismatic envelope is flat over (A,I) and its formation commutes with completed derived base change on a (p,I)-completely flat map $B \to B'$.

Then we need to show that (F_0, J) is good. We have the following observations:

- Good pairs are stable under filtered colimit in the category of δ-pairs (B,J) that J is derived (p,I)-complete. (Because filtered colimits of flat modules are flat(5.4.1.6).)
- If (B,J) is a δ-pair over A with B completely (p,I)-flat over A, and $B \to B'$ is a (p,I)-completely f.f. map that $(B',(JB')^\wedge)$ is good, then (B,J) is good. (This follows from(8.9.1.13) and the f.f. descent(8.9.1.13).)

Then we can write B as a filtered colimit of (p,I)-complete algebras $B_s \twoheadrightarrow R$, and the kernel of each of them is locally generate by a (p,I)-completely regular sequence, so we can use the observations to pass to f.f. localization and filtered colimit to show that (B,J) is good. Cf.[Prism, Scholze, 3.14].**?**
□

Lemma (8.9.4.12) [Products]. The category $(R/A)_{\Delta}$ admits products. ⌟

Proof: For δ-rings $B, C \in (R/A)_{\Delta}$, we can take the δ-ring colimit $D_0 = B \otimes_A C$(5.5.4.13), but it may not be compatible with R-actions. Instead, let J be the kernel of the natural map

$$D_0 \to D_0/ID_0 \to B/IB \otimes_{A/IA} C/IC \to B/IB \otimes_R C/IC,$$

then (D_0, J) is a δ-ring over (A,I), and then we can use(8.9.1.13) to get a prism (D, ID) over (A,I), then the maps $R \to B/IB \to D_0/ID_0 \to D/ID$ and $R \to C/IC \to D_0/ID_0 \to D/ID$ are equal(because they all factor through D/J), thus giving a product object in $(R/A)_{\Delta}$. □

Prop. (8.9.4.13) [Čech-Alexander Construction for Prismatic Cohomology]. By(6.3.1.20)(8.9.4.10) and the lemmas(8.9.4.11)(8.9.4.12) above, the prismatic complex $\Delta_{R/A}$ is represented by the complex

$$F^0 \to F^1 \to F^2 \to \ldots.$$

In particular, $F^0 = F$ as constructed in(8.9.4.11) and each F^n are (p,I)-completely A-flat, I-torsion-free and (p,I)-complete δ-rings by(8.9.1.11) and(8.9.1.14).

Moreover, this complex is the prismatic envelope functor applied to the Čech nerve of $A \to F_0$, w.r.t. the Čech nerve $F^\bullet$ of ideals $J^\bullet = \ker(F^\bullet \to F_0 \to R)$, because prismatic envelope is a left adjoint hence commutes with tensor product of pairs(8.9.1.13). ⌟

Cor. (8.9.4.14). $\Delta_{R/A}$ is derived (p,I)-complete and $\overline{\Delta}_{R/A}$ is derived p-complete, because each term of the complex $F^\bullet$ is derived (p,I)-complete, so does its cohomology groups(5.9.6.8), thus so does $\Delta_{R/A}$ itself. Similarly for $\overline{\Delta}_{R/A}$, because each term of $F^\bullet/I$ is p-complete(8.9.4.13) hence derived p-complete, by(5.9.6.16). ⌟

5 Hodge-Tate Comparison

Def. (8.9.5.1) [Breuil-Kisin Twist]. Let I be an invertible ideal of A, then for any A/I-module M, we define the **Breuil-Kisin twist** of M as $M\{n\} = M \otimes (I/I^2)^n$. Notice this definable for $n \in \mathbb{Z}$ because I/I^2 is an invertible $\mathcal{O}_{A/I}$-module, by definition(8.9.1.1). Also it is definable in the level of $D(A/I)$, as $(I/I^2)^n$ is locally free thus flat. ⌟

Def. (8.9.5.2)[Completed de Rham Complex]. The **completed de Rham complex** is the derived p-completion of the de Rham complex of $\Omega_{X/(A/I)}$. We will use the derived p-completed de Rham complex in the sequel. It has a property that it coincides with the p-completion of its separate terms by(5.9.7.8) and (5.9.6.16) and the fact $\Omega_{X/(A/I)}$ is finite projective hence flat(5.4.5.12).

In fact, as $\Omega_{X/S}$ is finite locally free, the derived p-completion is just by tensoring $-\otimes_{R_0} R$, where R_0 is a smooth A-algebra that $R_0^\wedge = R$ by(5.9.7.9). In particular, the completed de Rham complex is compatible with base change and p-completely étaleextension, because the ordinary de Rham complex does(5.4.3.6)(5.4.7.6). ⌟

Prop. (8.9.5.3) [Hodge-Tate Comparison Theorem]. We have a structure map $\eta^0:\mathcal{O}_X\to H^0(\overline{\mathbb{\Delta}}_{X/A})$, and $H^\bullet(\overline{\mathbb{\Delta}}_{X/A})$ is a dga by(5.9.1.3) applied to $M^\bullet=\mathbb{\Delta}_{X/A}$and(5.9.2.1) noticing $\overline{\mathcal{O}}_{\mathbb{\Delta}}$ is a sheaf of algebras. then the universal property of de Rham complex(8.2.1.4) and lemma(8.9.5.4) shows η^0 extends to a map

$$\eta_R^\bullet:\Omega^\bullet_{X/(A/I)}\to H^\bullet(\overline{\mathbb{\Delta}}_{X/A})\{\bullet\}$$

of sheaves of A/I-dgas on $X_{\text{ét}}$.

Then this is an isomorphism of differential graded A/I-algebra. In particular $\overline{\mathbb{\Delta}}_{X/A}\in D(X_{\text{ét}},A/I)$ is a perfect complex with $H^i(\overline{\mathbb{\Delta}}_{X/A})\cong\Omega^i_{X/(A/I)}\{-i\}$. ⌟

Proof: The proof of the isomorphism is given in(8.9.6.10). □

Lemma (8.9.5.4). For any local section $f\in\mathcal{O}_X(U)$, the differential $\beta_I(f)\in H^1(\overline{\mathbb{\Delta}}_{X/A})\{1\}(U)$ squares to 0. ⌟

Proof: This follows from(8.9.6.9) in the affine line case because $H^2(\overline{\mathbb{\Delta}}_{X/A})\{1\}(U)=0$, and for the general case, use the étalelocalization(8.9.6.2) and base change theorem(8.9.6.1), noticing that cup product survives through derived tensor product. □

Cor. (8.9.5.5)[Base Change]. The formation of $\mathbb{\Delta}_{X/A}\in D(X_{\text{ét}},A)$ commutes with base change along a bounded prism $(A,IA)\to(B,IB)$: Let $g:X_B=X\otimes_{\mathrm{Spf}\,A/IA}\mathrm{Spf}\,B/IB\to X$ be the projection, then

$$(g^*\mathbb{\Delta}_{X/A})^\wedge\cong\mathbb{\Delta}_{X_B/B},\quad (g^*\overline{\mathbb{\Delta}}_{X/A})^\wedge\cong\overline{\mathbb{\Delta}}_{X_B/B}$$

where $()^\wedge$ is the derived (p,I)-completion or p-completion. ⌟

Proof: Because both side are derived (p,I)-complete, we take their cylinder object and by derived Nakayama w.r.t. $B/(p,I)$(5.9.6.10) it suffices to show the second, which is true because this is true for completed de Rham complexes(8.9.5.2). □

6 Proof of Hodge-Tate Comparison

The strategy is as follows: we study the affine case to construct and prove the Hodge-Tate comparison isomorphism in the affine case, and then this gives the construction of Hodge-Tate map in the general case, then we can also prove the general Hodge-Tate comparison by localizing at affine subschemes, so the affine case is important.

To prove the Hodge-Tate comparison isomorphism in the affine case, we use étalelocalization to reduce to the polynomial case, and then use flat base change to reduce to the oriented case. Then we use a slick strategy to reduce to the crystalline case, and finally reduce to crystalline comparison.

Lemma (8.9.6.1) [Base Change]. Let R be a p-completely smooth A/I-algebra and $(A, I) \to (A', I')$ be a map of bounded prisms that $A \to A'$ has finite (p, I)-complete Tor amplitude(5.9.7.1). If $R' = R\widehat{\otimes}_A^L A'$ for the the base change, then the natural map induces an isomorphism

$$\mathbb{\Delta}_{R/A}\widehat{\otimes}_A^L A' \cong \mathbb{\Delta}_{R'/A'}, \quad \overline{\mathbb{\Delta}}_{R/A}\widehat{\otimes}_A^L A' \cong \overline{\mathbb{\Delta}}_{R'/A'}$$

⌟

Proof: We use the Čech nerve of a weakly final object (8.9.4.13) to compute the cohomology, then we notice the (p, I)-completed base change $-\widehat{\otimes}_A^L A'$ applied termwise to the Čech nerve of $A \to F^0$ is the Čech nerve of $A \to F^0\widehat{\otimes}_A A'$, which is weakly final in $(R'/A')_{\mathbb{\Delta}}$, by the universal property and the fact (p, I)-completed base change is a left adjoint.

Finally we use(5.9.7.8) to see that this termwise completed derived base change just represents $\mathbb{\Delta}_{R/A}\widehat{\otimes}_A^L A'$ because each term of the prismatic envelope F is (p, I)-completely flat over A and the completed derived base change of F^n is discrete by(8.9.4.13). □

Lemma (8.9.6.2) [Étale Localization]. Let $R \to S$ be a p-completely étalemap of p-completely smooth algebras, then the natural map

$$\overline{\mathbb{\Delta}}_{R/A}\widehat{\otimes}_R^L S \to \overline{\mathbb{\Delta}}_{S/A}$$

is an isomorphism. ⌟

Proof: Firstly the forgetful functor $(R/A)_{\mathbb{\Delta}} \to (S/A)_{\mathbb{\Delta}}$ has a right adjoint, described as follows: a prims $(B, IB) \in (B/S)_{\mathbb{\Delta}}$ induces a p-completely étalemorphism of (discrete)rings $B/IB \to B/IB\widehat{\otimes}_R^L S$ by(5.9.7.5), and by Elkik's algebrization(5.9.7.9), this is a derived p-completion of some étalemap $B/IB \to T_0$, and we can lift it to some étalemap $B \to S_0$ by Henselian pair property(5.9.6.12)(5.3.10.9), then we can also take the derived (p, I)-completion(discrete by(8.9.1.11)) S_B of S_0, then $S_B/IS_B \cong B/IB \otimes_R^L S$**?**. So we have the following base change diagram:

$$\begin{array}{ccccc} B & \longrightarrow & S_0 & \longrightarrow & S_B \\ \downarrow & & \downarrow & & \downarrow \\ B/IB & \longrightarrow & T_0 & \longrightarrow & B/IB\widehat{\otimes}_R^L S \end{array}$$

For the adjointness, it suffices for every prism (T, IT) with morphisms $B \to T, B/IB \otimes_R^L S \to T/IT$, we can lift to a map $S_B \to T$. But if we consider the p-completely étalemap $T \to T\widehat{\otimes}_B B_S$ and its base change, it suffices to find a section of this map, and this is by Henselian pair (T, IT)(5.3.10.6)(8.9.1.11)(5.3.10.9). Moreover, S_B has a δ-structure by(5.5.4.19) so it is clearly a prism, and the right adjoint F just takes $(T, IT) \to (S_B, IS_B)$.

This right adjoint preserves weakly final objects and products, and it is just the completed derived tensor $-\widehat{\otimes}_R^L S$ when modulo I by construction, so when combined with(5.9.7.8) we get the conclusion. □

Remark (8.9.6.3). Notice these two lemmas(8.9.6.1)(8.9.6.2) are consequences of Hodge-Tate comparison isomorphism, once we proved it! ⌟

Crystalline Comparison in Characteristic p

Prop. (8.9.6.4) [Crystalline Comparison in Characteristic p]. Let $(A,(p))$ be a crystalline prism and let $I \subset A$ be a pd-ideal with $p \in I$, in particular the Frobenius $A/p \to A/p$ factors through A/I by(5.6.0.3), inducing a map $\psi = \psi_I : A/I \to A/p$. Let R be a smooth A/I-algebra and let $R^{(1)} = R \otimes_{A/I,\psi} A/p$, then there is a canonical

$$\Delta_{R^{(1)}/A} \cong R\Gamma_{\text{crys}}(R/A)$$

of E_∞-A-algebras compatible with Frobenius action. ⌟

Proof: **?** □

Cor. (8.9.6.5). If we have a smooth R over A/p and let $\widetilde{R} = R \otimes_{A/p} A/I$, then $\widetilde{R}^{(1)} = \varphi_* R$, and we can apply this theorem to $\widetilde{R}$ to get a canonical isomorphism

$$\varphi^* \Delta_{R/A} \cong R\Gamma_{\text{crys}}(\widetilde{R}/A)$$

of E_∞-A-algebras compatible with Frobenius action. ⌟

Lemma (8.9.6.6) [Hodge-Tate Comparison for the Affine Line over $(\mathbb{Z}_p,(p))$]. If $(A,(p))$ is a p-torsionfree crystalline prism and $R = \mathbb{F}_p\langle X\rangle$, then the Hodge-Tate map constructed in(8.9.5.3) is an isomorphism. ⌟

Proof: WARNING: This proof will not use the construction of the Hodge-Tate map in degree> 1 and this lemma will be used in the proof of Hodge-Tate map in the general case, so there is no cycle in the reasoning.

The map

$$\Omega^\bullet_{R^{(1)}/(A/p)} \to H^*(R\Gamma_{\text{crys}}(R/A) \otimes^L_A A/p)\{*\} \cong H^*(\Delta_{R^{(1)}/A} \otimes^L_A A/I)\{*\} = H^*(\overline{\Delta}_{R^{(1)}/A})\{*\}$$

is an isomorphism by Cartier isomorphism**?**, where the middle is by prismatic-crystalline comparison(8.9.6.4).

It suffices to check this is the Hodge-Tate map for $R^{(1)}/(A/p)$. But the Hodge-Tate map is induces by the inclusion $\mathcal{O}_X \to H^0(\overline{\Delta}_{X/S})$. It is fairly easy to check the proof of(8.9.6.4) and(8.8.6.9) the composition is also the canonical one. Finally if we choose $\mathbb{F}_p\langle X\rangle = R = R^{(1)}$, then we get the desired Hodge-Tate isomorphism. □

Lemma (8.9.6.7) [Hodge-Tate Comparison for $(\mathbb{Z}_p,(p))$]. If $(A,(p))$ is a p-torsionfree crystalline prism and $R = \mathbb{F}_p[X_1,\ldots,X_n]$, then the Hodge-Tate map constructed in(8.9.5.3) is an isomorphism. ⌟

Proof: The proof is the same as that of(8.9.6.6), notice now we already have the Hodge-Tate Comparison map. □

Direct proof of the Hodge-Tate comparison for $(\mathbb{Z}_p,(p))$

The proof of(8.9.6.6) and(8.9.6.7) is sloppy because we somehow lose track of whether the composition morphism is the Hodge-Tate comparison map. As the situation is so explicit, we decided to give a direct proof.

Mix Characteristic Case

Prop. (8.9.6.8) [Comparing with the Characteristic p]. Let A be a universal oriented prism in any characteristic and $A \to B$ as in(8.9.1.5), let $\alpha : (A,(d)) \xrightarrow{\varphi} (A,(d)) \to (B,(p))$, then α is a map of prisms by(8.9.1.6), and:

1. α/p factors as $A/p \to A/(p,d) \xrightarrow{\varphi} A/(p,d^p) \to B/p = D_{A/p}((d))$ where the first map has finite Tor amplitude and the last two maps are f.f., thus α/p has finite Tor amplitude.
2. The functor $\widehat{\alpha^*} : D_{\mathrm{comp}}(A,(p,d)) \to D_{\mathrm{comp}}(B,(p))$ reflects isomorphisms.
3. For any p-completely smooth A/I-algebra R, let $R_B = R\widehat{\otimes}_A B$, then the map
$$\widehat{\alpha^*}\Delta_{R/A} \to \Delta_{R_B/B}$$
is an isomorphism.

⌟

Proof: 1: It factors because $d^p = p!\gamma_p(d) \in pB$, and $B/p = D_{A/p}((d))$ by(5.6.0.16), noticing $D_A((d)) = D_A((p,d))$. The first map is of finite Tor amplitude(5.9.7.1) because d is a nonzero-divisor in A/p by(8.9.1.4). φ is f.f. because it is a base change of $\varphi_{A/p}$ and the latter is f.f.(8.9.1.4). The last one is f.f. because it is a free summand as $D_{A/p}((d)) = A/p[X_1, X_2, \ldots]/(a^p, X_1^p, X_2^p, \ldots)$ by(5.6.0.20).

2: Because $D_{\mathrm{comp}}(A,I)$ is a weak Serre subcategory of $D(A)$(5.9.6.8), to show it reflects isomorphisms, by item1 and derived Nakayama applied to $-\otimes_B^L B/p$, it suffices to show if $X \in D_{\mathrm{comp}}(A,(p,d))$, if $X \otimes_A^L A/p \otimes_{A/p}^L A/(p,d) = 0$, then $X = 0$, but $X \otimes_A^L A/p \otimes_{A/p}^L A/(p,d) = X \otimes_A^L A/(p,d)$, and this follows from derived Nakayama again.

3: α has finite (p,d) Tor amplitude by(5.9.7.3) and(8.9.1.4), so 3 follows from(8.9.6.1). □

Final Proof

Prop. (8.9.6.9) [Hodge-Tate Comparison in the Affine Line Case]. In situation(8.9.4.8), If $R = A/I\langle X\rangle$, $\eta_R^0 : R \to H^0(\overline{\Delta}_{R/A})$ and the twisted morphisms $\eta_R^1\{-1\} : \Omega^1_{R/(A/I)}\{-1\} \to H^1(\overline{\Delta}_{R/A})$ defined by the universal property of $\Omega_{R/(A/I)}$ are isomorphisms, and $H^i(\overline{\Delta}_{R/A}) = 0$ for $i > 1$.

In particular, by étalelocalization of prismatic cohomology(8.9.6.2), lemma(8.9.5.4) holds for any p-completely smooth algebra R over A/I. But this doesn't say that higher cohomologies vanish for any R, this is because cup product can survive derived tensor but cohomology groups cannot. ⌟

Proof: In this case, $\Omega_{R/S}$ is topologically free over R, thus we can choose a map
$$\eta : R \oplus \Omega^1_{R/A}\{-1\}[-1] \to \overline{\Delta}_{R/A}$$
lifting $\eta_R^0 \oplus \eta_R^1\{-1\}$.

Firstly if $(A,I) = (\mathbb{Z}_p,(p))$, this case is done by(8.9.6.6).

Next, if $(A,(d))$ is oriented, then there is a map of prisms from the universal oriented prism(8.9.1.4) $A_0 \to A$, then we have a pushout diagram of simplicial commutative rings
$$\begin{array}{ccccc} & & A_0 & \longrightarrow & A \\ & & \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\beta} \\ \mathbb{Z}_p & \longrightarrow & D_0 & \longrightarrow & E = A\widehat{\otimes}^L_{A_0} D_0 \end{array}$$

and $(E,(p))$ is a simplicial prism.

Now the warning is what we have done so far can all be extended to the derived algebraic geometry setting, or at least to the "animated commutative algebra" setting!

We denote the composite of the lower row as γ, because $\widehat{\alpha^*}$ reflects isomorphisms, so does $\widehat{\beta^*}$, and we can show $\widehat{\beta^*}\overline{\Delta}_{R/A} \cong \widehat{\gamma^*}\overline{\Delta}_{\mathbb{F}_p\langle X\rangle/\mathbb{Z}_p}$, and identifies the Hodge-Tate map: This is because we are in the polynomial case, so we can make the construction of $\Delta_{R/A}$ clear: we just take the F^0 to be the derived (p,I)-completion of the free δ-rings $A\{X\}$ in the construction of weakly final object(8.9.4.11), then the resulting Čech-Alexander complex is free and compatible with base change in the complex level.

Also β has finite (p,d)-Tor amplitude because α has because (p,d) is regular in A_0(8.9.1.4), also γ has finite p-Tor amplitude because E is p-torsionfree by(8.9.1.11), and use(5.9.7.3). So we are reduced to the $(\mathbb{Z}_p,(p))$ case, which we have done.

Finally, for a general bounded prism (A,I), we can reduce to the oriented case by base change along the f.f. extension defined in(8.9.1.11), then we reduce to the orientable case by(8.9.6.1). □

Prop. (8.9.6.10) [Hodge-Tate Comparison Theorem in General]. The map

$$\eta_R^\bullet : \Omega^\bullet_{X/(A/I)} \to H^\bullet(\overline{\Delta}_{X/A})\{\bullet\}$$

constructed in(8.9.5.3) is an isomorphism of sheaves of A/I-dgas on $X_{\text{ét}}$. ⌟

Proof: Because we already have the Hodge-Tate comparison map, it suffices to prove the theorem for affine subscheme Spf R, and because both prismatic cohomology and de Rham complex are étale-local(8.9.6.2)(8.9.5.2), it suffices to prove for the polynomial case. In this case, $\widehat{\Omega}^i_{R/A}$ is topological free over R, then we can lift the Hodge-Tate map(8.9.5.3) to the level of chain complexes:

$$\eta : \otimes_{i=0}^n \Omega^i_{R/(A/I)}\{-i\}[-i] \to \overline{\Delta}_{R/A}.$$

And then the rest is the same as the proof of(8.9.6.9), where in the $(\mathbb{Z}_p,(p))$ case, we use(8.9.6.7) instead of(8.9.6.6). □

de Rham Comparisons

Prop. (8.9.6.11)[de Rham Comparison]. In situation(8.9.4.2), if $W(A/I)$ is p-torsionfree, then there is a natural isomorphism

$$\Delta_{X/A}\widehat{\otimes}^L_{A,\varphi}A/I \cong \Omega^\bullet_{X/(A/I)}$$

of commutative algebra objects in $D(A/I)$. ⌟

Proof: Cf.[Sholze, Prism, 6.4].

It suffices to construct locally a functorial isomorphism $\Delta_{R/A}\widehat{\otimes}^L_{A,\varphi}A/I \cong \Omega^*_{R/(A/I)}$ and then glue.

Let $A \to W(A/I)$ be the canonical map, and $\psi : A \xrightarrow{\varphi} A \to W(A/I)$, then it takes I into (p)**?**. But the map $\psi/p : A/I \to W(A/I)/p = A/I$ factors through $A/(p,I)$, thus R' also equals $R/p \otimes_{A/(p,I)} W(A/I)/p$, so there is a base change diagram:

$$\begin{array}{ccccc} R & \longrightarrow & R/p & \longrightarrow & R^{(1)} = R\otimes_{A/I,\psi} W(A/I)/p \\ \uparrow & & \uparrow & & \uparrow \\ A/I & \longrightarrow & A/(p,I) & \xrightarrow{\psi_{(p,[p])}} & W(A/I)/p = A/I \end{array}$$

Base change for prismatic cohomology(8.9.5.5) gives an isomorphism

$$\Delta_{R/A}\widehat{\otimes}^L_{A,\psi}W(A/I)\cong\Delta_{R'/W(A/I)}.$$

Note that $W(A/I)\to A/(p,I)$ is a pd-thickening with ideal $(p,[p])$**?**, so we can use crystalline comparison w.r.t. the crystalline prism $(W(A/I),(p))$**?** to show that

$$\Delta_{R^{(1)}/W(A/I)}\cong R\Gamma_{\mathrm{crys}}((R/p)/W(A/I)).$$

Then finally we use the crystalline de Rham comparison**?** to get the desired result. □

Remark (8.9.6.12). The technical condition $W(A/I)$ is p-torsionfree can be removed, by [Scholze, Prism, 15.4]. ⌟

7 Derived de Rham Cohomology

Def. (8.9.7.1) [Derived de Rham Cohomology]. For an $\mathbb{F}_p$-algebra k, the **derived de Rham cohomology** functor $dR_{-/k}:\mathcal{CA}\mathrm{lg}/k\to D(k)$ is the left derived functor of the functor $\mathcal{P}\mathrm{oly}_k\to D(k)$ given by $R\to\Omega^\bullet_{R/k}$ via(5.8.4.2). ⌟

Prop. (8.9.7.2) [Derived Cartier Isomorphism]. ⌟

Regular Semiperfect Rings

Def. (8.9.7.3) [Regular Semiperfect Rings]. Let k be a perfect ring, a **regular semiperfect ring** over k is an k-algebra of the form R/I where R is a perfect k-algebra and I is an ideal generated by a regular sequence. ⌟

Prop. (8.9.7.4). Let k be a perfect field and S be a regular semiperfect ring, then ⌟

8 Derived Prismatic Cohomology

Prop. (8.9.8.1) [Derived Hodge-Tate Comparison]. ⌟

9 q-de Rham Cohomology

Prop. (8.9.9.1) [Hodge-Tate isomorphism via q-de Rham Complex]. Cf.[Bhatt, Prism, 5.3.9.]. ⌟

10 Étale Comparison

Prop. (8.9.10.1) [Frobenius Fixed Points]. Fix an $\mathbb{F}_p$-algebra B with an element t, let $D(B[F])$ be the **derived category of Frobenius B-modules**: this is a category whose objects are (M,φ) where $M\in D(B)$ and φ is a morphism $M\to M\otimes^L_{B,\varphi}B$ in $D(B)$. And let $D_{\mathrm{comp}}(B[F])$ be the full subcategory spanned by pairs (M,φ) where $M\in D_{\mathrm{comp}}(B,(t))$(5.9.6.4).

Given $(M,\varphi)\in D_{\mathrm{comp}}(B[F])$, let $M^{\varphi=1}=R\operatorname{Hom}_{D(B[F])}((B,\varphi),(M,\varphi))\in D(F_p)$**?**, called the **Frobenius fixed pts** of M. ⌟

Prop. (8.9.10.2). Fix an $\mathbb{F}_p$-algebra B with an element t, then

- The functor $D_{\text{comp}}(B[F]) \to D(\mathcal{F}_p)$ given by $M \to M^{\varphi=1}$ and $M \mapsto (M[t^{-1}])^{\varphi=1}$ commute with colimits.
- For any $(M, \varphi) \in D_{\text{comp}}(B[F])$ and

$\lrcorner$

11 Almost Purity

8.10 Motives

Main references are [Sta]Chap45, [Ful98], [Kle94], [Mil12] and [Lectures on Pure Motives, Murre]. [Jannsen, Uwe Motivic sheaves and filtrations on Chow groups. Motives (Seattle, WA, 1991), 245–302, Proc. Sympos. Pure Math., 55, Part 1, Amer. Math. Soc., Providence, RI, 1994.], [Jannsen, Uwe Equivalence relations on algebraic cycles. The arithmetic and geometry of algebraic cycles (Banff, AB, 1998), 225 – 260, NATO Sci. Ser. C Math. Phys. Sci., 548, Kluwer Acad. Publ., Dordrecht, 2000], [Jannsen, Uwe Mixed motives and algebraic K-theory. With appendices by S. Bloch and C. Schoen. Lecture Notes in Mathematics, 1400. Springer-Verlag, Berlin, 1990. xiv+246 pp. ISBN: 3-540-52260-3].

Notation (8.10.0.1).
- Let $k \in \texttt{Field}$.

┘

1 Correspondences

Def. (8.10.1.1). The full subcategory of $\mathcal{S}\mathrm{ch}/k$ consisting of smooth projective schemes over k is denoted by $\mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$.

Any $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$ has a decomposition $X = \coprod_n X_n$ into clopen subschemes that X_n is equidimensional of dimension n by(8.1.2.28). Thus we can talk about Rings $\mathrm{CH}^*(X)$ and $GH^*(X)$(8.1.2.29).
┘

Def. (8.10.1.2) [Adequate Equivalent Relations of Cycles]. An **adequate equivalent relation** on cycles is an equivalence relation on $Z^*(X)$ for each $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$ s.t.
- it is compatible with gradings and additions.
- it is compatible with products: $Z \sim 0 \implies Z \times Y \sim 0$.
- it is compatible with intersections: $Z_1 \sim 0 \implies Z \cdot W = 0$.
- it is compatible with projections: If $Z \sim 0 \in Z^*(X \times Y) \implies (\mathrm{pr}_X)_*(Z) \sim 0$.
- it satisfies moving lemma: Given $Z, W_1, \ldots, W_\ell \in Z^*(X)$, there exists $Z' \sim Z$ s.t. Z' and W_i intersect properly for any i.

┘

Def. (8.10.1.3) [(Rational)Correspondences]. Let $X, Y \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$ the group of (rational)**correpondences** from X to Y of degree(codimension) $r \in \mathbb{Z}$ is defined to be

$$\mathrm{Corr}^r_{\mathrm{rat}}(X, Y) = \bigoplus_d \mathrm{CH}^{d+r}(X_d \times_k Y)_{\mathbb{Q}} \subset \mathrm{CH}^*(X \times Y)_{\mathbb{Q}}.$$

Similarly we can define the groups of **Grothendieck correspondences** $\mathrm{Corr}^r_{\mathrm{num}}(X, Y)$. ┘

Def. (8.10.1.4) [Compositions of Correspondences]. Let $X, Y, Z \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$, there is a **composition of correspondences** map

$$\mathrm{Corr}^s(Y, Z) \times \mathrm{Corr}^r(X, Y) \to \mathrm{Corr}^{r+s}(X, Z) : (c', c) \mapsto c' \circ c = \mathrm{pr}_{13*}(\mathrm{pr}_{23}^* c' \cdot \mathrm{pr}_{12}^* c').$$

Then composition of correspondences are $\mathbb{Q}$-linear and associative. ┘

Proof: Cf.[Sta]0FG0. □

Prop. (8.10.1.5) [Tensor Product of Correspondences]. Let $X, Y, X', Y' \in \mathcal{S}m\mathcal{P}roj/k$, there is a **tensor product of correspondences** map

$$\otimes : \mathrm{Corr}^r(X,Y) \times \mathrm{Corr}^s(X',Y') \to \mathrm{Corr}^{r+s}(X \times_k X', Y \times_k Y') : (c, c') \mapsto \mathrm{pr}_{13}^*(c) \cdot \mathrm{pr}_{24}^*(c').$$

which is $\mathbb{Q}$-linear and associative, and commutes with compositions in both coordinates. ⌟

Prop. (8.10.1.6). $\mathrm{Corr}^0(\mathbb{P}^1_k) = \mathrm{CH}^1(\mathbb{P}^1_k \times \mathbb{P}^1_k)_{\mathbb{Q}} \cong \mathbb{Q} \oplus \mathbb{Q}$, where a basis is given by $c_0 = [\{0\} \times \mathbb{P}^1]$ and $c_2 = [\mathbb{P}^1 \times \{0\}]$. And the diagonal $\Delta = c_0 + c_2$.

Also $c_0 \circ c_0 = c_0, c_2 \circ c_2 = c_2, c_0 \circ c_2 = 0 = c_2 \circ c_0$, so $\mathrm{Corr}^0(\mathbb{P}^1_k) \cong \mathbb{Q} \oplus \mathbb{Q}$ as a $\mathbb{Q}$-algebra. ⌟

Def. (8.10.1.7) [Push and Pull via Correspondences]. Let $c \in \mathrm{Corr}^r_{\mathrm{rat}}(X,Y)$, we can define the

- (Pullback): $\mathrm{CH}_k(Y) \to \mathrm{CH}_{k-r}(X) : \beta \mapsto c^*(\beta) = \mathrm{pr}_{1,*}(c \cdot \mathrm{pr}_2^* \beta)$.
- (Pushforward): $\mathrm{CH}^k(X) \to \mathrm{CH}^{k+r}(Y) : \alpha \mapsto c_*(\alpha) = \mathrm{pr}_{2,*}(c \cdot \mathrm{pr}_1^* \alpha)$.

by using stratification and (8.1.2.12)(8.1.2.9). ⌟

Prop. (8.10.1.8) [Correspondences and Chow Groups].

- There are canonical isomorphisms

$$\mathrm{CH}_{-r}(X)_{\mathbb{Q}} \cong \mathrm{Corr}^r_{\mathrm{rat}}(X, \mathrm{Spec}\, k)$$

s.t. pullbacks by correspondences correspond to compositions.

- There are canonical isomorphisms

$$\mathrm{CH}^r(X)_{\mathbb{Q}} \cong \mathrm{Corr}^r_{\mathrm{rat}}(\mathrm{Spec}\, k, X)$$

s.t. pushforwards by correspondences correspond to compositions.

⌟

Proof: Cf.[Sta]0FG0. □

Cor. (8.10.1.9). Pushforwards and pullbacks by correspondences commute with compositions, by(8.10.1.8) and(8.10.1.4). ⌟

Prop. (8.10.1.10) [Graphs]. Let $f : X \to Y \in \mathcal{S}m\mathcal{P}roj/k$, its transposed graph Γ_f^t defines a correspondence $[\Gamma_f^t] \in \mathrm{Corr}^0(Y,X)$. $[\Gamma_{\mathrm{id}_X}] \in \mathrm{Corr}^0(X,X)$ is denoted by $[\Delta_X]$. ⌟

Def. (8.10.1.11) [Transpose]. Let $X, Y \in \mathcal{S}m\mathcal{P}roj/k$ be equidimensional, then the isomorphism $X \times_k Y \cong Y \times_k X$ induces a **transpose isomorphism**

$$(-)^t : \mathrm{Corr}^r(X,Y) \to \mathrm{Corr}^{\dim X - \dim Y + r}(Y,X).$$

In particular, when $f : X \to Y \in \mathcal{S}m\mathcal{P}roj/k$ and X, Y are equidimensional, then $[\Gamma_f^t]^t = [\Gamma_f]$. ⌟

Prop. (8.10.1.12). Let $\alpha \in \mathrm{Corr}^*(X,Y), \beta \in \mathrm{Corr}^*(Y,Z)$, then

1. $(\beta \circ \alpha)^t = \alpha^t \circ \beta^t$.
2. If $\beta = [\Gamma_g^t]$, then $\beta \circ \alpha = (\mathrm{id}_X \times g)^! \alpha$.
3. If $\alpha = [\Gamma_f^t]$, then $\beta \circ \alpha = (f \times \mathrm{id}_Z)_* \beta$.
4. If $\alpha = [\Gamma_f^t], \beta = [\Gamma_g^t]$, then $\beta \circ \alpha = [\Gamma_{fg}^t]$.

5. $\Delta_Y \circ \alpha = \alpha, \quad \beta \circ \Delta_Y = \beta.$

⌟

Proof: 1: This follows from commutativity and naturality of intersection products.
2: By(8.1.4.6) and(8.1.8.9),

$$[\Gamma_g^t] \circ \alpha = \mathrm{pr}_{13*}(\mathrm{pr}_{23}^*[\Gamma_g^t] \cdot \mathrm{pr}_{12}^* \alpha) = \mathrm{pr}_{13*}(1,g,1)_*((1,g,1)^! \,\mathrm{pr}_{12}^! \alpha) = (1,g)^! \alpha.$$

3 is similar to item2.
4, 5 follow from item2, 3. □

Prop. (8.10.1.13) [Push and Pull by Graphs]. Let $f : X \to Y \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$, then

- Pushforward by $[\Gamma_f]^t$ agrees with the Gysin map $f^! : \mathrm{CH}^*(Y) \to \mathrm{CH}^*(X)$.
- Pullback by $[\Gamma_f]^t$ agrees with the pushforward $f_* : \mathrm{CH}_*(X) \to \mathrm{CH}_*(Y)$.

⌟

Proof: These follows from(8.10.1.8) and(8.10.1.12). □

Prop. (8.10.1.14). Let $f : Y \to X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$ where X, Y are equidimensional, then there are commutative diagram of correspondences

$$\begin{array}{ccccc}
X \times Y & \xrightarrow{[\Gamma_f^t]\otimes\Delta_Y} & Y \times Y & \xrightarrow{[\Gamma_{\Delta_Y}^t]} & Y \\
\big\downarrow{\scriptstyle \Delta_X \otimes [\Gamma_f]} & & & & \big\downarrow{\scriptstyle [Y]} \\
X \times X & \xrightarrow{[\Gamma_{\Delta_X}^t]} & X & \xrightarrow{[X]} & \mathrm{Spec}\, k
\end{array}$$

⌟

Proof: By(8.10.1.12), it suffices to show that $(\mathrm{id}_X \times f)^!(\Delta_X)_*[X] = (f \times \mathrm{id}_Y)_*(\Delta_Y)_*[Y]$. But both sides equal $[\Gamma_f^t]$. ($(\mathrm{id}_X \times f)^![\Delta_X] = [\Gamma_f^t]$ follows from [Sta]0FF7**?**). □

Prop. (8.10.1.15) [Virtual Number of Coincidences]. Let $X, Y \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k, \alpha, \beta \in \mathrm{Corr}^*(X, Y)$, then

$$\mathrm{pr}_{1*}(\alpha \cdot \beta) = (\beta^t \circ \alpha) \cdot \Delta_X = (\alpha^t \circ \beta) \cdot \Delta_X.$$

In particular, if X, Y are equidimensional of dimension n, and $\alpha, \beta \in \mathrm{Corr}^0(X, Y)$, then the **virtual number of coincidence** of α and β, defined as $\int_{X\times Y} \alpha \cdot \beta$, equals the virtual number of fixed points of $\beta^t \circ \alpha$. ⌟

Proof: Cf.[Ful98]P309. □

Def. (8.10.1.16) [Degenerate Correspondences]. Let $X, Y \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$, then the subgroup of **degenerate correspondences** from X to Y is the subgroup of $\mathrm{Corr}^*(X, Y)$ generated by exterior products $\mathrm{CH}^*(X) \times \mathrm{CH}^*(Y)$(8.1.8.3). The subgroup of degenerate correspondences from X to Y is denoted by $I(X, Y)$.

Then $I(X, X)$ is a two-sided ideal in $\mathrm{Corr}^*(X, X)$, and is stable under transpose if X are equidimensional. ⌟

Def. (8.10.1.17) [Valence]. Let $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}^n/k$, then $\alpha \in \mathrm{Corr}^0(X, X)$ is said to be of **valence** ν iff $\alpha + \nu[\Delta_X] \in I(X, X)$. ⌟

Def. (8.10.1.18) [Degree of Correspondences]. Let $X, Y, Z \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}^n/k$ be irreducible, then for $\alpha \in \mathrm{Corr}^n(X, Y)$, the **degrees of** α is defined to

$$\alpha_*[X] = \mathrm{pr}_{2*}(\alpha) = d_2(\alpha)[Y], \quad \alpha^*[Y] = \mathrm{pr}_{1*}(\alpha) = d_1(\alpha)[X].$$

Then

- Let $\beta \in \mathrm{Corr}^n(Y, Z)$, then $d_i(\beta \circ \alpha) = d_i(\alpha)d_i(\beta)$.
- If $P \subset X$ is a rational point, then $d_1(\alpha) = \int_{X\times Y} \alpha \cdot [P \times Y]$.

⌟

Proof: 1 is clear. 2 follows by composing with the correspondence $[\Gamma_P] \in \mathrm{Corr}^{-n}(P, X)$. □

2 Weil Cohomology Theories

Pre-Weil Cohomology Theories

Prop. (8.10.2.1) [Non-Existence of a $\mathbb{Q}$-Cohomology Theory]. For any $p \in \mathbf{P} \cup \{0\}$, there exists an alg.closed field of characteristic p s.t. there doesn't exists a cohomology theory on the category of smooth projective varieties over k with coefficients in $\mathbb{Q}$ that specializes to the étale cohomology with $\mathbb{Q}_\ell$ coefficients, where $\ell \in \mathbf{P} \cap \{\mathbf{p}\}$. ⌟

Proof: For $p = 0$, take $k = \mathbb{C}$. For a smooth projective variety X over k, it is defined over a subfield k_0 finite over $\mathbb{Q}$. Let $\Gamma = \mathrm{Gal}(k/k_0)$, then Γ acts on $H^*(X, \mathbb{Q}_\ell)$. If $H^*(X, \mathbb{Q}_\ell)$ is specialized from a $\mathbb{Q}$-cohomology $\widetilde{H}^*(-, \mathbb{Q})$, then the continuous Γ-action on $H^*_{\text{ét}}(X, \mathbb{Q}_\ell)$ stablizes $\widetilde{H}^*(X, \mathbb{Q})$. But it is known that

$$H^*_{\text{ét}}(X, \mathbb{Q}_\ell) \cong H^*_{\text{Betti}}(X, \mathbb{Q}) \oplus \mathbb{Q}_\ell,$$

so $\dim_{\mathbb{Q}} \widetilde{H}^*(X, \mathbb{Q}) = \dim H^*_{\text{Betti}}(X, \mathbb{Q}) < \infty$. Then because infinite Galois group is uncountable, Γ acts $\widetilde{H}^*(X, \mathbb{Q})$ through a finite quotient. But this is not true in general.? In fact, This contradicts Tate's conjecture.

If $p > 0$, let $k = \overline{F}_p$ and E be an supersingular elliptic curve over $\overline{k}$, which exists by(15.11.3.12), then $\mathrm{End}(E) \otimes \mathbb{Q}$ is a definite quaternion algebra Q over $\mathbb{Q}$, and $\dim_{\mathbb{Q}_\ell} H^1_{\text{ét}}(E, \mathbb{Q}_\ell) = 2$(15.7.6.15), so if $H^*(X, \mathbb{Q}_\ell)$ is specialized from a $\mathbb{Q}$-cohomology $\widetilde{H}^*(-, \mathbb{Q})$, $\dim_{\mathbb{Q}} \widetilde{H}^1(E, \mathbb{Q}) = 2$, and $\mathrm{End}(E) \otimes \mathbb{Q}$ acts on it. But there is no ring homomorphism $Q \to M_2(\mathbb{Q})$. □

Def. (8.10.2.2) [Weil Cohomology Theories]. Let $k, F \in$ `Field`, $\mathrm{char}\, F = 0$, then a **pre-Weil cohomology theory** over k with coefficients in F is given by a tuple $(F(1), H^*, \gamma, \mathrm{tr})$, where

- $F(1)$ is a 1-dimensional vector space over F. And denote $F(n) = F(1)^{\otimes n}$, $F(-n) = F(n)^*$, and for any $V \in \mathcal{V}\mathrm{ect}_F$, define $V(n) = V \otimes F(n)$.
- H^* is a functor $H^* : \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k \to \mathcal{C}\mathcal{R}\mathrm{ing}^{\mathrm{gr}}/F$. $H^*(X)$ is called the **cohomology ring of** X, and its multiplication is denoted by $\cup$.
- For every $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$ and $i \in \mathbb{N}$, γ_X is a homomorphism $\gamma_X : \mathrm{CH}^i(X) \to H^{2i}(X)(i)$, called the **cycle class maps** of X.
- For any $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}^d/k$, tr_X is a map $\mathrm{tr}_X : H^{2d}(X)(d) \to F$, called the **trace map** of X. The trace map is sometimes also denoted by $\int_X$.

that satisfy the following properties:

Poincaré duality: For any $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}^d/k$,

1. $\dim_F H^i(X) < \infty$ for any i and $H^i(X) = 0$ unless $0 \le i \le 2n$.

2. $H^i(X)\otimes_F H^{2d-i}(X)(d)\xrightarrow{\cup} H^{2d}(X)(d)\xrightarrow{\mathrm{tr}_X} F$ is a perfect pairing.

Künneth formula: For any $X, y\in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$,

$$H^*(X)\otimes_F H^*(Y)\to H^*(X\times_k Y):(a,b)\mapsto \mathrm{pr}_1^* a\cup \mathrm{pr}_2^* b$$

is an isomorphism in $\mathcal{CR}\mathrm{ing}^{\mathrm{gr}}/F$.

Cycle class map is natural:

1. For any $f:X\to Y\in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$, $\gamma(f^!\beta)=f^*\gamma(\beta)$ for $\beta\in H^*(Y)$ and $\gamma(f_*\alpha)=f_*\gamma(\alpha)$ for $\alpha\in H^*(X)$.
2. $\gamma(a\cdot b)=\gamma(a)\cup\gamma(b)$.
3. $\int_{\mathrm{Spec}\,k}\gamma(\mathrm{Spec}\,k)=1$.

H^* is called a **Weil cohomology theory** if moreover it satisfies:

- For $X\in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$ and $\Gamma(X,\mathcal{O}_X)=k'$, then the natural map $H^0(\mathrm{Spec}\,k')\to H^0(X)$ is an isomorphism.

⌟

Prop. (8.10.2.3) [Pushforward]. Let $k, F\in$ `Field` and H^* be a pre-Weil cohomology theory, for $f:X\to Y\in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$ where $\dim X=d, \dim Y=e$, we can define a **pushforward map of cohomology** $H^{2d-*}(X)(d)\to H^{2e-*}(Y)(e)$ via Poincaré duality, i.e.

$$\int_X f^*b\cup a=\int_Y b\cup f_*a$$

for any $a\in H^{2d-i}(X)(d), b\in H^i(Y)$. Then

- $f_*(f^*b\cup a)=b\cup f_*a$.
- $g_*f_*=(gf)_*$.

⌟

Proof: Use duality and the corresponding properties of f^*. □

Prop. (8.10.2.4) [$H^*(\mathrm{Spec}\,k)$]. Let $k,F\in$ `Field` and H^* be a pre-Weil cohomology, then $H^i(\mathrm{Spec}\,k)=0$ unless $i=0$, and there is a unique F-algebra isomorphism $H^0(\mathrm{Spec}\,k)\cong F$, sending $\gamma([\mathrm{Spec}\,k])$ to 1 and $\mathrm{tr}_{\mathrm{Spec}\,k}$ is identity under this identification. ⌟

Proof: Cf.[Sta]0FHE. □

Prop. (8.10.2.5) [Coproducts]. Let $k,F\in$ `Field` and H^* be a pre-Weil cohomology, then for $X,Y\in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$, $H^*(X\coprod Y)\to H^*(X)\times H^*(Y)$ is an isomorphism. ⌟

Proof: Cf.[Sta]0FHJ. □

Weil Cohomology Theories

Prop. (8.10.2.6) [Characterizing Weil Cohomology Theories]. Let $k,F\in$ `Field` and H^* be a pre-Weil cohomology theory, for $X\in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$ and $\Gamma(X,\mathcal{O}_X)=k'$, the following are equivalent:

- There exists f.m. geometric points $x_1,\ldots,x_r\in X$ s.t. $H^0(X)\to H^0(x_1)\oplus\ldots H^0(x_r)$ is injective.
- The map $H^0(\mathrm{Spec}\,k')\to H^0(X)$ is an isomorphism.

If these hold, then $H^0(X)$ is finite étale over F. Moreover, if X is equidimensional of dimension d, then these are further equivalent to

- The classes of closed points of X generate $H^{2d}(X)(d)$ as a module over $H^0(X)$.

⌟

Prop. (8.10.2.7) [Non-negativeness]. Let $k, F \in \texttt{Field}$ and H^* be a Weil cohomology theory, then for any $Y \in \mathcal{S}m\mathcal{P}roj/k$, $H^i(Y) = 0$ for $i < 0$. ⌟

Proof: If $H^i(Y) \neq 0$ for some $Y \in \mathcal{S}m\mathcal{P}roj/k$ and $i < 0$, we may assume Y is irreducible by(8.10.2.5), and also we may assume $i = -2j$ is even by changing Y to $Y \times Y$ using Künneth formula. Then take $X = Y \times (\mathbb{P}^1_k)^j$, then Künneth formula shows

$$H^0(Y) \oplus H^i(Y) \otimes H^2(\mathbb{P}^1_k)^{\otimes l} \subset H^0(X),$$

so $H^0(X)$ cannot be isomorphic to $H^0(\operatorname{Spec}\Gamma(X, \mathcal{O}_X)) = H^0(\operatorname{Spec}\Gamma(Y, \mathcal{O}_Y)) \cong H^0(Y)$. □

Prop. (8.10.2.8). ? Let $k, F \in \texttt{Field}$ and H^* be a Weil cohomology theory, then

- If $X \in \mathcal{S}m\mathcal{P}roj^d/k$, then $\operatorname{tr}_X \circ \gamma = \deg : \operatorname{CH}^d(X) \to F$(8.1.2.27).
- If $X, Y \in \mathcal{S}m\mathcal{P}roj/k$, then $\operatorname{tr}_{X \times_k Y} = \operatorname{tr}_X \otimes \operatorname{tr}_Y$ via Künneth formula(8.10.2.2). In particular, for $a \in H^{2\dim X}(X)(\dim X), b \in H^*(\dim Y)$, $\operatorname{pr}_{2,*}(a \otimes b) = (\int_X a)b \in H^*(Y)$.

⌟

Proof: 1: This holds for $X = \operatorname{Spec} k$ by hypothesis, and also for any other $x \in X(k)$ by pushforward.

2: For any $x \in X(k), y \in Y(k)$, by item1, $\gamma([x \times y]) \in H^{\mathrm{top}}(X \times Y)$ is mapped to $1 \in F$ via $\operatorname{tr}_{X \times Y}$, and it equals $\gamma([x]) \otimes \gamma([y])$ by(8.10.2.2) as $[a \times b] = \operatorname{pr}_1^!(a) \cdot \operatorname{pr}_2^!(b)$. The latter is also mapped to $1 \in F$ by $\operatorname{tr}_X \otimes \operatorname{tr}_Y$.

For the last assertion, notice $\int_Y \operatorname{pr}_{2,*}(a \otimes b) \cup c = \int_{X \times Y}(a \otimes b) \cup (1 \otimes c) = (\int_X a) \int_Y (b \cup c)$ □

Prop. (8.10.2.9). If $Z \in \operatorname{CH}^*(X)$ satisfies mZ is algebraically trivial for some $m \in \mathbb{Z}^*$, then $\gamma_X(Z) = 0$. ⌟

Proof: Cf.[Algebraic Cycles and the Weil Conjecture, Kleiman, Prop1.2.1]. □

Prop. (8.10.2.10) [Lefschetz Trace Formula]. Let $k, F \in \texttt{Field}$ and H^* be a Weil cohomology theory, then for $X \in \mathcal{S}m\mathcal{P}roj/k$ and $\alpha, \beta \in H^{2*}(X \times X)(*)$, then

$$(\alpha \cdot \beta) = \sum_i (-1)^i \operatorname{tr}(\beta \circ \alpha | H^i(X)).$$

⌟

Proof: Cf.[Sta]0FH0.? □

Cor. (8.10.2.11). Let $k, F \in \texttt{Field}$ and H^* be a Weil cohomology theory, then for $X \in \mathcal{S}m\mathcal{P}roj/k$,

$$\sum_{i=0}^{2\dim X} (-1)^i \dim_F H^i(X) = \deg([\Delta_X] \cdot [\Delta_X]) = \deg(c_d(\mathcal{T}_X) \cap [X]).$$

⌟

Conj. (8.10.2.12) [Betti Numbers]. Let $k, F \in \texttt{Field}, k = \overline{k}$ and H^* be a Weil cohomology theory, is it true that for a smooth projective variety over k, the numbers $\beta_i = \dim_F H^i(X)$ are independent of F and the cohomology theory? ⌟

Proof: ? □

3 Pure Motives

Conj. (8.10.3.1) [Category of Motives as a Universal Cohomology Theory]. Let $k \in \texttt{Field}$, then there should be a category of motives $\mathrm{Mot}(k)$ s.t.

- $\mathrm{Mot}(k)$ is a Tannakian category over $\mathbb{Q}$.
- There is a functor $h : \mathcal{S}m\mathcal{P}\mathrm{roj}/k \to \mathrm{Mot}(k)$.
- Every correspondence $X \to Y$ of degree 0 defines a map $hX \to hY$.
- Every Weil cohomology theory(8.10.2.2) on the $\mathcal{S}m\mathcal{P}\mathrm{roj}/k$ factors uniquely through h.

⌟

Proof: ? □

Def. (8.10.3.2) [Chow Motives]. The category $\mathrm{Mot}_{\mathrm{rat}}(k)$ of **Chow motives** over k consist of triples (X, e, m) where $X \in \mathcal{S}m\mathcal{P}\mathrm{roj}/k$, e is an idempotent in $\mathrm{Corr}^0_{\mathrm{rat}}(X, X)_{\mathbb{Q}}$ and $m \in \mathbb{Z}$. And morphisms in $M_{\mathrm{rat}}(k)$ are defined to be

$$\mathrm{Hom}((X, e, m), (Y, f, n)) = f \circ \mathrm{Corr}^{n-m}_{\mathrm{rat}}(X, Y) \circ e.$$

The category $\mathrm{Mot}^{\mathrm{eff}}_{\mathrm{rat}}(k)$ of **effective Chow motives** over k is defined to be the full subcategory of $\mathrm{Mot}_{\mathrm{rat}}(k)$ consisting of triples $(X, e, 0)$.

There is a contravariant functor $\mathcal{S}m\mathcal{P}\mathrm{roj}/k \to \mathrm{Mot}^{\mathrm{eff}}_{\mathrm{rat}}(k) : X \mapsto (X, [\Delta_X], 0)$ and $f \mapsto [\Gamma^t_f]$. ⌟

Def. (8.10.3.3) [Grothendieck Motives]. The category $\mathrm{Mot}_{\mathrm{num}}(k)$ of **Grothendieck motives** over k consist of triples (X, e, m) where $X \in \mathcal{S}m\mathcal{P}\mathrm{roj}/k$, e is an idempotent in $\mathrm{Corr}^0_{\mathrm{num}}(X, X)_{\mathbb{Q}}$ and $m \in \mathbb{Z}$. And morphisms in $M_{\mathrm{num}}(k)$ are defined to be

$$\mathrm{Hom}((X, e, m), (Y, f, n)) = f \circ \mathrm{Corr}^{n-m}_{\mathrm{num}}(X, Y) \circ e.$$

The category $\mathrm{Mot}^{\mathrm{eff}}_{\mathrm{num}}(k)$ of **effective Grothendieck motives** over k is defined to be the full subcategory of $\mathrm{Mot}_{\mathrm{num}}(k)$ consisting of triples $(X, e, 0)$. ⌟

Prop. (8.10.3.4). There are natural functors $\mathrm{Mot}^{\mathrm{eff}}_{\mathrm{rat}}(k) \to \mathrm{Mot}^{\mathrm{eff}}_{\mathrm{num}}(k)$ and $\mathrm{Mot}_{\mathrm{rat}}(k) \to \mathrm{Mot}_{\mathrm{num}}(k)$, by definition(8.10.1.3). ⌟

Def. (8.10.3.5) [Tate Twists]. In $M_{\mathrm{rat}}(k)$ or $M_{\mathrm{num}}(k)$, define $\mathbb{1}(n) = (\mathrm{Spec}\, k, \mathrm{id}, n)$, and for any object M, define $M(n) = M \otimes \mathbb{1}(n)$. ⌟

Prop. (8.10.3.6). $M_{\mathrm{rat}}(k)$ and $M_{\mathrm{num}}(k)$ are Karoubian categories(4.8.1.15) and symmetric monoidal categories with identity $\mathbb{1}(0)$(8.10.3.5). ⌟

Proof: The symmetric monoidal structure is given by(8.10.1.4). It is clearly an additive category. To show it is Karoubian, for $M = (X, e, m) \in M_{\mathrm{rat}}(k), p \in \mathrm{End}(M)$ be an idempotent, then $p = epe$, and $N = (X, p, m) \in M_{\mathrm{rat}}(k)$, and $p : N \to M$ is a morphism. □

Prop. (8.10.3.7). $h(\mathbb{P}^1_k) = \mathbb{1} \oplus \mathbb{1}(-1) \in M_{\mathrm{rat}}(k)$. ⌟

Proof: Cf.[Sta]0FGG. □

Prop. (8.10.3.8) [$\mathrm{Mot}_{\mathrm{rat}}(k)$ as Inverting c_2]. For any $\mathbb{Q}$-Karoubian category $\mathcal{C}$ and a symmetric monoidal functor $f : M^{\mathrm{eff}}_{\mathrm{rat}}(k) \to \mathcal{C}$ s.t. $f(c_2) \in f(\mathbb{P}^1_k)$ is an invertible object, f factors through uniquely through a symmetric monoidal functor $M_{\mathrm{rat}}(k) \to \mathcal{C}$. ⌟

Proof: Cf.[Sta]0FGH. □

Prop. (8.10.3.9)[Left Duals]. Let $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}^d/k$, then $h(X)(d)$ is a left dual of $h(X)$. In particular, every element in $M_{\mathrm{rat}}(k)$ has a left dual. ⌟

Proof: Cf.[Sta]0FGI, 0FGJ.? □

Def. (8.10.3.10) [Chow Groups of Motives]. Let $k \in \texttt{Field}$ and $M = (X, e, m) \in M_{\mathrm{rat}}(k)$, the i-th **Chow group** of M is defined to be

$$\mathrm{CH}^i(M) = e \circ \mathrm{CH}^{i+m}(X)_{\mathbb{Q}} = \mathrm{Hom}(\mathbb{1}(-i), M).$$

Then each CH^i defines a functor $M_{\mathrm{rat}}(k) \to \mathcal{V}\mathrm{ect}_{\mathbb{Q}}$ via pushforwards?. ⌟

Prop. (8.10.3.11) [Manin]. Let $k \in \texttt{Field}$ and $M \in M_{\mathrm{rat}}(k)$. If $c : M \to N \in \mathrm{Mot}_{\mathrm{rat}}(k)$ satisfies that for $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$, the map $c \otimes 1 : M \otimes h(X) \to N \otimes h(X)$ induces isomorphisms on Chow groups, then c is an isomorphism. ⌟

Proof: Cf.[Sta]0FGN.? □

Prop. (8.10.3.12) [Weil Cohomologies and Chow Motives]. Let $k, F \in \texttt{Field}$, $k = \overline{k}$, $\mathrm{char}\, F = 0$, then a classical Weil cohomology over k with coefficients in F is equivalent to a $\mathbb{Q}$-linear monoidal functor $G : \mathrm{Mat}_{\mathrm{rat}}(k) \to \mathcal{CR}\mathrm{ing}^{\mathrm{gr}}/F$ together with an isomorphism $F[2] \to G(\mathbb{1}(1))$ s.t.

- $G(h(X)) \subset \mathcal{CR}\mathrm{ing}^{\mathrm{gr}\geq 0}/F$.
- $\dim_F G^0(h(X)) = 1$.

⌟

Proof: Cf.[Sta]0FH3. □

Theorems

Thm. (8.10.3.13) [Voisin-Voevodsky]. For $k \in \texttt{Field}$ and $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$, $Z^i_{\mathrm{alg}}(X)_{\mathbb{Q}} \subset Z^i_{\times}(X)_{\mathbb{Q}}$. ⌟

Proof: Cf.[Lectures on Pure Motives, Murre]P19. □

Thm. (8.10.3.14) [Jannsen]. For $k \in \texttt{Field}, k = \overline{k}$, let $\sim$ be an adequate equivalence relation(8.10.1.2), and $F \in \texttt{Field}^0$, then the following are equivalent:

- $\mathrm{Mot}_\sim$ is an Abelian semisimple category.
- $\sim$ is the numerical equivalence relation.
- For all $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$, $\mathrm{Corr}^0_\sim(X, X)_F$ is a f.d. semisimple F-algebras.

⌟

Proof: Cf.[Lectures on Pure Motives, Murre]P39 or [Jan92]. □

Realizations

Cor. (8.10.3.15) [Realization Functors]. For $k \in \texttt{Field}$, suppose the category of motives exists(8.10.3.1), then there should be **realization functors**

- $\mathrm{Real}_p : \mathrm{Mot}(k) \to \mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_k)$ s.t. $H^i(-, \mathbb{Q}_p) = \mathrm{Real}_p \circ h^i$,
- $\mathrm{Real}_{\iota,\mathrm{Betti}} : \mathrm{Mot}(k) \to \mathrm{Hdg}_{\mathrm{int}}$ s.t. $H^i_{\iota,\mathrm{Betti}}(-, \mathbb{Z})_{\mathrm{lf}} = \mathrm{Real}_\iota \circ h^i$, for each embedding $\iota : k \to \mathbb{C}$.

- $\mathrm{Real}_{\mathrm{dR}} : \mathrm{Mot}(k) \to \mathrm{Fil}_K$ s.t. $H^i_{\mathrm{dR}}(-) = \mathrm{Real}_{\mathrm{dR}} \circ h^i$.

And comparison isomorphisms

$$I_\ell : \mathrm{Real}_\iota \otimes \mathbb{Q}_\ell \cong \mathrm{Real}_\ell : \mathrm{Mot}(k) \to \mathcal{V}\mathrm{ect}\,/\mathbb{Q}_\ell$$

$$I_{\mathrm{dR}} : \mathrm{Real}_{\iota,\mathrm{Betti}} \otimes \mathbb{C} \cong \mathrm{Real}_{\mathrm{dR}} \otimes_{k,\iota} \mathbb{C} : \mathrm{Mot}(k) \to \mathrm{Fil}^\bullet_{\mathbb{C}}$$

and the Tate twist(8.10.3.5) acts on the relations via

- $\mathrm{Real}_{\iota,\mathrm{Betti}}(M(r)) = (\Lambda, \Lambda^{p,q}_{\mathbb{C}})$ is given as follows:

$$\Lambda = (2\pi\,\mathrm{i})^r\,\mathrm{Real}_{\iota,\mathrm{Betti}}(M), \quad \Lambda^{p,q}_{\mathbb{C}} = (2\pi\,\mathrm{i})^r\,\mathrm{Real}_{\iota,\mathrm{Betti}}(M)^{p-r,q-r}.$$

- $\mathrm{Real}_p(M(r)) = \mathrm{Real}_p(M)(r) = \mathrm{Real}_p(M) \otimes \mu_{p^\infty}^{\otimes r}$.
- $\mathrm{Real}_{\mathrm{dR}}(M(n)) = \mathrm{Real}_{\mathrm{dR}}(M)$.

⌟

Proof: It suffices to show that these are all Wei cohomology theories,? □

Prop. (8.10.3.16). By(12.10.3.7), if $\iota : k \to \mathbb{C}$ factors through $\mathbb{R}$, then

$$I_{\mathrm{dR}} : \mathrm{Real}_{\iota,\mathrm{Betti}} \otimes \mathbb{C} \cong \mathrm{Real}_{\mathrm{dR}} \otimes_{k,\iota} \mathbb{C}$$

identifies $\mathtt{c}^* \otimes \mathtt{c}$ on the LHS with $\mathtt{c}$ on the RHS. ⌟

Prop. (8.10.3.17) [Tate Conjecture and Motives]. The Tate conjecture(15.15.1.2) and Grothendieck-Serre conjecture(8.4.7.39) hold iff the functor $\mathrm{Mot}(k) \to \mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_K) : M \mapsto \mathrm{H}^*_{\mathrm{\acute{e}t}}(M)$ is fully faithful. ⌟

Proof: ? □

Prop. (8.10.3.18). For $k \in \mathtt{Field}$, the functor $\mathrm{Mot}(k) \to \mathrm{Hdg}(M)$ is fully faithful iff the Hodge conjecture holds for k. ⌟

Proof: Cf.[Hodge-de Rham Structure and Periods of Automorphic Forms, Michael Harries, in Motives 2]Prop1.2.? □

Chow-Künneth Decompositions

Def. (8.10.3.19) [Chow-Künneth Decompositions]. For $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}^d/k$, a **Chow-Künneth decomposition** is a decomposition

$$\Delta_X = \sum_{i=0}^{2d} \pi_i \in \mathrm{CH}^d(X \times X, \mathbb{Q})$$

s.t.

- $\pi_j \pi_i = \delta_{i,j}\pi_i$.
- For any Weil cohomology over $\overline{k}$, π_i is mapped to the usual Künneth component $\Delta(2d-i,i)$?.

⌟

4 Mixed Motives

Remark (8.10.4.1). The motives are conjectured to be the subcategory of semisimple objects in a larger category of **mixed motives**.

There is at present no definition of a category of mixed motives, but several mathematicians have constructed triangulated categories that are candidates to be its derived category; it remains to define a T-structure on one of these categories whose heart is the category of mixed motives.**?** ⌟

Beilinson-Bloch-Murre Filtration Conjecture

Conj. (8.10.4.2) [Beilinson]. For X/k, there exists a descending filtration $\mathrm{Fil}^\bullet\,\mathrm{CH}^\bullet(X)_\mathbb{Q}$ s.t.

- $\mathrm{Fil}^0\,\mathrm{CH}^j(X)_\mathbb{Q} = \mathrm{CH}^j(X)_\mathbb{Q}$, $\mathrm{Fil}^1\,\mathrm{CH}^j(X)_\mathbb{Q} = \mathrm{CH}^j(X)_\mathbb{Q} = \mathrm{CH}^j(X)_{\mathrm{hom}\,0,\mathbb{Q}}$.
- this filtration is multiplicative.
- $\mathrm{gr}^v\,\mathrm{CH}^j(X)_\mathbb{Q}$ only depends on the motive modulo homological equivalence, $h^{2j-v}(X)$.
- $\mathrm{Fil}^{j+1}\,\mathrm{CH}^j(X)_\mathbb{Q} = 0$.

And moreover, if $k = \mathbb{Q}$, then $\mathrm{Fil}^2 = 0$. ⌟

Proof: □

5 Standard Conjectures

Cf. [Kle94].

Remark (8.10.5.1). The standard conjectures over k are necessary conditions to make the $\mathrm{Mot}_{\mathrm{num}}(k)$ a universal cohomology theory(8.10.3.1). ⌟

Conj. (8.10.5.2) [Lefschetz Standard Conjecture]. Let $k, F \in \mathtt{Field}, k = \overline{k}$ and H^* be a Weil cohomology theory, $X \subset \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}^d/k$, then the Lefschetz operator $L : \mathrm{CH}^i(X) \to \mathrm{CH}^{i+2}(X)$ satisfies for any $i \le d$,

$$L^{n-i} : H^i(X) \to H^{2d-i}(X)$$

is an isomorphism**?**. and for $i \le d$ we can define

$$\Lambda = (L^{d-i+2})^{-1}L(L^{d-i}) : H^i \to H^{i-2}, \Lambda = L^{n-i}L(L^{n-i+2})^{-1} : H^{2n-i+2}(X) \to H^{2n-i}(X),$$

then this Λ is induced from a correspondence from X to X of degree -1. ⌟

Conj. (8.10.5.3) [Standard Conjecture D]. Let $k, F \in \mathtt{Field}, k = \overline{k}$ and H^* be a Weil cohomology theory, then for $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$, a cycle $Z \in \mathrm{CH}^*(X)$ is numerically trivial iff $\gamma_X(Z) = 0$. ⌟

Remark (8.10.5.4). This conjecture was shown by Lieberman for varieties of dimension≤ 4 and for Abelian varieties. ⌟

Conj. (8.10.5.5) [Künneth Standard Conjecture]. Let $k \in \mathtt{Field}$. Assume the conjecture D(8.10.5.3) holds, which implies $\mathrm{Corr}^r_{\mathrm{num}}(X)$ can acts on $H^*(X)$ for any Weil cohomology H^*.

Then for any $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$, there exists a decomposition of $\Delta_X \in \mathrm{Corr}^{\dim X}_{\mathrm{num}}(X \times X)$ into orthogonal idempotents

$$\Delta_X = h^0(X) + \ldots + h^{2\dim X}(X)$$

s.t. it induces the decomposition

$$H^*(X) = H^0(X) \oplus H^1(X) \oplus \ldots \oplus H^{2\dim X}(X)$$

for any Weil cohomology theory H^*. ⌟

Remark (8.10.5.6) [Murre]. Murre even conjecture that such a decomposition exists in $\mathrm{CH}^*(X)$ with certain properties, which is equivalent to a filtration on $\mathrm{CH}^*(X)$, conjectured by Beilinson and Bloch.**?** ⌟

Prop. (8.10.5.7) [Hodge Standard Conjecture]. Let $k, F \in \mathtt{Field}, k = \overline{k}$ and H^* be a Weil cohomology theory, $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}^d/k$, $P^k(X) = \ker(L|H^k(X))$ be the primitive cohomologies, $A^i(X) = \gamma_X(\mathrm{CH}^i(X))$, then for any $i < d/2$, the $\mathbb{Q}$-valued pairing on $A^i(X) \cap P^{2i}(X)$:

$$(x, y) \mapsto (-1)^i \langle L^{r-2i} x, y\rangle$$

is positive definite. ⌟

Remark (8.10.5.8). This conjecture is true in characteristic 0 by Hodge theory. This conjecture is shown for surfaces by Grothendieck(1958). This conjecture is shown for Abelian varieties of dimension 4 by Ancona(2020). ⌟

Prop. (8.10.5.9). The conjecture D implies the Lefschetz standard conjecture. The Hodge standard conjecture and the Lefschetz standard conjecture implies conjecture D. ⌟

Proof: □

Prop. (8.10.5.10) [Hodge Conjecture and Standard Conjecture]. The Hodge conjecture(15.15.4.3) implies the Lefschetz and Künneth standard conjectures and conjecture D for varieties over fields of characteristic 0. ⌟

Proof: □

Prop. (8.10.5.11). If the Lefschetz standard conjecture and the Hodge standard conjecture hold, then for any $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$,

- $\mathrm{Corr}^*_{\mathrm{num}}(X, X)$ is a semisimple $\mathbb{Q}$-algebra.
- (Generalized Riemann Hypothesis)If k is a finite field with Frobenius φ, then for any Weil cohomology H^*, the Frobenius action Φ on $H^i(X)$ is semisimple with characteristic polynomial in $\mathbb{Z}[T]$, and eigenvalues of absolute value $q^{i/2}$.

⌟

Proof: Cf.[Kle94]P19. □

Prop. (8.10.5.12) [Tate Conjecture and Standard Conjectures]. The Tate conjecture implies Lefschetz, Künneth standard conjectures and conjecture D for ℓ-adic étale cohomology over any field. ⌟

Proof: □

8.11 Motivic Cohomology(Voevodsky-Suslin)

References are [Motivic Cohomology, Voevodsky], [$\mathbb{A}^1$-Homology of Schemes, Voevodsky], [Bloch-Kato conjecture and motivic cohomology with finite coefficients, Suslin-Voevodsky] and [Voe02].

Def. (8.11.0.1) [Bloch's Motivic Cohomology Groups]. For $k \in \texttt{Field}$ and $X \in \mathcal{S}m\mathcal{P}\mathrm{roj}\,/k$, define the complex

$$C^p_{\mathrm{Blo},\bullet}(X) = C^p(X \times \mathbb{A}^\bullet),$$

and it is a complex via the pullback along the embedding from edges of $\Delta^n \subset \mathbb{A}^n$. And in fact the cycles must satisfy that the intersections are all proper.(This is what makes it impossible to work with.)

Then define

$$H^{2p-q}_{\mathrm{Mot}}(X, \mathbb{Z}(p)) = \mathrm{CH}^p(X, q).$$

⌟

Def. (8.11.0.2) [Beilinson's Motivic Cohomology Groups]. For $X \in \mathcal{S}m\mathcal{P}\mathrm{roj}\,/\mathbb{Q}$,

$$H^p_{\mathrm{Mot}}(X, \mathbb{Q}(q)) = (K_{2q-p}(X)_{\mathbb{Q}})^{(q)},$$

where the RHS is the Adam operator q-part.

Then this definition is compatible with Bloch's definition(8.11.0.1).? In particular, $H^{2q}_{\mathrm{Mot}}(X, \mathbb{Q}(q)) = \mathrm{CH}^q(X)_{\mathbb{Q}}$, and

$$\bigoplus \mathrm{CH}^p(X, q) \otimes \mathbb{Q} \cong K_q(X).$$

⌟

Proof: □

Prop. (8.11.0.3) [Comparison Maps]. There are ℓ-adic comparison maps

$$H^p_{\mathrm{Mot}}(X, \mathbb{Q}(q)) \to \mathrm{H}^p_{\text{ét}}(X, \mathbb{Q}_\ell(q)), \ell \in \mathbf{P},$$

and Deligne comparison maps

$$H^p_{\mathrm{Mot}}(X, \mathbb{Q}(q)) \to H^p_{\mathrm{Del}}(X, \mathbb{Q}(q)).$$

⌟

Proof: □

Conj. (8.11.0.4) [Integral Motivic Cohomology Groups]. For $X \in \mathcal{S}m\mathcal{P}\mathrm{roj}\,/\mathbb{Q}$, define

$$H^p_{\mathrm{Mot}}(X_{\mathbb{Z}}, \mathbb{Q}(q)) = H^p_{\mathrm{Mot}}(\mathcal{X}, \mathbb{Q}(q)),$$

Where $\mathcal{X}/\mathbb{Z}$ is a proper flat model of X, which always exists?. ⌟

Proof: Cf.[Bei85]2.4.2?. □

Conj. (8.11.0.5) [Beilinson]. For $k \in \texttt{Field}$ and any $n \in \mathbb{N}$, there exists sheaf $\mathbb{Z}(n) \in K(\mathcal{S}h(\mathcal{V}ar^{\mathrm{sm},quasi-proj}_{\mathrm{Zar}}\,/k))$ s.t.

1. $\mathbb{Z}(0) = \mathbb{Z}[0]$, $\mathbb{Z}(1) = \mathcal{O}^*[-1]$,
2. $H^n(\operatorname{Spec} F, \mathbb{Z}(n)) = K^n_{\mathrm{Mil}}(F)$ for any $F \in \mathtt{Field}$.
3. $H^{2n}(X, \mathbb{Z}(n)) = \mathrm{CH}^n(X)$.
4. $H^p(X, \mathbb{Z}(n)) = 0$ for $p < 0$.
5. There are spectral sequences
$$H^{p-q}(X, \mathbb{Z}(-q)) \implies K_{-p-q}(X).$$
6. For $\ell \in \mathfrak{P} \setminus \{\operatorname{char} k\}$,
$$\mathbb{Z}(n) \otimes^{\mathrm{L}} \mathbb{Z}/(\ell) \cong \tau_{\leq n}(R\pi_* \mu_\ell^{\otimes n}).$$
7. $H^i(X, \mathbb{Z}(n)) \otimes \mathbb{Q} \cong H^i_{\mathrm{Mot}}(X, \mathbb{Q}(n))$(8.11.0.2).

⌟

Proof: ? Voevodsky constructed candidates $\mathbb{Z}(n)$ satisfying these conditions except for item4. □

Def. (8.11.0.6) [Absolute Chern Class Maps]. There are Chern class maps:
$$c_{j,m} : K_j(X) \to H^{2m-j}_{\mathrm{Del}}(X/\mathbb{R}, \mathbb{R}(m)),$$
$$\mathrm{ch}_j = \sum_{m \geq 0} \frac{(-1)^{m-1}}{(m-1)!} c_{j,m} : K_j(X) \otimes \mathbb{Q} \to \bigoplus_{m \geq 0} H^{2m-j}_{\mathrm{Del}}(X/\mathbb{R}, \mathbb{R}(m)).$$
such that ch_j maps $(K_j(X)_{\mathbb{Q}})^m$ to $H^{2m-j}_{\mathrm{Del}}(X/\mathbb{R}, \mathbb{R}(m))$. ⌟

Proof: Cf.[Notes on Beilinson's Conjecture, Yihang] or [Nekovar]. □

Curve case

Prop. (8.11.0.7). Let $k \in \mathtt{Field}$, X a non-singular complete curve over k, and $C \subset X$ a finite subscheme, $U = X \setminus C$. Suppose $\mathrm{Pic}^0(C)$ is of finite order in $\mathrm{Jac}(X)$, then
$$H^2_{\mathrm{Mot}}(U, \mathbb{Q}(2)) = H^2_{\mathrm{Mot}}(X, \mathbb{Q}(2)) + \{\mathcal{O}(U)^\times, k^\times\}.$$

⌟

9 Algebraic Geometry III: Group Theory

9.1 Group Schemes I: Structure Theory

Main references are [Sta]Chap38, [Mil17].

1 Group Schemes

Def. (9.1.1.1) [Group Scheme]. A **monoid scheme** over S is a monoid object in the Cartesian monoidal category $\mathcal{S}\mathrm{ch}/S$. The category $\mathcal{G}\mathrm{rp}_S$ of **group schemes** over S consists of group objects in the Cartesian category $\mathcal{S}\mathrm{ch}/S$(4.1.1.66).

An **open/closed subgroup scheme** of a group scheme G/S is an open/closed subscheme of G/S that represents a subgroup functor of G/S.

A **smooth/flat/separated/... group scheme** is a group scheme G/S that G is smooth/flat/separated/... over S.

We have the left(right)translation for an elements in $G(R)$, equivalently, a natural transformation on G, and base change $(G\otimes_S S')(T'/S') = G(T'/S)$ ⌟

Remark (9.1.1.2) [Yoneda Interpretation]. We do not need to verify all the relations, whenever we have a functorial commutative group structure on all the set $\mathrm{Hom}(T,G)$, we immediately recover the map $m: G\times G\to G$ as $\mathrm{pr}_1\cdot\mathrm{pr}_2\subset G(G\times G)$, $\mathrm{inv}: G\to G$ as inv in $G(G)$, $u: S\to G$ as e in $G(S)$, by Yoneda lemma. ⌟

Cor. (9.1.1.3) [Group Schemes as Functors]. From the Yoneda Interpretation and strong Yoneda lemma(9.6.1.1), a group scheme over S is equivalent to a contravariant functor

$$\mathcal{A}\mathrm{ff}_S\to\mathcal{G}\mathrm{rp}: R\mapsto\mathrm{Hom}(\mathrm{Spec}\,R, G)$$

(or equivalently a functor $\mathcal{S}\mathrm{ch}_S\to\mathcal{G}\mathrm{rp}$) that is represented by a scheme over S.

In particular, the category of affine group scheme over $\mathrm{Spec}\,R$ is equivalent to the category of commutative Hopf algebras over R(3.11.4.1). ⌟

Def. (9.1.1.4) [Categorical Group Definitions]. Because we can regard group schemes as functors by(9.1.1.3), we can define categorical constructions of group schemes:

- (Trivial Group Scheme)S is a trivial group scheme over S. It is the zero object in $\mathcal{G}\mathrm{rp}_S$, denoted by e.
- (Commutative Group Schemes)A group scheme G is called a **commutative group scheme** if each $G(R)$ is commutative.
- ($[n]_G$)For any $n\geq 1$, the natural transformation of commutative groups functors $x\mapsto x^n$ induces a morphism of commutative group schemes $[n]: G\mapsto G$ for any group scheme G.

- (Semi-Direct Product)Let G be a group scheme acting on a group scheme H, then we can form a **semi-direct product group scheme** $G \ltimes H$ representing the functor $T \mapsto G(T) \ltimes H(T)$. and $G \ltimes H$ is isomorphic to $G \times H$ as schemes.
- (Kernel)For a homomorphisms of group schemes $\varphi : G \to H$ over R, we define the **kernel group scheme** $\ker \varphi$ representing the functor $R \mapsto \ker(\varphi(R))$. it is represented by the fibered product
$$\begin{array}{ccc} \ker\varphi & \longrightarrow & \operatorname{Spec} R \\ \downarrow & & \downarrow{\scriptstyle \varepsilon_H} \\ G & \xrightarrow{\varphi} & H \end{array}$$
then it is a group scheme over R.
When G, H are affine group schemes, it corresponds to the cokernel Hopf algebra defined in(3.11.4.15).
- (Short Exact Sequences)A sequence of homomorphisms of algebraic groups $e \to N \xrightarrow{i} G \xrightarrow{q} Q$ is called an **exact** if they are exact as sheaves in $\mathcal{S}\mathrm{h}(\mathcal{A}\mathrm{ff}_S)$(or $\mathcal{S}\mathrm{h}(\mathcal{S}\mathrm{ch}_S)$). Exact sequences are stable under base change of fields
- (Quotient Scheme)Let $H \subset G$ be subgroup schemes. If $\widetilde{G}/\widetilde{H}$ is representable, then it is called the **quotient group scheme**, denoted by G/H.
- (Monomorphism)A homomorphism $H \to G$ of group schemes is called a **monomorphism** if $\widetilde{H} \to \widetilde{G}$ is injective.
- (Quotient Map)A homomorphism $H \to G$ of group schemes is called a **quotient map** if $\widetilde{G} \to \widetilde{H}$ is surjective.
- (Normal/Characteristic/Central Subgroups)A subgroup scheme H of G is called normal/characteristic/central if $H(R)$ is normal/characteristic/central in $G(R)$ for any k-algebra R.
- (Normalizing) Let H, N be subgroup schemes of G, then we say H normalizes N if H is contained in the normalizer of N in G.
- (Product Subgroup)Let H, N be algebraic subgroups of an algebraic group G such that H normalizes N, then we define $NH \subset G$ be the algebraic subgroup that is the image of the homomorphism $N \rtimes H \to G$, if it is representable.
- (Generated Subgroup Scheme)Let $\{X_i \to G\}$ be a family of maps to a group scheme G, then the smallest algebraic subgroup H of G generated by φ_i is called the **generated subgroup scheme** if it is representable, denoted by $\langle X_i, \varphi_i \rangle$. It is clear such generated subgroup scheme commutes with base change of fields.
- (Commutator Subgroup)If H_1, H_2 are subgroups of G, let $[H_1, H_2]$ be the subgroup generated by the commutators of H_1, H_2 if it is representable. Or equivalently, it is the subgroup generated by the map $H_1 \times H_2 \to G : [h_1, h_2] \mapsto h_1 h_2 h_1^{-1} h_2^{-1}$.
- (Derived Series)For a group scheme G, define $G^{(1)} = [G, G]$ and define inductively $G^{(n+1)} = [G^{(n)}, G^{(n)}]$.
- (Derived Central Series)For a group scheme G, define $G^1 = [G, G]$ and define inductively $G^{n+1} = [G^n, G^n]$.
- (Subnormal Series)For a group scheme G, a **subnormal series** is a finite sequence of algebraic subgroups $G = G_0 \rhd G_1 \rhd \ldots \rhd G_r = e$ s.t. G_{i+1} is normal in G_i.

- (Solvable Group Schemes) A **solvable group scheme** is a group scheme G that has a subnormal series $G = G_0 \rhd G_1 \rhd \ldots \rhd G_s = \{e\}$ that each quotient G_i/G_{i+1} is commutative.
- (Nilpotent Group Schemes) A **nilpotent group scheme** is a group scheme G that has a subnormal series $G = G_0 \rhd G_1 \rhd \ldots \rhd G_s = \{e\}$ that each quotient G_i/G_{i+1} is central in G/G_{i+1}. Such a sequence is called a **central series**
- (Split Solvable(resp. Nilpotent) Group Schemes)A **split solvable(resp. nilpotent) group** is a group scheme G that has a subnormal(resp. central) series $G = G_0 \rhd G_1 \rhd \ldots \rhd G_s = \{e\}$ that each quotient G_i/G_{i+1} is isomorphic to either $\mathbb{G}_a$ or $\mathbb{G}_m$.
- (Perfect Group Schemes)A group scheme G is called **perfect** if $G = [G, G]$.

⌟

Lemma (9.1.1.5) [Butterfly Lemma]. Let H_1, H_2 be algebraic subgroups of an algebraic group G, N_1, N_2 are normal subgroups of H_1 and H_2, then there is a canonical isomorphism of algebraic groups:

$$N_1(H_1 \cap H_2)/N_1(H_1 \cap N_2) \cong N_2(H_2 \cap H_1)/N_2(H_2 \cap N_1).$$

⌟

Proof: Use the Butterfly lemma for groups(3.1.8.2) and shifify. □

Def. (9.1.1.6) [Translation Map]. For $G \in \mathcal{G}\mathrm{rp}/S$ and any $a \in G(S)$, there is a (left)translation map

$$l_a : G \cong S \times_S G \xrightarrow{(a,\mathrm{id})} G \times_S G \xrightarrow{m} G.$$

and it satisfies l_a, l_b by associativity. ⌟

Prop. (9.1.1.7) [Common Group Schemes].

- $D(\Gamma) = \operatorname{Spec} \mathbb{Z}[\Gamma]$ for a group Γ(3.11.4.3).
- $\mu_n = \mathbb{Z}[T]/(T^n - 1)$(3.11.4.5)
- $\mathbb{G}_a = \mathbb{Z}[T]$(3.11.4.6)
- $\underline{\Gamma} = \operatorname{Spec} \prod_{\gamma \in \Gamma} \mathbb{Z}$(3.11.4.9).
- $\alpha_{p^r} = \operatorname{Spec} \mathbb{F}_p[X]/X^{p^r}$(3.11.4.13).
- $V_{\mathfrak{a}} = \operatorname{Spec} \operatorname{Sym}(V^\vee)$(3.11.4.8).

⌟

Prop. (9.1.1.8). $\operatorname{Hom}(\mathbb{G}_{m,R}, \mathbb{G}_{a,R}) = 0$. ⌟

Proof: Such a homomorphism corresponds to an element $f(T) = \sum a_i T^i$ s.t. $\sum a_i T^i \otimes T^i = \sum a_i (T^i \otimes 1 + 1 \otimes T^i)$, which implies $a_i = 0$ for all i. A homomorphism $\mathbb{G}_{m,R} \to \mathbb{G}_{a,R}$ corresponds to an element $f(T) = \sum a_i T^i$ s.t. $\sum a_i T^i \otimes T^i = \sum a_i (T^i \otimes 1 + 1 \otimes T^i)$, which implies $a_i = 0$ for all i. □

Prop. (9.1.1.9). $\operatorname{Hom}(\mathbb{G}_{a,R}, \mathbb{G}_{m,R}) = 0$. ⌟

Proof: The proof is the same as that of(9.1.1.8). □

Prop. (9.1.1.10). If R is reduced, then $\operatorname{Aut}(\mathbb{G}_{a,R}) \cong R$. ⌟

Proof: Any endomorphism of $\mathbb{G}_{a,R}$ is of the form $X \mapsto a_0 + a_1X + \ldots + a_nT^n$. If it is an automorphism, then for any prime ideal $\mathfrak{p}$, $a_0 \notin \mathfrak{p}$ and $a_i \in \mathfrak{p}, i > 0$, thus a_0 is a unit and a_i are nilpotent for $i > 1$, so $a_i = 0$ for $i > 1$. □

Prop. (9.1.1.11). For $G \in \mathcal{G}\mathrm{rp}/S$, there is a Cartesian diagram:

$$\begin{array}{ccc} G & \xrightarrow{\Delta_{X/S}} & G \times_S G \\ \downarrow & & \downarrow{\scriptstyle (g,g')\mapsto m(i(g),g')} \\ S & \xrightarrow{e} & G \end{array}$$

This can be seen by a testing scheme T. ⌟

Cor. (9.1.1.12) [Separatedness]. $G \in \mathcal{G}\mathrm{rp}/S$ is (quasi-)separated iff e is qc(closed immersion). In particular, if S is a field, then G is separated. ⌟

Def. (9.1.1.13)[Character Group]. A **character** of a group scheme G is a homomorphism $G \to \mathbb{G}_m$. It is easy to see that a character of G is equivalent to a group-like element(3.11.4.17) in $\Gamma(G)$. The characters of G form a group, denoted by $\mathbb{X}(G)$. $\mathbb{X}(G)(k)$ is denoted by $X(G)$.

Moreover, let k^s/k be a separable closure, then the character group of G_{k^s} is denoted by $\mathbb{X}^*(G)$.

In particular, if G is an algebraic group scheme over a field, then the set of characters of G are linearly independent, by(3.11.4.18). ⌟

Prop. (9.1.1.14)[Sheaf of Differentials is Parallel]. If $f : G \to S \in \mathcal{G}\mathrm{rp}/S$, then there are canonical isomorphisms

$$\Omega_{G/S} \cong f^*\mathcal{C}_{G/S} \cong f^*e^*\Omega_{G/S}.$$

In particular, if S is the spectrum of a local ring, then $\Omega_{G/S}$ is a free $\mathcal{O}_G$-module. ⌟

Proof: By base change, $\Omega_{G\otimes_S G/S} = \pi_0^*\Omega_{G/S}$, and the transition map

$$\tau : G \otimes_S G \to G \otimes_S G : (g, h) \mapsto (m(g, h), h)$$

is an automorphism of $G \otimes_S G$ over G, so there is an isomorphism

$$\tau^*\pi_0^*\Omega_{G/S} \cong \pi_0^*\Omega_{G/S}$$

but $\pi_0 \circ \tau = m$, showing this isomorphism is $m^*\Omega_{G/S} \cong \pi_0^*\Omega_{G/S}$. Now pulling this isomorphism along the isomorphism by $(e \circ f, \mathrm{id}) : G \to G \otimes_S G$ we obtain the isomorphism

$$\Omega_{G/S} \cong f^*e^*\Omega_{G/S}.$$

Finally $e^*\Omega_{G/S} \cong \mathcal{C}_{S/G}$ by(6.5.5.14). □

Prop. (9.1.1.15). If $k \in \texttt{Field}$, then any $G \in \mathcal{G}\mathrm{rp}/k$ is geo.reduced. ⌟

Proof: Cf.[Sta]047O.**?** □

Prop. (9.1.1.16) [Galois Descent]. Let $k \in \texttt{Field}, G \in \mathcal{G}\mathrm{rp}/k$ and K/k is a Galois extension with Galois group Γ. If H' is a subgroup of $G \otimes_k K$, then H' is stable under the action of Γ iff there exists a subgroup H of G that $H \otimes_k K = H'$. In this case, H is unique. ⌟

Proof: Use(6.1.5.19) and(6.1.5.22). □

Prop. (9.1.1.17). Let X, Y be varieties over a field k that both have at least one K-point, and X is complete. Then any morphism $X \times Y \to G$ to a group scheme G over k factorizes as $f(x,y) = g(x)h(y)$, where $f : X \to G$ and $h : Y \to G$. ⌟

Proof: Fix a $y_0 \in Y(K)$ and define a morphism $g : X \to G : x \mapsto f(x, y_0)$, then the morphism $F : X \times Y \to G : (x,y) \mapsto g(x)^{-1} f(x,y)$ is constant on $X \times \{y_0\}$. Then the rigidity lemma(6.11.1.20) and(9.1.1.12) shows $F(x,y) = h(y)$ where $h : Y \to G$ is a morphism. Then we are done. □

Cor. (9.1.1.18). Any morphism from a $\mathbb{P}^1_K$ to a group scheme G is constant. ⌟

Proof: Let (x_0, x_1) be a homogenous coordinate of $\mathbb{P}^1$, consider the morphism $s : \mathbb{P}^1 \times \mathbb{A}^1 \to \mathbb{P}^1 : (x_0, x_1) \times y \mapsto (x_0, x_0 + x_1 y)$. Let $f : \mathbb{P}^1 \to G$ be a morphism, consider the composition

$$\mathbb{P}^1 \times \mathbb{A}^1 \xrightarrow{s} \mathbb{P}^1 \xrightarrow{f} G$$

then by(9.1.4.19), $f \circ s$ factors as $f(s(x,y)) = g(x)h(y)$.

We take $y = 0$, then $s(x,0) = x$, and $g(x) = f(x)h(0)^{-1}$. Thus $f(s(x,y)) = f(x)h(0)^{-1}h(y)$. Next we take $x = (0,1)$, then $s((0,1),y) = (0,1)$, and $f((0,1)) = f((0,1))h(0)^{-1}h(y)$. This shows $h(y) = h(0)$ is constant, thus $f(s(x,y)) = f(x)$. Finally, let $x = (0,1)$, then $s((0,1),y) = y$, and $f(y) = h(0)$ is constant. □

Cor. (9.1.1.19). Let U be an open subset of $\mathbb{P}^1$, then any morphism from U to a group variety G is constant. In particular, G contains no rational curve, and any morphism from a rationally connected variety to G is constant, in particular $\mathbb{P}^n_K$. ⌟

Proof: Any rational map from $\mathbb{P}^1$ to G can be extended to a morphism, by(6.12.1.15), thus it is constant, by the proposition above. □

Prop. (9.1.1.20)[Weil's Extension Theorem]. Let $S \in \mathrm{N}\,\mathcal{S}\mathrm{ch}_{\mathrm{nom,qc}}$, $Z \in \mathcal{S}\mathrm{ch}^{\mathrm{sm}}/S$, $G \in \mathcal{G}\mathrm{rp}^{\mathrm{sm,sep}}/S$. If $\varphi : Z \to G$ is an S-rational map, then every irreducible component of $X \setminus \mathrm{dom}(\varphi)$ is of codimension 1. ⌟

Proof: Cf.[BLR90]P109.**?** □

Classification of groups schemes of height 1 over a field

Quotients of Group Schemes

Prop. (9.1.1.21) [Grothendieck]. Let G be a group scheme of f.t. over S and H is a closed subgroup scheme of G. If H is proper flat over S and if G is quasi-projective over S, then the quotient functor $\widetilde{G}_{fppf}/\widetilde{H}_{fppf}$ is representable by a scheme, denoted by G/H. ⌟

Proof: Cf.[Grothendieck, A. Technique de descente et theoremes d'existence en geometrie algebrique, III]. □

Cor. (9.1.1.22) [Existence of Quotient Schemes]. Let $H \to G$ be a monomorphism of algebraic groups over a field k(9.1.5.6), then the quotient functor $\widetilde{G}_{\mathrm{fppf}}/\widetilde{H}_{\mathrm{fppf}}$ is representable by an algebraic scheme. And $G \to G/H$ is faithfully flat. ⌟

Proof: Cf.[Mil17b]P605.**?** □

Cor. (9.1.1.23)[Quotient by Normal Subgroups]. Every normal algebraic group N of an algebraic group G arises as the kernel of a quotient map $G \to G/N$. And if G is affine, G/N is also affine. ⌟

Proof: This is a corollary of(9.1.1.22) and(9.1.1.26) and(9.6.1.12).

The second assertion follows from[Mil17]P103.? □

Cor. (9.1.1.24)[Quotient Map is a Cokernel]. Let $q : G \to Q$ be a quotient map of algebraic groups over k and let N be the kernel, then every homomorphism $G \to H$ whose kernel contains N factors uniquely through q. ⌟

Prop. (9.1.1.25). Let G/H be a quotient space, then the map

$$(g, h) \mapsto (g, gh) : G \times H \mapsto G \times_{G/H} G$$

is an isomorphism. ⌟

Proof: This is because for any R, $G(R) \times H(R) \to G(R) \times_{G(R)/H(R)} G(R)$ is an isomorphism, and use the fact $G(R)/H(R) \subset (G/H)(R)$ as $\widetilde{G}/\widetilde{H}$ is a subfunctor of $\widetilde{G/H}$. □

Cor. (9.1.1.26). For any k-algebra R, the nonempty fibers of $G(R) \to G/H(R)$ are cosets of $H(R)$. In particular, the fiber over $o \in G/H$ is just H. ⌟

Cor. (9.1.1.27)[Quotient is a Torsor]. G is a (fppf) H-torsor over G/H. ⌟

Proof: This follows from(9.1.1.22) and(9.1.1.27). □

Prop. (9.1.1.28) [Additivity of Dimensions]. Let G be an algebraic group and H an algebraic subgroup, then

$$\dim G = \dim H + \dim G/H.$$

⌟

Proof: This follows from(6.6.3.17) and(9.1.1.26). (Notice $G(\overline{k}) \to H(\overline{k})$ is surjective(9.1.5.5)). □

Thm. (9.1.1.29)[Homomorphism Theorem]. Every homomorphism of algebraic groups $f : G \to H$ factors uniquely as

$$G \xrightarrow{q} I \xrightarrow{i} H$$

where q is a quotient map and i is a monomorphism. I is called the **image of** f. ⌟

Proof: Let $N = \ker(f)$, and $q : G \to I = G/N$(9.1.1.23), then by(9.1.1.24), f factors through I via a monomorphism I by(9.1.1.21). □

Cor. (9.1.1.30). A homomorphism of algebraic groups is a quotient map iff it is an epimorphism in the category of algebraic schemes. ⌟

Proof: For any homomorphism of group schemes $\varphi : G \to H$, factor it as in(9.1.1.29), then we can form the quotient space H/I, so if it is an epimorphism, $I = H$, and φ is a quotient map. Conversely, if it is a quotient map, then $\mathcal{O}_H \to \varphi_* \mathcal{O}_G$ is injective by(9.1.5.3), thus it is an epimorphism. □

Cor. (9.1.1.31). If f is surjective and H is reduced, then f is a quotient map. ⌟

Prop. (9.1.1.32). Let H, N be subgroup schemes of G with N normal, then the canonical map

$$N \rtimes H \to G$$

is an isomorphism iff $N \cap H = e$ and $NH = G$. ⌟

Proof: This follows from the exact sequence $e \to N \cap H \to N \rtimes H \to NH \to e$. □

Prop. (9.1.1.33) [Isomorphism Theorem]. Let H, N be algebraic subgroups of an algebraic group G such that H normalizes N, then $H \cap N$ is a normal algebraic subgroup of H, and the natural map

$$H/H \cap N \to HN/N$$

is an isomorphism. ⌟

Proof: The isomorphism is induced by shifification of the natural isomorphism

$$T_R : H(R)/H(R) \cap N(R) \cong H(R)N(R)/N(R)(3.1.2.8).$$

□

Prop. (9.1.1.34)[Correspondence Theorem]. Let N be a normal algebraic subgroup of an algebraic group G, then

- An algebraic subgroup H of G, the inverse image of the image of H in G/N is HN.
- The map $H \mapsto H/N$ is a bijection between the set of algebraic subgroups of G containing N to the set of algebraic subgroups of G/N.
- An algebraic subgroup H of G containing N is normal in G iff H/N is normal in G/N, in which case the natural map $G/H \to (G/N)/(H/N)$ is an isomorphism.

⌟

Proof: Cf.[Mil17]P113.**?** □

Prop. (9.1.1.35) [Group Formation]. WARNING: the category $\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}_k$ of algebraic groups is not Abelian, not even an exact category, but it is a group formation(4.3.2.1), and its subcategory $\mathcal{C}\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}_k$ of commutative algebraic groups is an Abelian category, by(9.1.1.23)(9.1.5.2)(9.1.1.4).

Also the subcategory of affine algebraic groups is a Serre subcategory, by(9.1.1.23) and(9.1.5.29). ⌟

Cor. (9.1.1.36). By taking shifification, it can be shown that the same categorical properties of $\mathcal{G}\mathrm{rp}$ holds for $\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}_k$, such as the nine lemma, five lemma, and the restrictive snake lemma. ⌟

2 Finite Groups

Main references are [Finite Flat Group Schemes and p-Divisible Groups, Jakob], [Finite Group Schemes, Pink], [Introduction to Finite Group Schemes], [Finite Flat Group Schemes, Tate].

Def. (9.1.2.1) [Finite Locally Free Group Schemes]. A **finite Locally Free group scheme** is a group scheme G that is finite locally free(6.6.2.22) over S. It is said to have **order/rank** d if G is finite locally free of rank d over S, where d is a locally constant integral-valued function on S. ⌟

Def. (9.1.2.2) [Finite Groups]. A finite locally free group scheme over a field k is called a **finite group scheme** over k. An **infinitesimal group scheme** is a finite group scheme G s.t. $|G| = e$. ⌟

Prop. (9.1.2.3) [Cartier]. Let k be a field of characteristic 0, then

- Every affine finite commutative group scheme over k is finite étale.
- If k is alg.closed, then there is an equivalence of categories between finite commutative group schemes over k and $\mathcal{A}$b, by $G \mapsto G(k)$ and $\Gamma \mapsto \underline{\Gamma}_k$.

⌟

Proof: 1: by(3.11.4.20) and(5.4.7.20).

2: $\underline{\Gamma}_k$ is clearly affine commutative group schemes over k. If A is finite locally free Hopf algebra over k, then it is finite étale by item1 and isomorphic to a fintie product of copies of k. Now the equivalence is clear. □

Prop. (9.1.2.4) [Finite Group Schemes of Order Invertible in S is Finite Étale]. A finite group scheme G over S of order invertible in S is finite étale. ⌟

Proof: Cf.[Jakob, P45].**?** □

Prop. (9.1.2.5) [Finite Étale Group Schemes]. Let X be a connected smooth scheme with a geometric point $\overline{x}$, then there is a equivalence of categories:

$$\{\text{Finite étale group schemes over } X\} \leftrightarrow \{\text{Finite groups with a continuous action of } \pi_1(X, \overline{x})\}$$

by(8.3.2.5). In particular, constant group schemes correspond to finite groups with trivial $\pi_1(X, x)$ actions. ⌟

Cor. (9.1.2.6). The category of finite étale commutative group schemes over X is Abelian.

The category of commutative group schemes over X of order invertible in X is Abelian, by(9.1.2.4). ⌟

Commutative Finite Groups

Prop. (9.1.2.7) [Cartier Duality]. Let G be a finite commutative locally free group scheme over S, then $\mathcal{O}_G$ is a finite locally free $\mathcal{O}_S$-Hopf algebra, then $\mathrm{Hom}_{\mathcal{O}_S}(\mathcal{O}_G, \mathcal{O}_S) = \mathcal{O}_G^\vee$ is again a finite locally free $\mathcal{O}_S$-Hopf algebra(6.2.5.2), and thus $\mathbf{Spec}\, \mathcal{O}_G$ is a finite locally free group scheme over S, called the **Cartier dual** G^D of G.

Moreover, this Cartier dual of G represents the Hom sheaf $\underline{\mathrm{Hom}}_{\mathcal{S}\mathrm{ch}/S}(G, \mathbb{G}_m)$.

If G is dual to G', then their base changes are dual, too.

Finally, $(G^D)^D = G$ by(6.2.5.2), so Cartier duality is a contravariant autoequivalence of the category of commutative finite locally free group schemes over S. ⌟

Proof: For the Hom sheaf, we need to show

$$G^D(T) \cong \mathrm{Hom}_T(G \otimes_S T, \mathbb{G}_{m,T})$$

for any T/S. Notice a $g \in G^D(T)$ corresponds to an R-algebra morphism $g \in \mathrm{Hom}_{\mathcal{O}_S}(\mathcal{O}_G^\vee \to \mathcal{O}_T) = \mathcal{O}_G \otimes_{\mathcal{O}_S} \mathcal{O}_T$(6.2.5.2) that satisfies

$$(\Delta \otimes \mathrm{id}_T)(g) = g \otimes_T g \in (\mathcal{O}_G \otimes_{\mathcal{O}_S} \mathcal{O}_G) \otimes_{\mathcal{O}_S} \mathcal{O}_T, \quad (\varepsilon \otimes \mathrm{id}_T)(g) = 1$$

Also, g is a unit, as

$$g \cdot (\iota \times \mathrm{id}_T)(g) = \mu \circ ((\mathrm{id}_{\mathcal{O}_G} \otimes \iota) \otimes \mathrm{id}_{\mathcal{O}_T})(g \otimes g) = \mu \circ ((\mathrm{id}_{\mathcal{O}_G} \otimes \iota) \otimes \mathrm{id}_T) \circ (\Delta \otimes \mathrm{id}_T)(g) = (\eta_{\mathcal{O}_G} \otimes \mathrm{id}_T)(\varepsilon \otimes \mathrm{id}_T)(g) = 1$$

so g corresponds to a $\mathscr{O}_T$-Hopf algebra map

$$\mathscr{O}_T[X,X^{-1}]\to\mathscr{O}_G\otimes_{\mathscr{O}_S}\mathscr{O}_T$$

which maps X to G, □

Prop. (9.1.2.8)[$\underline{\Gamma}$ is Cartier Dual to $D(\Gamma)$]. Let Γ be a finite commutative group and S be a scheme, then $\underline{\Gamma}_S$ is Cartier dual to $D(\Gamma)_S$. ⌟

Proof: By(9.1.2.7), it suffices to show for $S=\operatorname{Spec}\mathbb{Z}$. Now $\underline{\Gamma}=\prod_{\gamma\in\Gamma}\mathbb{Z}$, and $\Delta(e_\gamma)=\sum_{gg'=\gamma}e_g\otimes e_{g'}$. Let $f_\gamma\in\underline{\Gamma}^\vee$ be dual to e_γ, then

$$f_\gamma\cdot f_{\gamma'}=\sum_{g\in\Gamma}\Delta^\vee(f_\gamma\otimes f_{\gamma'})(e_g)f_g=\sum_{g\in\Gamma}f_\gamma\otimes f_{\gamma'}(\sum_{st=g}e_s\otimes e_t)f_g=f_{\gamma\gamma'}$$

so $\underline{\Gamma}^\vee\cong\mathbb{Z}[\Gamma]$, and

$$\Delta(f_\gamma)=\sum_{g,g'\in\Gamma}\mu^\vee(f_\gamma)(e_g\otimes e_{g'})f_g\otimes f_{g'}=f_\gamma\otimes f_\gamma.$$

□

Cor. (9.1.2.9). $\underline{\mathbb{Z}/n\mathbb{Z}}$ is Cartier Dual to μ_n. ⌟

Prop. (9.1.2.10) [α_p is Cartier Dual to α_p]. Over a $\mathbb{F}_p$-scheme S, the group scheme $\alpha_{p,S}$ is Cartier dual to itself. ⌟

Proof: By(9.1.2.7), it suffices to show for $S=\operatorname{Spec}\mathbb{F}_p$. Then $\alpha_p=\mathbb{F}_p[X]/X^p$ with

$$\Delta(X)=X\otimes 1+1\otimes X,\quad \varepsilon(X)=0,S(X)=-X.$$

Let $Y_i\in\alpha_p^\vee$ dual to X^i then

$$Y_i\cdot Y_j=\sum_{k=0}^{p-1}\Delta^\vee(Y_i\otimes Y_j)(X^k)Y_k=\sum Y_i\otimes Y_j(\Delta(X^k))Y_k=\sum Y_i\otimes Y_j(\sum_{a+b=k}\binom{k}{a}X^a\otimes X^b)Y_k=\binom{i+j}{i}$$

Now $\binom{i+j}{i}$ is unit, so $\alpha_p^\vee=\mathbb{F}_p[Y]/Y^p$ where $Y=Y_1$. and

$$\Delta(Y)=\sum_{a,b}\mu^\vee(Y)(X^a\otimes X^b)Y_a\otimes Y_b=\sum Y(X^{a+b})=Y\otimes 1+1\otimes Y,$$

so $\alpha_p^\vee=\alpha_p$. □

Prop. (9.1.2.11). If G_1,G_2 are finite groups over a field k, then there are no non-trivial homomorphism from G_1 to G_2 or from G_2 to G_1 if G_1 is étaleand G_2 is connected. ⌟

Proof: Cf.[Van de Geer, P67]. □

Prop. (9.1.2.12). If $e\to G_1\to G\to G_2\to e$ is an exact sequence of finite locally free group schemes over S, then $\operatorname{rank}(G)=\operatorname{rank}(G_1)\cdot\operatorname{rank}(G_2)$. ⌟

Proof: Cf.[Van de Geer, P68]. □

Prop. (9.1.2.13). Let $\operatorname{char}k=p>0$, then the rank of any finite group over k is a power of p. ⌟

Proof: Cf.[Van de Geer, P68]. □

Cor. (9.1.2.14). Let char $k = p > 0$, then a finite group over k is étaleand coétaleiff $p \nmid \mathrm{rank}(G)$. ⌟

Proof: Cf.[Van de Geer, P68]. □

Prop. (9.1.2.15). Over a $\mathbb{F}_p$-scheme S, the three group schemes $\underline{\mathbb{Z}/p\mathbb{Z}}_S, \mu_{p,S}, \alpha_{p,S}$ are mutually non-isomorphic. ⌟

Proof: We may take a fiber and assume $S = \mathrm{Spec}\, K$, then $\underline{\mathbb{Z}/p\mathbb{Z}}_S$ is reduced, $\mu_{p,S}$ is non-reduced and $\alpha_{p,S}$ is non-reduced. Then we can look at the reducedness of the group scheme and its Cartier dual. □

Prop. (9.1.2.16) [The Order Kills the Group, Deligne]. If G is a finite locally free commutative group scheme over S of constant order n, then $[n]_G = 0 : G \to G$. ⌟

Proof: Cf.[Jakob P12].? □

Finite Locally Free Group Schemes over Henselian Local Rings

Remark (9.1.2.17). Throughout this subsubsection, let R be a Henselian local ring $(R, \mathfrak{m})$. ⌟

Prop. (9.1.2.18). ⌟

Proof: □

Cor. (9.1.2.19). Let R be a equicharacteristic Henselian local ring of characteristic $p > 0$, then every finite locally free group scheme over R of prime order is automatically commutative. ⌟

Proof: Cf.[Shatz, P50]. □

Cor. (9.1.2.20). Let R be a strict Henselian local ring with residue field of characteristic $p > 0$, then any connected finite locally free group scheme over R has order p^t for some $t > 0$. ⌟

Proof: Cf.[Shatz, P50]. □

Commutative p-Group Schemes

Cf.[Finite Flat Group Schemes, Tate]Section4.

3 Groupoid Schemes

Cf.[Sta]Cha38, 39.

4 Algebraic Groups over Fields

All group schemes G in this subsection are algebraic over a field k.

Prop. (9.1.4.1) [Smoothness and Geo.Reducedness]. For a locally algebraic group scheme G over a field k, smoothness is equivalent to geo.reducedness at a closed point. ⌟

Proof: If G is smooth, then it is geo.regular thus geo.reduced. The converse follows from(9.2.1.10). □

Cor. (9.1.4.2) [Cartier]. Any locally algebraic group scheme over a field of char 0 is smooth. ⌟

Proof: This is a consequence of (9.1.1.15) and (9.1.4.1). Alternative proof: $\Omega_{G/k}$ is free, by (9.1.1.14), so it is smooth by (6.6.4.15). □

Prop. (9.1.4.3) [Reduced Structure]. If G_{red} is geo.reduced, then it is a subgroup of G. This is the case if k is perfect. ⌟

Proof: This is because $G_{\text{red}} \times G_{\text{red}}$ is reduced so the multiplication factors through $G_{\text{red}} \times G_{\text{red}}$. □

Prop. (9.1.4.4) [Smoothness in Characteristic p]. Let G be an affine algebraic groups over a perfect field k of characteristic $p \neq 0$, and $r \geq 0$, then image of the relative Frobenius $F_{G/k} : G \to G^{(p^r)}$ is geo.reduced group scheme when r is sufficiently large. ⌟

Proof: To show it is a group scheme, notice F^r is a homomorphism and use homomorphism theorem (9.1.1.29). And It corresponds to

$$\Gamma(G) \otimes_{k,\varphi^r} k \to \Gamma(G) : a \otimes c \mapsto ca^{p^r}.$$

The image of which is just $\Gamma(G)^{p^r}$ as k is perfect. To show it is geo.reduced, we can assume k is alg.closed, then the nilradical N of $\Gamma(G)$ is nilpotent, so some $N^m = 0$, and then the image is reduced for any $p^r > m$. □

Prop. (9.1.4.5) [Smoothness and Tangent Space]. A locally algebraic group scheme G over a field is smooth iff it is regular iff $\dim_k T_e \leq \dim_e G$, where e is the identity element. ⌟

Proof: By homogeneity and the fact smooth locus is open, G is smooth iff it is smooth at e. Now e is a rational point, by (5.4.5.26), G is smooth at e iff it is regular at e. □

Prop. (9.1.4.6) [Closed Subgroups and Points]. Let G be a locally algebraic subgroup over k and $S \subset G(k)$ a closed subgroup, then there is a unique reduce closed subgroup H of X that $H(k) = S$. Moreover, H is geo.reduced. The algebraic subgroups of G arising in this way are exactly those that $H(k)$ is schematically dense in H. linear In particular, when k is sep.closed, then $H \mapsto H(k)$ is a bijection between closed subgroups of G and closed subgroups of $G(k)$, by (6.4.3.10). ⌟

Proof: Let H be a reduced closed subscheme of G that $H(k) = S$, then S is dense in $|H|$ and H is reduced, so by (6.4.3.5) and (6.4.3.8) shows S is schematically dense in H and H is geo.reduced. Therefore $H \times H$ is reduced and thus multiplication map $H \times H \to G$ factors through H, also does inversion and unit, so H is a subgroup of G.

The converse is also true. □

Cor. (9.1.4.7) [Zariski Closure]. Let G be a locally algebraic subgroup over k and $S \subset G(k)$ a subgroup, then there is a unique geo.reduced closed subscheme H of G, called the Zariski closure of S in G, such that $H(k)$ is the Zariski closure of $S \subset G(k)$. ⌟

Prop. (9.1.4.8) [Algebraic Group Scheme is Quasi-Projective]. Any algebraic group scheme over a field k is quasi-projective. ⌟

Proof: Cf.[Sta]0BF7**?**. □

Prop. (9.1.4.9) [Center Subgroup]. For a locally algebraic group scheme G over a field k, its center is an algebraic subgroup of G. ⌟

Proof: Cf.[Sta]0BF8. □

Prop. (9.1.4.10). Every étale normal subgroup of a connected algebraic group is central. ⌟

Proof: This is because the automorphism group scheme of an étale group scheme is étale**?**. □

Prop. (9.1.4.11) [Identity Components]. For a locally algebraic group G over a field k, consider its identity component G^0, then

- It commutes with the formation of identity component commutes with base change of fields. In particular, G^0 is geo.connected.
- G is locally connected(6.4.1.23), thus G^0 is clopen in G.
- G^0 is a a characteristic algebraic subgroup of G

⌟

Proof: $1, 2$ follows from(6.4.3.15).

3: By(6.4.3.12), $G^0 \times G^0$ is connected, thus $G^0 \times G^0$ is mapped into G^0, and it is an open subscheme, thus it is an algebraic subgroup of G. □

Cor. (9.1.4.12) [$\pi_0(G)$]**.** Let G be a locally algebraic group, then group structure induces a group structure on the maximal étalesubalgebra of $\Gamma(G)$, thus $G \to \pi_0(G)$ is a group homomorphism(8.3.1.1), which is faithfully flat by(8.3.1.3), and the stabilizer of the identity in $\pi_0(G)$ is just G^0 by(8.3.1.3) again. Thus $\pi_0(G) = G/G^0$ by(9.2.1.11). ⌟

Prop. (9.1.4.13). Every connected component of a locally algebraic group G over a field k is irreducible. ⌟

Proof: By(9.1.4.11), $G^0_{\overline{k}}$ is connected. To show it is irreducible, it suffices to consider its reduced structure, and in this case it is smooth(Notice in this case G^0_{red} is an algebraic group because $G^0_{\mathrm{red}} \times G^0_{\mathrm{red}}$ is reduced). Thus no closed point is connected in two irreducible component, thus it is irreducible. Then G^0, as a quotient space of $G^0_{\overline{k}}$, is also irreducible.

For another connected component H, choose a closed point h, let L be a finite normal extension of k containing $k(h)$, then each connected component of H_L maps surjectively onto H, thus contains one of the finitely many inverse images of h in H_L. And they are all rational points, thus isomorphic to G^0_L, which is irreducible, thus H is also irreducible. □

Cor. (9.1.4.14) [Connected Algebraic Group is Geo.Irreducible]. A connected algebraic group over a field is geo.irreducible by(9.1.4.11) and(9.1.4.13). ⌟

Cor. (9.1.4.15). If G is a connected algebraic group over a field k, then for any non-empty open subschemes U, V of G, $U \times V \to G$ is surjective. ⌟

Proof: By(6.4.1.29), it suffices to check on closed points. Let p be a closed point, by base change, we may assume $x \in G(k)$, then $xV^{-1} \cap U \neq \varnothing$ as G is geo.irreducible(9.1.4.14), thus $x \in UV$. □

Cor. (9.1.4.16). Every connected component of a locally algebraic group scheme over a field k is algebraic over k. ⌟

Proof: For the identity component, take a non-empty affine open subset U, then $U^2 = G^0$ by(9.1.4.15), thus G^0 is quasi-compact. For the other components, the same proof as that of(9.1.4.13) shows they are also quasi-compact. □

Def. (9.1.4.17) [Torsion Component]. Let G be a locally algebraic commutative group over k, then $G^\tau = \cup_{n>0}[n]^{-1}G^0 \subset G$ is an open group subscheme, called the **torsion component** of G. Forming G^τ commutes with change of fields, and if G^τ is quasi-compact, it is a clopen subgroup. ⌟

Prop. (9.1.4.18). Let G be a locally algebraic commutative group over k, then any algebraic subgroup of G is contained in G^τ. In particular, if G^τ is algebraic over k, then it is the maximal algebraic subgroup of G. ⌟

Proof: As H is qc, it is covered by f.m. translates of G^0, thus G^0 has finite index in G^0H, which means $[n](H) \subset G^0$ for some $n \in \mathbb{Z}_+$. □

Prop. (9.1.4.19). Let X, Y be varieties over a field k that both have at least one K-point, and X is complete. Then any morphism $X \times Y \to G$ to a group scheme G over k factorizes as $f(x, y) = g(x)h(y)$, where $f : X \to G$ and $h : Y \to G$. ⌟

Proof: Fix a $y_0 \in Y(K)$ and define a morphism $g : X \to G : x \mapsto f(x, y_0)$, then the morphism $F : X \times Y \to G : (x, y) \mapsto g(x)^{-1}f(x, y)$ is constant on $X \times \{y_0\}$. Then the rigidity lemma(6.11.1.20) and(9.1.1.12) shows $F(x, y) = h(y)$ where $h : Y \to G$ is a morphism. Then we are done. □

Cor. (9.1.4.20). Any morphism from a $\mathbb{P}^1_K$ to a group scheme G is constant. ⌟

Proof: Let (x_0, x_1) be a homogenous coordinate of $\mathbb{P}^1$, consider the morphism $s : \mathbb{P}^1 \times \mathbb{A}^1 \to \mathbb{P}^1 : (x_0, x_1) \times y \mapsto (x_0, x_0 + x_1 y)$. Let $f : \mathbb{P}^1 \to G$ be a morphism, consider the composition

$$\mathbb{P}^1 \times \mathbb{A}^1 \xrightarrow{s} \mathbb{P}^1 \xrightarrow{f} G$$

then by(9.1.4.19), $f \circ s$ factors as $f(s(x, y)) = g(x)h(y)$.

We take $y = 0$, then $s(x, 0) = x$, and $g(x) = f(x)h(0)^{-1}$. Thus $f(s(x, y)) = f(x)h(0)^{-1}h(y)$. Next we take $x = (0, 1)$, then $s((0, 1), y) = (0, 1)$, and $f((0, 1)) = f((0, 1))h(0)^{-1}h(y)$. This shows $h(y) = h(0)$ is constant, thus $f(s(x, y)) = f(x)$. Finally, let $x = (0, 1)$, then $s((0, 1), y) = y$, and $f(y) = h(0)$ is constant. □

Cor. (9.1.4.21). Let U be an open subset of $\mathbb{P}^1$, then any morphism from U to a group variety G is constant. In particular, G contains no rational curve, and any morphism from a rationally connected variety to G is constant, in particular $\mathbb{P}^n_K$. ⌟

Proof: Any rational map from $\mathbb{P}^1$ to G can be extended to a morphism, by(6.12.1.15), thus it is constant, by the proposition above. □

Def. (9.1.4.22) [Anti-Affine Group Schemes]. An **anti-affine algebraic group** is an algebraic group over k s.t. $\Gamma(G) = k$. For example, Abelian varieties are anti-affine by(6.11.1.12) ⌟

Prop. (9.1.4.23). Let $\varphi : G \to H$ be a homomorphism of algebraic groups over k that G is anti-affine and H is connected, then φ factors through the center of H(9.1.4.9). ⌟

Proof: Cf.[Mil17]P151. □

Cor. (9.1.4.24). If G is a connected algebraic group over k, then every anti-affine algebraic subgroup is contained in the center of G. ⌟

Cor. (9.1.4.25). Any anti-affine algebraic group is commutative and connected. ⌟

Proof: $G \to \pi_0(G)$ is surjective but $\pi_0(G)$ is affine thus this map is trivial, so G is connected. Then it is also commutative by(9.1.4.24). □

Construction of Algebraic Groups

Prop. (9.1.4.26)[Generated Closed Subgroup]. Let $\varphi_i : X_i \to G$ be a family of maps from algebraic schemes X to an algebraic group over a field k.

- If X_i and G are all affine, then the generated group scheme is representable by an algebraic subgroup H.
- If X_i are all geo.reduced. Then the generated group scheme is representable by a smooth subgroup H.

Moreover, in both cases, if there is only a single map $\varphi : X \to G$ and X is geo.connected, and $e \subset \varphi(X)$, then $\langle X, \varphi\rangle$ is geo.connected. ⌟

Proof: Cf.[Mil17]P54, 55, 56. □

Def. (9.1.4.27) [Commutator Group]. Let G be an algebraic group that is affine or smooth, then $[G, G]$ exists by(9.1.4.26), and:

- $[G, G]$ is the intersection of all normal subgroups H of G s.t. G/H is commutative.
- For a field extension k'/k, $[G_{k'}, G_{k'}] = [G, G]_{k'}$.
- If G is geo.connected/smooth, then $[G, G]$ is also geo.connected/smooth.
- If G is an affine smooth geo.connected group scheme, then $[G, G]$ is the unique smooth geo.connected subgroup scheme that satisfies $[G, G](\overline{k}) = [G(\overline{k}), G(\overline{k})]$.

⌟

Proof: 1: Cf.[Mil17]P129.
2: This is formal.
3: This follows from(9.1.4.26).
1: Cf.[Mil17]P130. □

Def. (9.1.4.28) [Transporter]. Let $G \times X \to X$ be an action of an algebraic group on a scheme, and Y, Z be subschemes of X, Z is a closed subscheme and Y is an algebraic scheme, then the functor

$$R \mapsto \{g \in G(R) | gY_R \subset Z_R\}$$

is represented by a closed subscheme of G, called the **transporter** $T_G(Y, Z)$. ⌟

Proof: $T_G(Y, Z)$ is in fact the sheaf $\mathcal{H}om(Y, Z) \times_{\mathcal{H}om(Y,X)} G$, and notice $\mathcal{H}om(Y, Z) \to \mathcal{H}om(Y, X)$ is a closed subfunctor(9.6.1.3), thus $T_G(Y, Z)$ is a closed subfunctor of G, thus represented by a closed subscheme of G. □

Cor. (9.1.4.29). Let $G \times X \to X$ be an action of an algebraic group on a scheme, and Y, Z be closed subschemes of X, then the functor

$$R \mapsto \{g \in G(R) | gY_R = Z_R\}$$

is represented by a closed subscheme of G. ⌟

Proof: In this case, the functor is represented by the closed subscheme $T_G(Y, Z) \cap \mathrm{inv}(T_G(Z, Y))$. □

Cor. (9.1.4.30) [Stablizer]. Let $G \times X \to X$ be an action of an algebraic group on a scheme, and Y be closed subschemes of X, then the functor

$$\mathrm{Stab}_G(Y) : R \mapsto \{g \in G(R) | gY_R = Y_R\}$$

is represented by a closed subscheme of G, called the **stablizer subgroup of** Y. ⌟

Def. (9.1.4.31) [Normalizer]. ⌟

Def. (9.1.4.32) [Centralizer]. ⌟

Group Varieties

Def. (9.1.4.33) [Group Varieties]. A **group variety** over a field k is a k-variety(6.11.1.3) that is also a group scheme. ⌟

Prop. (9.1.4.34) [Group Varieties are Smooth]. For $k \in$ `Field`, a group variety over k is smooth by(9.1.4.1). Conversely, any smooth connected algebraic group over k is a group variety, by(9.1.4.14)(9.1.1.12). ⌟

Prop. (9.1.4.35) [Tangent Bundle Trivial]. For a group variety over a field k, $T_{X,e}$ is the tangent space at e, then there is a natural isomorphism $\Omega_{X/k} \cong T^*_{X,e} \otimes \mathcal{O}_X$. Also true for $\mathcal{T}_X$(because $\Omega_{X/k}$ is locally free as X is smooth(9.1.4.34)(6.11.1.14)). ⌟

Proof: There should be another proof using relation in(6.5.5.14)**?**.

Use a dual number characterization of tangent spaces and tangent vector fields(6.6.4.22)(6.11.1.15), then notice a tangent vector $\tau \in T_{X,e}$ is a $S = k[\varepsilon]$-point of X, then right translation gives a translation $X_S \to X_S$ that is invariant on X, which gives a tangent vector on X.

So there is a map $T_{X,e} \otimes \mathcal{O}_X \to \Omega_{X/k}$. To check isomorphism, both are locally free of the same rank, so it suffices to show it is surjective. But on closed pts, pass to Nakayama, this is clearly true, so it is surjective by(6.11.1.13). □

Prop. (9.1.4.36) [Dimension Theorem]. Let $\varphi : G \to H$ be a surjective homomorphism of group varieties, then

$$\dim(G) = \dim(H) + \dim(\ker(\varphi)).$$

⌟

Proof: This is a consequence of(6.6.3.19), as the fiber over any closed pt is isomorphic to a field base change of $\ker(\varphi)$. □

Prop. (9.1.4.37). Every binational homomorphism of a connected affine group varieties is an isomorphism. ⌟

Proof: Such an isomorphism induces a homomorphism $A \to B$ of integral Hopf algebras that is an isomorphism on the fraction field, then it is an isomorphism by(3.11.4.22). □

Def. (9.1.4.38) [Quasi-Central Homomorphisms]. A **quasi-central homomorphism** $\varphi : G' \to G$ of group varieties over k is a homomorphism the kernel of $\varphi(\overline{k})$ is central in $G'(\overline{k})$. ⌟

Prop. (9.1.4.39). If a homomorphism of group varieties $\varphi : G' \to G$ is quasi-central and the kernel of $\mathrm{Lie}(\varphi)$ is central, then $\ker(\varphi) \subset Z(G')$. ⌟

Proof: Cf.[Bruhat-Tits, 2.1]. □

Prop. (9.1.4.40) [1-Dimensional Group Varieties]. Let G be a group variety over a field $k = \overline{k}$, then either $G \cong \mathbb{G}_a$, $\mathbb{G}_m$ or an elliptic curve. ⌟

Proof: Cf.[Sil99]. □

5 Homomorphisms

Prop. (9.1.5.1) [Connected-Étale Sequence]. Cf.[Mil17]P114, [Finite Flat Group Schemes, Tate]Section3.7 and [Mil17b]P117. ⌟

Prop. (9.1.5.2) [Algebraic Subgroups are Closed]. Algebraic subgroups H of an algebraic group G are closed subgroups. In particular, an algebraic subgroup of an affine algebraic group is affine.

WARNING: H must first be an algebraic group, so we can use Chevalley theorem to show it is locally closed. ⌟

Proof: As $H_{k'} \to H$ is a quotient map(6.4.6.3), we can assume k is alg.closed, and also assume H, G are reduced. Now Chevalley shows that the image is a constructible set of G. Then we can consider all on the level of $\overline{k}$ points, because G is Jacobson. Then H contains an open subset of $\overline{H}$ by(4.12.3.17), which implies $H(\overline{k})$ is open in $\overline{H} \cap G(\overline{k})$. Now $\overline{H} \cap G(\overline{k})$ is the closure of $H(\overline{k})$ in $G(\overline{k})$, thus it is also a subgroup of $G(\overline{k})$, and we can consider the coset of $H(\overline{k})$ in $\overline{H} \cap G(\overline{k})$. H is open in $\overline{H}$, and $\overline{H}$ is compact, and also $\overline{H} \cap G(\overline{k})$ is compact because G is Jacobson, so there are only f.m. coset, thus $H(\overline{k})$ is also closed in $\overline{H} \cap G(\overline{k})$, thus H is also closed in $\overline{H}$, so $H = \overline{H}$. **?** Cf.[Mil17]P19. □

Prop. (9.1.5.3) [Characterizating Quotient Maps]. The following conditions on a homomorphism $\varphi : G \to Q$ of algebraic groups are equivalent:

- φ is fully faithful.
- φ is a quotient map(9.1.1.4).
- The homomorphism $\mathcal{O}_Q \to \varphi_* \mathcal{O}_G$ is injective.

⌟

Proof: $1 \to 2$ follows from the very definition of fat subfunctors, as f.f. map is a fppf cover. Cf.[Mil17]P109.**?** □

Prop. (9.1.5.4). Let $\varphi : G \to H$ be a surjective homomorphism of group schemes and H is reduced, then φ is a quotient map. ⌟

Proof: The hypothesis implies $G(\overline{k})$ acts transitively on $H(\overline{k})$, thus φ is faithfully flat by(9.2.1.4). □

Prop. (9.1.5.5) [Check Quotient Map on Closed Points]. Let $\varphi : G \to H$ be a quotient map of locally algebraic groups, then $\varphi : G(\overline{k}) \to H(\overline{k})$ is surjective. The conversely is also true if H is reduced. In particular, if $e \to N \to G \to H \to e$ is an exact sequence, then $e \to N(\overline{k}) \to G(\overline{k}) \to H(\overline{k}) \to e$ is exact.

Moreover, if φ is étale, then $\varphi : G(k^s) \to H(k^s)$ is also surjective. ⌟

Proof: This follows from the fact for any $x \in H(\overline{k})$(resp. k^s), G_x is non-empty and locally algebraic(resp. étale) over $k(x)$, thus has a $\overline{k}$(resp. k^s-point).

For the converse, notice the image of φ has the same $\overline{k}$-points as H, thus it equals H as H is reduced and locally algebraic. □

Prop. (9.1.5.6) [Characterizing Monomorphisms]. For a homomorphism $\varphi : G \to H$ of algebraic groups over k, the following are equivalent:

- φ is a monomorphism.
- $\ker(\varphi) = e$(9.1.1.4).
- φ is a monomorphism in the category of algebraic groups over k.
- φ is a monomorphism in the category of algebraic schemes over k.

Moreover, a monomorphism is just a closed embedding. ⌟

Proof: $1 \to 4 \to 3$ is obvious.

$3 \to 2$: the composition of $\ker(\varphi) \to G$ with φ is trivial, thus $\ker(\varphi)$ is trivial.

$2 \iff 1$: This follows from the definition of $\ker(\varphi)$(9.1.1.4).

For the last assertion, if φ is a closed embedding, then it is a monomorphism in the category of algebraic schemes over k(6.4.4.72). Conversely, if φ is a monomorphism, consider the quotient space $G \to G/H$(9.1.1.21), then by(9.1.1.26), H is the fiber over $o \in G/H$, thus a closed subscheme. □

Def. (9.1.5.7) [Embeddings]. Following(9.1.5.6), define an **embedding of algebraic groups** to be a closed immersion of algebraic groups. ⌟

Isogenies

Def. (9.1.5.8) [Finite Index Subgroups]. An algebraic subgroup H of an algebraic group scheme G is said to have finite index if the quotient G/H is a finite scheme. ⌟

Prop. (9.1.5.9). For any algebraic group G over k, the identity component G^0 is of finite index in G. ⌟

Proof: Notice an algebraic group H is finite iff $\#H(\overline{k}) < \infty$. And $(G/G^0)(\overline{k}) = G(\overline{k})/G^0(\overline{k})$(9.1.4.11) is finite as G is compact. □

Def. (9.1.5.10) [Isogeny]. A homomorphism of algebraic groups $G \to H$ is called an **isogeny** if its kernel is finite and its image is of finite index in H(9.1.5.8). ⌟

Def. (9.1.5.11) [Strongly Connected Groups]. An algebraic group G is called a **strongly connected group** if it has no non-trivial subgroup of finite index. ⌟

Def. (9.1.5.12) [Strongly Identity Components]. The **strongly identity component** G^{s0} of an algebraic group G is defined to be the intersection of the algebraic subgroups of finite index. Thus it is a characteristic subgroup of G. ⌟

Prop. (9.1.5.13). G/G^{s0} is a a finite scheme. In particular, G^{s0} is the smallest algebraic subgroup having the same dimension as G. ⌟

Proof: As G is Noetherian, $G^{s0} = H_1 \cap \ldots H_r$ for G/H_i finite schemes. Thus $G/G^{s0} \hookrightarrow H_1 \cap \ldots H_r$ is a finite scheme. □

Prop. (9.1.5.14)[Strongly Identity Components and Identity Components]. G^{s0} is connected, and the converse is true if G is smooth. In fact, if G is smooth, $G^{s0} = G^0$.

In particular, a group variety has no algebraic subgroup of finite index. Thus an isogeny to a group varieties is surjective(thus a quotient map by(9.1.1.31)). ⌟

Proof: G^{s0} is connected because the identity component is of finite index(9.1.5.9). Conversely, G^0/G^{s0} is smooth and connected and finite(9.1.5.29), thus it is a group variety of dimension0, which is trivial. □

Prop. (9.1.5.15). Let G be an algebraic group over a perfect field k, then $G^0_{\text{red}} = G^{s0}$. ⌟

Proof: Cf.[Mil17]P122. □

Def. (9.1.5.16). A **central/multiplicative isogeny** is an isogeny that the kernel is central/of multiplicative type. ⌟

Prop. (9.1.5.17). Any isogeny with kernel order prime to the characteristic has étalekernel by(9.1.2.4), thus it is central, by(9.1.4.10). ⌟

Prop. (9.1.5.18). Every multiplicative isogeny from a connected algebraic group is central, by(9.2.3.22). ⌟

Def. (9.1.5.19). A composition of multiplicative isogenies is a multiplicative isogeny. ⌟

Proof: This is because there is an exact sequence $e \to \ker(\varphi_1) \to \ker(\varphi_2 \circ \varphi_1) \to \ker(\varphi_2) \to e$, thus $\ker(\varphi_2 \circ \varphi_1)$ is central, hence of multiplicative type by(9.2.3.16). □

Prop. (9.1.5.20) [Isogenies between Group Varieties]. Let $\varphi : G \to H$ be a surjective homomorphism of group varieties, then φ is flat. And if $\dim G = \dim H$, then φ is finite, and the rank of $\ker(\varphi)$ equals the separable degree of $K(G)/K(H)$. ⌟

Proof: φ is flat by(9.2.1.4). By(6.11.3.4), there exists a dense open subscheme U' s.t. $\varphi^{-1}(U') \to U'$ is finite, thus by homogeneity, φ is finite, and rank of $\ker(\varphi)$ is $[K(G) : K(H)]_s$. □

Subnormal Series

Prop. (9.1.5.21) [Solvability]. Let G be an algebraic group that is either affine of smooth, then G is solvable iff $G^{(n)} = e$ for some n large. In particular, for a field extension k'/k, G is solvable iff $G_{k'}$ is solvable. ⌟

Prop. (9.1.5.22) [Nilpotency]. Let G be an algebraic group that is either affine of smooth, then G is nilpotent iff $G^n = e$ for some n large. In particular, for a field extension k'/k, G is solvable iff $G_{k'}$ is solvable.

In particular, if G is a nilpotent and geo.connected, then it contains a non-trivial geo.connected subgroup scheme in its center, by(9.1.4.27). ⌟

Prop. (9.1.5.23). A split solvable algebraic group G is an affine group variety, by(9.1.5.29) and(9.1.5.29). ⌟

Lemma (9.1.5.24). If $G = G_0 \rhd G_1 \rhd \ldots \rhd G_s = \{e\}$ is a subnormal series and $\dim G = \dim G_i/G_{i+1}$ for some i, then $G \sim G_i/G_{i+1}$. ⌟

Proof: The maps $G_i \to G_i/G_{i+1}$ and $G_i \to G_{i-1} \to \ldots \to G_0 = G$ are isogenies(9.1.5.10). □

Def. (9.1.5.25)[Composition Series]. A **composition series of** G is defined to be a maximal object among the subnormal series

$$G = G_0 \rhd G_1 \rhd \ldots \rhd G_s = \{e\}$$

that satisfies $\dim G_0 > \dim G_1 \ldots > \dim G_s$. ⌟

Prop. (9.1.5.26). Any two composition series of an algebraic group G has refinements that the quotients are isogenous. ⌟

Cor. (9.1.5.27) [Jordan-Holder]. ⌟

Maximal Subgroup with Properties

Def. (9.1.5.28)[Good Properties]. A property of algebraic groups is called a **good property** s.t.

- e has P.
- Every extension of groups with property P has P.
- Every quotient of a group with property P has P.

⌟

Prop. (9.1.5.29)[List of Good Properties(Not Complete)].

1. Strongly connectedness.
2. Solvability. Moreover, subgroups of solvable groups are solvable.
3. Smoothness.
4. Unipotency.
5. Affineness.
6. Connectedness.
7. Finiteness. Moreover, subgroups of finite groups are finite.
8. Unipotency. Moreover, subgroups of unipotent groups are unipotent.

⌟

Proof:

1. This follows from the isomorphism and correspondence theorems(9.1.1.33)(9.1.1.34).
2. This follows from standard argument and correspondence theorems(9.1.1.33)(9.1.1.34).
3. Let $e \to N \to G \to H \to e$ be an exact sequence of algebraic groups, then if G is smooth, then so is H by(9.2.1.10) and the fact G/H is geo.reduced by(6.1.5.28) and(9.1.5.3). If N, H are smooth, then so is G by the fact smoothness is stalkwise.
4. Quotient case is clear. If N is a normal subgroup of G s.t. N and G/N are both unipotent, then (for) any non-zero linear representation V of G, $V^N \neq 0$, and V^N is stable under G-actions, thus G/N acts on V^N, thus $V^G = (V^N)^{G/N} \neq 0$.
5. Notice by(9.1.1.27) and(6.1.5.29). $G \to Q$ is affine.
6. Cf.[Mil17]P114.
7. This follows from(9.1.1.28).

8. Cf.[Mil17]P282.

□

Prop. (9.1.5.30) [Maximal Group Variety Exists]. If P is a good property of algebraic groups, then every algebraic group G over k contains a largest normal subgroup variety H with property H. And also G/H has contains no non-trivial such subgroups. ⌟

Proof: G contains at least one normal subgroup variety, namely e. There exists a maximal such one, by taking the one with maximal dimension(because smooth varieties are reduced), then it is the largest, because if H' is another, then HH' is a larger one, by(9.1.5.29) and the fact NH is a quotient of $N \rtimes H$.

And if G/H contains a normal subgroup variety H' that has P, then the inverse image of H' in G is also a normal subgroup variety that has P, contradiction. □

6 Cohomology and Extensions

Cf.[Mil17]Chap15.

9.2 Group Schemes II: Solvable Groups

1 Group Actions

Remark (9.2.1.1). Group action of an group functor on an object is defined in(4.1.1.67). ⌟

Prop. (9.2.1.2) [Group Action]. An action of an algebraic group G on an algebraic group X is equivalent to a right $\Gamma(G)$-comodule structure on $\Gamma(X)$ as $\Gamma(G)$-modules. This action will induce a right comodule structure on $\Gamma(X)$.

The action of G on itself is called the **regular action** of G. ⌟

Prop. (9.2.1.3). Let $\mu : G \times X \to X$ be an action of an group scheme G on a scheme X, then it is faithfully flat, and it is called a smooth/finite/...action if μ is smooth/finite/.. ⌟

Proof: We can see this from the commutative diagram(4.1.1.68). □

Prop. (9.2.1.4) [Image of Equivariant Map]. Let G be a group functor and X, Y be non-empty algebraic schemes on which G acts, and $f : X \to Y$ is an equivariant map.

- If Y is reduced and $G(\bar{k})$ acts transitively on $Y(\bar{k})$, then f is faithfully flat.
- If $G(\bar{k})$ acts transitively on $X(\bar{k})$, then the set $f(|X|)$ is locally closed in $|Y|$, so we can let $f(X)_{\text{red}}$ denote its reduced subscheme structure(6.4.1.14).
- If X is reduced and $G(\bar{k})$ acts transitively on $X(\bar{k})$, then f factors into

$$X \xrightarrow{\text{faithfully flat}} f(X)_{\text{red}} \xrightarrow{\text{immersion}} Y.$$

Moreover, $f(X)_{\text{red}}$ is stable under the action of G.

⌟

Proof: Cf.[Mil17]P26.?

1:

2:

3: f factors through $f(X)_{\text{red}}$ because X is reduced(6.4.1.14). Then the first assertion follows from 1 and 2. The last assertion follows from universal property again. □

Def. (9.2.1.5) [Orbit Map]. Let $\mu : G \times X \to X$ be an action of an algebraic group G on an algebraic scheme X. For any $x \in X(k)$, the **orbit map**

$$\mu_x : G \to X : g \mapsto gx$$

is defined to be the restriction to μ to $G \times \{x\} \cong G$. The image of the orbit map is locally closed in X by(9.2.1.4), and then its reduced structure subscheme is called the **orbit scheme** O_x of x. ⌟

Prop. (9.2.1.6) [Fixed Subscheme]. Let $\mu : G \times X \to X$ be an action of a group functor G on a separated algebraic scheme over k, then the functor

$$\widetilde{X}^G : R \mapsto \{x \in X(R) | \mu(g, x_{R'}) = x_{R'}, \forall R-\text{algebra } R', g \in G(R')\}$$

is representable by a closed subscheme X^G of X, called the **fixed subscheme** of this action. Then it can be seen directly that the formation of fixed subscheme commutes with extension of base fields.
⌟

Proof: An element $x \in X(R)$ defines two functors

$$G(R') \to X(R') : g \mapsto gx_{R'}$$

$$G(R') \to X(R') : g \mapsto x_{R'}$$

which are both natural in R'. Thus we get a map $X(R) \to \mathrm{Hom}(G_R, X_R \times X_R)$ which is also natural in R, thus induce a map $X \mapsto \mathcal{H}om(G, X \times X)$.

Then there is a Cartesian diagram

$$\begin{array}{ccc} \widetilde{X}^G & \longrightarrow & \mathcal{H}om(G, \Delta_X) \\ \downarrow & & \downarrow \text{closed} \\ \widetilde{X} & \longrightarrow & \mathcal{H}om(G, X \times X) \end{array}.$$

The right vertical map is a closed subfunctor by(9.6.1.10), as Δ_X is closed in $X \times X$ because X is separated. Hence $\widetilde{X}^G$ is a closed subfunctor of $\widetilde{X}$, thus represented by a closed subscheme of X, by(9.6.1.3). □

Def. (9.2.1.7) [Isotropy Group]. Let G be a group scheme acting on an algebraic scheme X, and $x \in X(k)$, then the **isotropy group scheme** G_x is defined to be the fiber of the orbit map $\mu_x : G \to X$ over x. ⌟

Prop. (9.2.1.8) [Orbit Map is Faithfully Flat]. Let $\mu : G \times X \to X$ be an action of an algebraic group G on an algebraic scheme X and $x \in X(k)$.

- If X is reduced and $G(\overline{k})$ acts transitively on $X(\overline{k})$, then the orbit map $\mu_x : G \to X$ is faithfully flat.
- If G is reduced, then O_x is stable under G, and the map $\mu_x : G \to O_x$ is faithfully flat. If G is smooth, then O_x is also smooth.

⌟

Proof: 1: this follows from(9.2.1.4).

2: The first statement follows from(9.2.1.4)3, and then $\mathcal{O}_{O_x} \to \mu_{x*}(\mathcal{O}_G)$ is universally injective. Therefore if G is smooth, then $\mathcal{O}_{O_x}$ is geometrically reduced. Then O_x is smooth by(9.2.1.10). □

Def. (9.2.1.9) [Homogenous Space]. A non-empty algebraic scheme X with an action of a group scheme G is called a **homogeneous space** for G if $G(\overline{k})$ acts transitively on $X(\overline{k})$, and for any(some) $x \in X(\overline{k})$, μ_x is faithfully flat (thus surjective). ⌟

Prop. (9.2.1.10) [Smoothness for Homogenous Spaces]. If G is a group scheme and X is a generically geo.reduced G-homogeneous space, then X is smooth. ⌟

Proof: By(6.6.4.21), it has an open dense smooth locus. Now smoothness can be checked after base change to alg.closed field(5.4.2.1), but then because $G(\overline{k})$ acts transitively on itself, thus all the geometric points are smooth. But geometric points are dense in G(6.4.1.26), thus G is smooth. □

<u>**Action of Algebraic Groups**</u>

Prop. (9.2.1.11) [Homogenous Space as Quotients]. Let $\mu : G \times X \to X$ be an action of an algebraic group G on a separated algebraic scheme X over k with a rational point $x \in X(k)$, then (X, x) is a quotient of G by G_x iff the orbit map $\mu_x : G \to X$ is faithfully flat. ⌟

Proof: If (X, x) is a quotient space, then by(9.1.1.22). Conversely, if it is faithfully flat, then clearly $\mu_x(\widetilde{G})$ is a fat subfunctor of $\widetilde{X}$, thus X represents the quotient functor $\widetilde{G}/\widetilde{G}_x$. □

Cor. (9.2.1.12). Let $\mu : G \times X \to X$ be an action of a reduced algebraic group G on a separated algebraic scheme X over k with a rational point $x \in X(k)$, then (O_x, x) is a quotient space of G by G_x. ⌟

Proof: Because G is reduced, $\mu_x : G \to O_x$ is faithfully flat by(9.2.1.8), and O_x is stable under the action of G by(9.2.1.4), thus(9.2.1.11) applies to this case. □

Prop. (9.2.1.13). Let $\mu : G \times X \to X$ be an action of a smooth algebraic group on an algebraic scheme.

- A reduced closed subscheme Y of X is stable under G iff $Y(\overline{k})$ is stable under $G(\overline{k})$.
- Let Y be a locally closed subscheme of X, then if Y is stable under G, then $(\overline{Y})_{\mathrm{red}}$ and $(\overline{Y}\backslash Y)_{\mathrm{red}}$ is also stable under G.

⌟

Proof: 1: Because G is geo.reduced and Y is reduced, $G\times Y$ is reduced(6.4.3.2), thus $\mu : G\times Y \to X$ factors through Y iff $\mu(\overline{k})$ factors through $Y(\overline{k})$.

2: $|\overline{Y}|_{\mathrm{red}}(\overline{k})$ is the closure of $Y(\overline{k})$ in $X(\overline{k})$**?**. So as $G(\overline{k})$ acts continuously on $X(\overline{k})$, if it fixes $Y(\overline{k})$, then it also fixes $(\overline{Y})(\overline{k})$ and $(\overline{Y}\backslash Y)(\overline{k})$, thus we finish by 1. □

Cor. (9.2.1.14). Let G be a smooth algebraic group acting on an algebraic scheme X and let Y be a non-empty locally closed subscheme of X stable under the action of G of the smallest dimension, then it is closed. ⌟

Proof: This is because $\dim Y > \dim(\overline{Y}\backslash Y)_{\mathrm{red}}$(Because irreducible components of $\overline{Y}$ is not contained in $\overline{Y}\backslash Y$). □

Cor. (9.2.1.15)[Orbit Lemma]. Let G be a smooth algebraic group acting on an algebraic group over an alg.closed field k, then every orbit of minimal dimension is closed. ⌟

Proof: If Y is an orbit of minimal dimension, then $(\overline{Y}\backslash Y)_{\mathrm{red}}$ is stable under G and has smaller dimensions. If it is non-zero, then it contains an orbit. □

Prop. (9.2.1.16). A representation (V, ρ) of an algebraic group G induces an action of G on the affine algebraic scheme $V_{\mathfrak{a}}$, and also an action of G on the projective algebraic scheme $\mathbb{P}(V)$. ⌟

Prop. (9.2.1.17). Let $G \times X \to X$ be an action of an affine algebraic group G on an affine algebraic scheme X over k, then there exists a f.d. representation (V, ρ) of G and an equivariant closed embedding $X \hookrightarrow V_{\mathfrak{a}}$. ⌟

Proof: Cf.[Mil17b]P145. □

Def. (9.2.1.18) [Linear Action]. A **linear action** of an algebraic group G on an algebraic scheme X is an action (r, V) s.t. there exists a f.d. linear representation (V, ρ) of G and an equivariant non-degenerate immersion $X \hookrightarrow \mathbb{P}(V)$. ⌟

Prop. (9.2.1.19). If $G \times X \to X$ is a transitive action of an affine algebraic group G on an algebraic variety X that $X(k)$ is non-empty, then this action is linear. ⌟

Proof: Cf.[Mil17b]P145. □

Def. (9.2.1.20) [Grassmannian Variety]. The **Grassmannian variety** $\mathrm{Gra}(n,k)$ is a scheme over $\mathbb{Z}$ defined to be the quotient of $\mathrm{GL}(n)$ by the algebraic subgroup B fixing a subspace of dimension k(9.1.1.21).

The Grassmannian varieties are projective by(9.7.1.16). ⌟

Remark (9.2.1.21). For an explicit construction of $\mathrm{Gra}(n,k)$, Cf.[Sta]089T or [Nit05]P6. ⌟

Def. (9.2.1.22) [Flag Varieties]. The **flag variety** is a scheme over $\mathbb{Z}$ defined to be the quotient of GL_n by the algebraic subgroup B_F fixing a flag F(9.1.1.21).

The flag varieties are projective by(9.7.1.19). ⌟

Prop. (9.2.1.23) [An Algebraic Theorem]. Let F be a local field and X is an algebraic variety over F, then the F-topology makes $X(F)$ into a locally profinite space(because varieties are closed, and use(4.4.4.6)). Let G be a linear algebraic group over F and $G \times X \to X$ is a F-rational map, then $G(F) \times X(F) \to X(F)$ is a continuous action, and this action is constructible(4.12.1.21). ⌟

Proof: Cf.[Bernstein-Zelevinsky, Appendix]. □

Prop. (9.2.1.24) [Projectivity of Quotient Spaces]. How to generally prove that a quotient space is projective**?**. ⌟

2 Lie Algebras of Algebraic Groups

In this subsection, all algebraic groups G is affine over a field k.

Def. (9.2.2.1) [Lie Algebra of an Algebraic Group]. Let k be a field and G a locally algebraic group, then the tangent space at the unit element $e \subset G$ define by(6.6.4.25) is isomorphic to

$$L(G) = \ker(G(k[\varepsilon]) \to G(k)), \varepsilon^2 = 0.$$

as a vector space. For any homomorphism $f : G \to H$, there is a Lie algebra map

$$\mathrm{Lie}(f) : \mathrm{Lie}(G) \to \mathrm{Lie}(H)$$

induced by f.

In particular, if G is affine, it is the set of homomorphisms $\Gamma(G) \to k[\varepsilon]$ that the composition with $k[\varepsilon] \to k$ is the counit map $\varepsilon : \Gamma(G) \to k$(9.1.1.2).

If G is affine, φ maps the augmentation ideal $I_G = \ker(\varepsilon)$ into (ε), and thus is trivial on I_G^2. So φ factors through $\Gamma(G)/I_G^2$. Now $\Gamma(G)/I_G^2 \cong k \oplus I_G/I_G^2$ by(3.11.4.11), so

$$L(G) \cong \mathrm{Hom}_k(I_G/I_G^2, k).$$

And we define $\mathrm{Lie}(G)$ to be $L(G)$.

In general, if R is any k-algebra, then we define $\mathfrak{g}(R) = \ker(G(R[\varepsilon]) \to G(R))$, then similarly

$$\mathfrak{g}(R) = \mathrm{Hom}_R(I_R/I_R^2, R) = \mathrm{Hom}_k(I_G/I_G^2, k) \otimes R = \mathfrak{g} \otimes R.$$

Now $G(R[\varepsilon])$ acts on $\mathfrak{g}(R)$ by inner automorphism, so also does $G(R)$. So we get a homomorphism of algebraic groups

$$\mathrm{Ad} : G \to \mathrm{GL}(\mathfrak{g}).$$

This homomorphism commutes with Lie algebra homomorphism: If $f : G \to H$ is a homomorphism of algebraic groups, then there is a commutative diagram

$$\begin{array}{ccc} G \times \mathfrak{g} & \xrightarrow{(x,X)\mapsto \mathrm{Ad}(x)X} & \mathfrak{g} \\ \downarrow f & & \downarrow \mathrm{Lie}(f) \\ H \times \mathfrak{h} & \xrightarrow{(y,Y)\mapsto \mathrm{Ad}(y)Y} & \mathfrak{h} \end{array}$$

Then we define a Lie bracket on $\mathfrak{g}$ as follows: $[X,Y] = \mathrm{ad}(X)(Y) = \mathrm{Lie}(\mathrm{Ad})(X)(Y)$. Then this is a Lie algebra structure on $\mathfrak{g}$, and it commutes with arbitrary base change. ⌟

Proof: To verify this is truly a Lie algebra, we take a faithful embedding of G into some GL_V (18.5.1.22). Thus it suffices to prove the Lie algebra of GL_V is a Lie algebra. Now for $A, B \in M_n(R)$, pondering the definition shows

$$(1+\delta A)(1+\varepsilon B)(1-\delta A) = 1 + \varepsilon B + \varepsilon\delta[X,Y] \in k[\varepsilon,\delta]/(\varepsilon^2,\delta^2).$$

So in fact $[X,Y] = XY - YX$, so it is truly a Lie algebra.

To show the group structure on $\mathrm{Lie}(G)$ equals the structure on the tangent space, use the Eckmann-Hilton argument, notice the hypothesis is satisfies because both composition is the morphism $\mathrm{Spec}\, k[\varepsilon] \to \mathrm{Spec}(k[\varepsilon] \otimes k[\varepsilon]) \xrightarrow{\varphi} G \times G \xrightarrow{\mu} G$, where $\varphi = (a,b,c,d) : k[\varepsilon] \otimes k[\varepsilon] \xrightarrow{\varphi} G \times G$. □

Cor. (9.2.2.2) [Exponential Map]. As there are natural isomorphisms $\mathfrak{g}(R) \cong \mathfrak{g} \otimes R$, we can write $e^{\varepsilon X}$ the element of $\mathfrak{g}(R) \subset G(R[\varepsilon])$ corresponding to $X \in \mathfrak{g} \times R$. Then $e^{\varepsilon X + \varepsilon Y} = e^{\varepsilon X} e^{\varepsilon Y}$, and by functoriality, for any homomorphism $f : G \to H$,

$$f(e^{\varepsilon X}) = e^{\varepsilon\,\mathrm{Lie}(f)(X)}.$$

Also

$$x \cdot e^{\varepsilon Y} x^{-1} = e^{\varepsilon\,\mathrm{Ad}(x)Y}$$

and also the commutative diagram in(9.2.2.1) means

$$f(e^{\varepsilon X}) = e^{\varepsilon\,\mathrm{Lie}(f)(X)}.$$

⌟

Cor. (9.2.2.3) [Lie algebra commutes with Limits]. It can be seen from the definition that the Lie algebra construction commutes with limits of algebraic groups. In particular it commutes with kernel map. ⌟

Prop. (9.2.2.4). Let $H \subset G$ be algebraic groups s.t. $\mathrm{Lie}(H) = \mathrm{Lie}(G)$. If H is smooth and G is connected, then $H = G$. ⌟

Proof: Recall that $\dim \mathfrak{g} \geq \dim G$, with equality iff G is smooth(9.1.4.5), so the condition forces G to be smooth. Now G is smooth and connected thus irreducible(9.1.4.14) and $\dim G = \dim H$, so $H = G$. □

Cor. (9.2.2.5). Let H_1, H_2 be connected algebraic subgroups of G and $H_1 \cap H_2$ is smooth. If $\mathrm{Lie}(H_1) = \mathrm{Lie}(H_2)$, then $H_1 = H_2$. ⌟

Cor. (9.2.2.6). If G is an algebraic group over a field of characteristic 0, then the connected subgroups of G corresponds 1 to 1 to Lie subalgebras of $\mathrm{Lie}(G)$, because every subgroup is smooth, by(9.1.4.2). ⌟

Cor. (9.2.2.7). Let H_i be a family of smooth algebraic subgroups of an algebraic subgroup G over a field k. If $\mathrm{Lie}(H_i)$ generate $\mathrm{Lie}(G)$ as a Lie algebra, then H_i generates G(9.1.4.26). ⌟

Proof: Let H be the subgroup they generate, then H is smooth(9.1.4.26) and $\mathrm{Lie}(H) = \mathrm{Lie}(G)$, thus $H = G$ by(9.2.2.4). □

Stabilizers, Centers and Centralizers

Prop. (9.2.2.8) [Lie Algebra of Stabilizer]. Let G be an algebraic group and (V, r) be a representation of G, then it induces an action of $\mathfrak{g}$ on W(9.2.2.1). Let $W \subset V$ be a subspace, then the stabilizer $\mathrm{Stab}_G(W)$ is a subgroup of G(18.5.1.3)

$$\mathrm{Lie}(\mathrm{Stab}_G(W)) = \mathrm{Stab}_{\mathfrak{g}}(W).$$

In particular, $\dim(\mathrm{Stab}_G(W)) \leq \dim \mathrm{Stab}_{\mathfrak{g}}(W)$, with equation iff $\mathrm{Stab}_G(W)$ is smooth. ⌟

Proof: By(9.2.2.2),

$$\begin{aligned} X \in \mathrm{Lie}(\mathrm{Stab}_G(W)) &\iff r(e^{\varepsilon X})W[\varepsilon] \subset W[\varepsilon] \\ &\iff e^{\varepsilon \,\mathrm{Lie}(r)(X)} W_R[\varepsilon] \subset W_R[\varepsilon] \\ &\iff (1 + \varepsilon \,\mathrm{Lie}(r)(X))(W_R + \varepsilon W_R) \subset (W_R + \varepsilon W_R) \\ &\iff \mathrm{Lie}(r)(X)(W_R) \subset W_R \\ &\iff X \subset \mathrm{Stab}_{\mathfrak{g}}(W) \end{aligned}$$

□

Prop. (9.2.2.9) [Lie Algebra of Center]. Let G be a smooth connected algebraic group, then

$$\dim z(\mathfrak{g}) \geq \dim Z(G),$$

and if equality holds, then $Z(G)$ is smooth and $\mathrm{Lie}(Z(G)) = z(\mathfrak{g})$. ⌟

Proof: There are maps

$$\mathrm{Ad} : G \mapsto GL_{\mathfrak{g}}, Z(G) \subset \ker(\mathrm{Ad}),$$

$$\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}_{\mathfrak{g}}, \ker(\mathrm{ad}) = z(\mathfrak{g}).$$

Because Lie algebra commutes with kernel(9.2.2.3), $\mathrm{Lie}(Z(G)) \subset \mathrm{Lie}(\ker(\mathrm{Ad})) = \ker(\mathrm{ad})$. So

$$\dim z(\mathfrak{g}) = \dim \ker(\mathrm{ad}) = \dim \mathrm{Lie}(\ker(\mathrm{Ad})) \geq \dim \ker(\mathrm{Ad}) \geq \dim Z(G)$$

with equality iff $\ker(\mathrm{Ad})$ is smooth and $\dim \ker(\mathrm{Ad}) = \dim Z(G)$ and thus $\ker(\mathrm{Ad})^0 = Z(G)^0$, so $Z(G)$ is also smooth. Finally, $\mathrm{Lie}(Z(G)) \subset z(\mathfrak{g})$, so they are equal if they have the same dimensions. □

Prop. (9.2.2.10)[Lie Algebra of Centralizer]. Let G be an algebraic group and H a subgroup, then H acts on $\mathfrak{g}$ by Ad. Then

$$\operatorname{Lie}(C_G(H)) = \mathfrak{g}^H, \quad \operatorname{Lie}(N_G(H))/\operatorname{Lie}(H) = (\operatorname{Lie}(G)/\operatorname{Lie}(H))^H.$$

⌟

Proof:

$$X \in \operatorname{Lie}(C_G(H)) \iff x(e^{\varepsilon X})_S x^{-1} = e^{\varepsilon X}_S, \quad \forall k[\varepsilon] \to S, x \in H(S)$$

$$X \in \mathfrak{g}^H \iff y e^{\varepsilon X_R} y^{-1} = e^{\varepsilon X_R}, \quad \forall k \to R, x \in H(R)$$

And it can be shown these two are equal. Similarly, there is a natural map $\operatorname{Lie}(N_G(H)) \to \operatorname{Lie}(G)/\operatorname{Lie}(H)$, and the image lies in the fixed subgroup of H, because

$$X \in \operatorname{Lie}(N_G(H)) \iff (e^{\varepsilon X})_S x (e^{\varepsilon X})^{-1}_S \subset H(S) \iff e^{\varepsilon \operatorname{ad}(x) X_S} \in H(S) e^{\varepsilon X_S}, \quad \forall k[\varepsilon] \to S, x \in H(S)$$

$$X \in (\operatorname{Lie}(G)/\operatorname{Lie}(H))^H \iff e^{\varepsilon \operatorname{ad}(x) X_R} \subset e^{\varepsilon (X_R + \operatorname{Lie}(H)(R))}, \quad \forall k \to R, x \in H(R)$$

Then it can be shown that X satisfies condition in 1 iff $\overline{X}$ satisfies condition in 2, thus we are done. □

3 Groups of Multiplicative Type

Throughout this subsection, G is an affine(linear) algebraic group over a field k.

Diagonalizable Groups

Def. (9.2.3.1)[Diagonalizable Groups]. An algebraic group G is called **diagonalizable** if the group-like elements in $\Gamma(G)$ generate $\Gamma(G)$ as a k-vector space. ⌟

Prop. (9.2.3.2). An algebraic group G is diagonalizable iff it is isomorphic to the the algebraic group corresponding to a group algebra $D(M)$ for some commutative group M. ⌟

Proof: For the group algebra $D(M)$, its group-like elements are just $\{m | m \in M\}$ by(3.11.4.19), and they clearly span $D(M)$. Conversely, if the set M of group-like elements in $\Gamma(G)$ spans $\Gamma(G)$, then by(3.11.4.18) they form a basis of $\Gamma(G)$, so there is an isomorphism of vector spaces $D(M) \to \Gamma(G)$. But this is also a homomorphism, because they are on a basis. □

Cor. (9.2.3.3) [Diagonalizable Groups].

- The functor $M \mapsto D(M)$ is a contravariant equivalence from $\mathcal{CA}\mathrm{lg}_k^{fg}$ to the category of diagonalizable algebraic groups, with inverse give by $G \mapsto X(G)$.
- This functor preserves exact sequences.
- Algebraic subgroups and quotient groups of diagonalizable groups are diagonalizable.

⌟

Proof: 1: By(9.2.3.2), it suffices to show that $\operatorname{Hom}(M, M') \to \operatorname{Hom}(D(M'), D(M))$ is an isomorphism. Because D sends direct sums to direct products, it suffices to check the case that M, M' is cyclic. This is easy to check, just notice that a group homomorphism maps group-like elements to group-like elements.

2: If $M' \to M$ is injective, then $k[M'] \to k[M]$ is injective, thus faithfully flat by(3.11.4.21), and $D(M) \to D(M')$ is a quotient map. Conversely, $D(M) \to D(M')$ is a quotient map iff $k[M'] \to k[M]$ is faithfully flat thus injective thus $M' \to M$ is injective. Now the kernel of $D(M) \to D(M')$ is represented by $k[M]/I_{k[M']}$, where $I_{k[M']}$ is the augmentation ideal. Then it is isomorphic to $k[M/M']$.

3: Let H be an algebraic subgroup of G, then the map $\Gamma(G) \to \Gamma(H)$ is surjective, and sends group-like elements to group-like elements, thus $\Gamma(H)$ is also spaned by group-like elements, and H is diagonalizable.

if $D(M) \to Q$ is a quotient map, then its kernel is an algebraic subgroup thus equals $D(M'')$ for some quotient M'' of M. Let M be the kernel of $M \to M''$, then $D(M) \to D(M')$ and $D(M) \to Q$ are quotient maps with the same kernel, so they are isomorphic, by(9.1.1.24). □

Prop. (9.2.3.4) [Representation of Diagonalizable Groups]. The following conditions are equivalent for an algebraic group G over a field k:

1. G is diagonalizable.
2. Every representation of G is diagonalizable.
3. Every f.d. representation of G is diagonalizable.

⌟

Proof: 1 → 2: We need to show for any comodule $\rho : V \to V \otimes \Gamma(G)$, V is a sum of 1-dimensional representations, or equivalently, it is spanned by vectors u that $\rho(u) \in ku \otimes \Gamma(G)$. Let $v \in V$, we can write $\rho(v) = \sum u_i \otimes e_i$ where e_i are group-like in G.

Applying comodule relations, we get

$$\sum u_i \otimes e_i \otimes e_i = \sum \rho(u_i) \otimes e_i, \quad v = \sum u_i (3.11.4.17).$$

so $\rho(u_i) = u_i \otimes e_i$ and they span V.

2 → 1: The regular representation of G is diagonalizable, so $\Gamma(G)$ is spanned by its eigenvectors, for any eigenvector $f \in \Gamma(G)$, so $\mu(f) = f \otimes e$ where e is group-like. Applying $\varepsilon \otimes \mathrm{id}$ shows $f = \varepsilon(f)e$, so G is diagonalizable.

2 → 3: trivial.

3 → 2: Every representation of G is a sum of f.d. representation, so it is a sum of 1-dimensional representations, so it is diagonalizable by(18.5.1.17). □

Tori

Def. (9.2.3.5) [Linear Tori]. Let k be a field, then a **split torus** over k is a linear group scheme of the form $T = \mathbb{G}_{m,k}^n$, and a **linear torus** over k is defined to be a linear algebraic group T over k that $T_{\overline{k}}$ is a split torus over $\overline{k}$. ⌟

Prop. (9.2.3.6). By(9.2.3.3), a split torus is just $D(\mathbb{Z}^n)$ for some n, and quotient of a split torus is a split torus.

Thus a quotient of a torus is a torus, and an algebraic subgroup of a torus is a torus iff it is a group variety. ⌟

Prop. (9.2.3.7). Any torus over a separably closed field is a split torus. in particular, any torus split over a finite separable extension. ⌟

Proof:

□

Def. (9.2.3.8) [Quasi-Split Tori]. Let A be a f.d. separable k-algebra, then there is a linear algebraic group G defined by $G(B)=G_m(A\otimes_k B)=(A\otimes_k B)^*$, denoted by $\mathrm{res}_{A/k}\mathbb{G}_m$.

This is a linear algebraic group because if we choose a basis $\{v_1,\ldots,v_r\}$ of A over k, which induces a ring homomorphism $\varphi:A\to M_r(k)$. Then $f=\det(\varphi(x_1v_1+\ldots+x_rv_r))$ is a polynomial in $x_1,\ldots,x_r$. Thus $G(B)$ is the set of points in $\mathbb{A}^r(B)$ that $f(x_1,\ldots,x_r)$ is invertible in B. So G is a linear algebraic variety. Moreover, as A is separable, $A\otimes_k\overline{k}\cong\oplus_{i=1}^r M_{n_i}(\overline{k})$, so $G_{\overline{k}}\cong\mathbb{G}^r_{m,\overline{k}}$, so G is a torus, called a **quasi-split torus** over k. ⌟

Def. (9.2.3.9) [Monoidal Transformation]. For a matrix $A\in SL(n,\mathbb{Z})$ with $\det A=\pm1$, we define an isomorphism of $\mathbb{G}_{n,k}$:

$$\varphi_A(x)=(x_1^{a_{11}}x_2^{a_{12}}\ldots x_n^{a_{1n}},\ldots,x_1^{a_{n1}}\ldots x_n^{a_{nn}}).$$

these isomorphisms φ_A is called the **monoidal transformations**. ⌟

Prop. (9.2.3.10). Let G be a group variety over k and T a central torus, then

- $T\cap[G,G]$ is finite.
- If G/T is perfect, then the sequence

$$e\to T\cap[G,G]\to T\times[G,G]\to G\to e$$

  is exact.

In particular, $G/[G,G]$ is a torus. ⌟

Proof: Cf.[Mil17]P246. □

Groups of Multiplicative Type

Def. (9.2.3.11) [Groups of Multiplicative Type]. An **algebraic group of multiplicative type** over a field k is an algebraic group G that G_K is diagonalizable over K for some field K containing k.

Subgroups and quotient groups of groups of multiplicative type are also of multiplicative type, because this is true for diagonalizable groups(9.2.3.3). ⌟

Prop. (9.2.3.12) [Characterization of Groups of Multiplicative Type]. The follows are equivalent for an algebraic group G over k:

- G is of multiplicative type.
- G is commutative and $\mathrm{Hom}(G,\mathbb{G}_a)=0$.
- G is commutative and $\Gamma(G)$ is coétale.
- G becomes diagonalizable over k^s.

⌟

Proof: Cf.[Mil17]237. □

Cor. (9.2.3.13). An algebraic group over k becomes diagonalizable over some field extension of k iff it becomes diagonalizable over some finite separable extension of k. ⌟

Cor. (9.2.3.14). If a group of multiplicative type splits over a purely inseparable extension of k, then it splits over k. ⌟

Proof: Cf.[Mil17]P238. □

Cor. (9.2.3.15). A smooth commutative algebraic group G over k is of multiplicative type iff $G(\overline{k})$ consists of semisimple elements. ⌟

Proof: We can assume that $k = \overline{k}$, and embed G into GL_n for some n(18.5.1.22). If G is of multiplicative type, then by(9.2.3.4), there is a basis that $G \subset \mathbb{D}_n$, so all the elements in $G(k)$ is diagonalizable hence semisimple. Conversely, if $G(k)$ are all semisimple, then they form a commutative family of semisimple elements, so $G(k) \subset \mathbb{D}_n(k)$ in some basis. Because G is smooth thus reduced, $G \subset \mathbb{D}_n$. □

Cor. (9.2.3.16). An extension of algebraic groups of multiplicative type is of multiplicative type iff it is commutative. ⌟

Proof: A exact sequence $e \to G' \to G \to G'' \to e$ of commutative group schemes gives rise to an exact sequence

$$0 \to \mathrm{Hom}(G'', \mathbb{G}_a) \to \mathrm{Hom}(G, \mathbb{G}_a) \to \mathrm{Hom}(G', \mathbb{G}_a)$$

of Abelian groups by(9.1.1.24), thus we can use characterization(9.2.3.12). □

Prop. (9.2.3.17) [Largest Subtorus]. Cf.[Mil17]P241. ⌟

Prop. (9.2.3.18) [Representation of Groups of Multiplicative Type]. Let G be an algebraic group over k, then $\mathrm{Rep}(G)$ is a semisimple Abelian category, and the isomorphism classes of simple objects in $\mathrm{Rep}(G)$ are classified by the orbits of Gal_k acting on $X^*(G)$.

Let (V, r) be a representation corresponding to an orbit Σ, and let $\chi \in \Sigma$, then $\mathrm{End}(V, r) \cong k_\chi$, where k_χ is the subfield of k^s fixed by the subgroup of Gal_k fixing χ. ⌟

Proof: The group G is split by a finite Galois extension K/k by(9.2.3.13). Let $\overline{\Gamma} = G(K/k)$, then $\overline{\Gamma}$ acts on $\Gamma(G_K)$ through its action on K. Let (V, r) be a representation of G_K and let ρ be the corresponding co-action, then by(6.1.5.24), the functor $V \mapsto V \otimes_k K$ induces an equivalence between $\mathrm{Rep}(G)$ and $\mathrm{Rep}(G_K)$ with a semi-linear action of $\overline{\Gamma}$ fixing ρ.

Let V be a representation of G over k, then $K \otimes V$ decomposes as a representation of G_K into

$$K \otimes V = \oplus_{\chi \in X(G_K)} V_\chi.$$

and an element $\gamma \in \overline{\Gamma}$ maps V_χ isomorphically onto $V_{\sigma\chi}$. Thus the set of χ occurring in $K \otimes V$ is stable under the action of $\overline{\Gamma}$.

Conversely, if Σ is an orbit of $\overline{\Gamma}$ in $X(G_K)$ and V is a 1-dimensional K vector space, then $\oplus_{\chi \in \Sigma} V_\chi$ has a natural semi-linear action of $\overline{\Gamma}$, so it arises from a simple representation of G over k. □

Prop. (9.2.3.19) [Density Theorem for Groups of Multiplicative Type]. Let G be a smooth algebraic group of multiplicative type, thus G is commutative. Let G_n be the kernel of multiplication by n on G.

- The only closed subscheme containing every G_n is G itself.
- If G is smooth, then the only closed subscheme containing G_n for n prime to characteristic of k, is G itself.

⌟

Proof: 1: 2: Cf.[Mil17]P242.**?** □

Cor. (9.2.3.20). Let G be an algebraic group of multiplicative type. If two homomorphisms from G to another algebraic group H coincides on G_n for all $n \geq 1$, then they are equal. ⌟

Proof: This is because the equalizer is a closed subscheme of G, as H is separated(9.1.1.12). □

Prop. (9.2.3.21) [Rigidity Theorem for Groups of Multiplicative Type]. Let G, H be diagonalizable groups over k, and let X be a connected group scheme over k. Let $\varphi : X \times G \to H$ be a morphism that for all k-algebra R and $x \in X(R)$, the map $g \mapsto \varphi(x, g) : G(R) \to H(R)$ is a homomorphism. Then for any $x_0 \in X(k)$, we have $\varphi(x, g) = \varphi(x_0, g)$ for any k-algebra R and $(x, g) \in X(R) \times G(R)$. ⌟

Proof: Cf.[Mil17]P243.**?** □

Cor. (9.2.3.22). Every action of a connected algebraic group G on an algebraic group H of multiplicative type by group homomorphisms is trivial. ⌟

Cor. (9.2.3.23). Every normal algebraic subgroup of multiplicative type of a connected algebraic group G is contained in the center of G. ⌟

Proof: The action of G on N by inner automorphism is trivial. □

Cor. (9.2.3.24). Let H be a subgroup of multiplicative type of an algebraic group G, then $N_G(H)^0 = C_G(H)$, i.e. $C_G(H)$ is an open subgroup of $N_G(H)$. ⌟

Proof: The inner action of $N_G(H)^0$ on H by inner automorphism is trivial. □

Cor. (9.2.3.25). If N is a normal subgroup of an algebraic group H that N and H/N are of multiplicative type, then every action of a connected algebraic group G on H by group homomorphisms preserving N is trivial. ⌟

Proof: The action of G on N is trivial, thus the action factors through $G \times H/N \to H$, thus also factors through $G \times H/N \to N$. Now the action is trivial, by(9.2.3.21). □

Cor. (9.2.3.26). An extension of algebraic groups of multiplicative type is of multiplicative type if it is connected. ⌟

Proof: The adjoint action of G is trivial, by(9.2.3.25), thus G is commutative. Thus it is of multiplicative type by(9.2.3.16). □

4 Actions of Tori

Prop. (9.2.4.1) [Białynicki-Birula Decomposition]. Cf.[Mil17]P272. ⌟

5 Solvable Groups

All group schemes G in this subsection are affine and algebraic over a field k.

Prop. (9.2.5.1). Let H be an algebraic group of a solvable group variety G, then G/H doesn't contain a proper subscheme of dimension> 0. In particular, $G = H$ if G/H is proper. ⌟

Proof: Cf.[Mil17]P353. □

Cor. (9.2.5.2). If G is a solvable group variety acting on a separated algebraic scheme X over k, then no orbits of X contains a proper subscheme of dimension> 0. ⌟

Proof: By(9.2.1.12), the orbits are quotients of G. □

Cor. (9.2.5.3) [Borel Fixed Point Theorem]. If G is a solvable group variety acting on a proper algebraic scheme X over k, then $X^G \neq \varnothing$, in particular, $X^G(\overline{k}) \neq \varnothing$. ⌟

Proof: It suffices to change to $\overline{k}$, then by(9.2.1.15) X has a closed orbit, which is then proper, thus must be a point. □

Triangularizable Algebraic Groups

Def. (9.2.5.4) [Triangularizable Algebraic Groups]. A **triangularizable algebraic group** is an algebraic group s.t. every simple representation has dimension 1. Equivalently, for any f.d. linear representation V of G, there exists a basis that G is mapped into $\mathbb{B}(n)$. ⌟

Prop. (9.2.5.5) [Lie-Kolchin]. Let G be a solvable group variety over an alg.closed field k, then G is triangularizable. In particular, any solvable group variety over k is a triangularizable after a finite field extension. ⌟

Proof: Let (V, r) be any linear representation of G, then G acts on the maximal flag variety of V. Thus by Borel's fixed point theorem(9.2.5.3), there is a flag in V that is fixed by G, which means G is mapped into $\mathbb{U}(V)$. □

Nilpotent Algebraic Groups

9.3 Group Theory III: Reductive Groups

All group schemes G in this section are assumed to be linear algebraic over a base scheme S.

Main references are [Mil17]. For relative reductive group schemes, Cf.[reductive group schemes, Conrad].

1 Borel Subgroups

Def. (9.3.1.1) [Borel Subgroups]. A **Borel subgroup** of a group variety G is a maximal solvable subgroup variety of G. A **Borel pair** is a pair (B, T) where B is a Borel subgroup of G and T is a maximal torus of G contained in B. ⌟

Def. (9.3.1.2) [Parabolic Subgroups]. A **parabolic subgroup** P of a group variety G is a subgroup variety s.t. G/P is proper. ⌟

Prop. (9.3.1.3) [Parabolic and Borel]. Parabolic subgroups are exactly those containing a Borel subgroup. In particular, if B be a Borel subgroup of G, then G/B is proper. ⌟

Proof: Cf.[Mil17]P354, P356.**?** □

Prop. (9.3.1.4) [Characterizing Borel Subgroups]. Let G be a group variety over k, then a subgroup B is Borel iff it is solvable and G/B is proper. ⌟

Prop. (9.3.1.5) [Borel Pairs are Conjugate]. Let G be a group variety over k, then

- Any two Borel subgroups of G are conjugate by an element of $G(k)$.
- Any two maximal tori of G are conjugate by an element of $G(k)$.
- Any two Borel pairs are conjugate by an element of $G(k)$.

⌟

Proof: Cf.[Mil17]P354.**?**

3: This follows from the first two(by applying item2 on a Borel subgroup B). □

Def. (9.3.1.6) [Split Group Variety]. A **split group variety** is a group variety whose Borel subgroup is split solvable. ⌟

Def. (9.3.1.7) [Cartan Subgroup]. A **Cartan subgroup** of a group variety is the centralizer of a maximal tori. ⌟

2 Geometric Aspects

Def. (9.3.2.1) [Simply Connected Groups]. A **simply-connected group variety** is a group variety G that every multiplicative isogeny(9.1.5.16) from a group variety $G' \to G$ is an isomorphism. ⌟

Prop. (9.3.2.2) [Lifting]. Let G be a simply connected group variety over k and $\varphi : G' \to G$ is a multiplicative isogeny, then φ admits a section if k is perfect or G is a perfect group. ⌟

Proof: Cf.[Mil17]P388. □

Def. (9.3.2.3) [Universal Covering]. A **universal covering** of a group variety G is a multiplicative isogeny $\pi : G' \to G$ from a simply connected group variety G'. If such a covering exists, $\ker \pi$ is called the **fundamental group** $\pi_1(G)$ of G. ⌟

Prop. (9.3.2.4) [Galois Theory]. Let $\pi : \widetilde{G} \to G$ be a universal covering of a group variety over k. If k is perfect or G is perfect, then π factors uniquely through any other multiplicative isogeny of group varieties $G' \to G$. ⌟

Proof: As $\widetilde{G}$ is a group variety, it admits no finite quotient(9.1.5.14), thus if $[G,G] = G$, then $[\overline{G},\overline{G}]\ker\pi = \overline{G}$, thus $G/[G,G]$ is finite, thus trivial, so $\widetilde{G}$ is also perfect.

The map $G' \times_G \widetilde{G}$ is surjective with finite kernel of multiplicative type, thus it has a section by(9.3.2.2), and the composite of this section with projection to G' is the desired lifting. If α,β are two liftings, then α/β is a map from $\widetilde{G}$ to $\ker(\varphi)$, which is finite, thus $\alpha = \beta$. □

Prop. (9.3.2.5). Every semisimple algebraic group admits an essentially unique isogeny $\widetilde{G} \to G$ that $\widetilde{G}$ is simply connected. ⌟

Proof: □

3 Reductive Groups

In this subsection, k is a field.

Linearly Reductive Groups

Def. (9.3.3.1) [Linearly Reductive Groups]. An algebraic group over a field is called **linearly reductive** if every f.d. representation of G is semisimple. ⌟

Prop. (9.3.3.2). Let G be an algebraic group over k, and k' a field containing k. If $G_{k'}$ is linearly reductive, then so is G. Conversely, if G is linearly reductive and k' is separable over k, then $G_{k'}$ is linearly reductive. ⌟

Proof: Cf.[Mil17]P248. □

Prop. (9.3.3.3). A commutative algebraic group is linearly reductive iff it is of multiplicative type. ⌟

Proof: Cf.[Mil17]P248. ? □

Prop. (9.3.3.4) [Hilbert]. Let G be a linearly reductive group of $\mathrm{GL}(n)$ and let $A = k[T_1,\ldots,T_n]$, then A^G is f.g. as a k-algebra. ⌟

Proof: Cf.[Mil17]P249. ? □

Semisimple Groups

Def. (9.3.3.5) [Radicals]. The **radical** $R(G)$ of an algebraic group G over a field k is the largest smooth connected solvable normal subgroup of G, which exists by(9.1.5.29) and(9.1.5.30).

G is called a **semisimple algebraic group** iff it is an affine group variety and $R(G_{\overline{k}}) = e$. ⌟

Prop. (9.3.3.6). Let k'/k be a field extension, then an algebraic group G over k is semisimple iff $G_{k'}$ is semisimple. ⌟

Proof: Affineness, Smoothness and geo.connectedness satisfies field descent by(6.1.5.26), so it suffices to prove for k',k alg.closed. But if N is non-trivial normal solvable subgorup variety of $G_{k'}$, it is defined on a f.g. field extension $K = k(x_1,\ldots,x_n)$ of k, thus N_K is a normal solvable subgroup variety of G_K, and they extends to smooth group varieties $\mathcal{G}$ and $\mathcal{N}$ on some open subscheme $\operatorname{Spec} A \subset \operatorname{Spec} k[x_1,\ldots,x_n]$. But on some maximal ideal $\mathfrak{m}$, $\mathcal{N}_{k(\mathfrak{m})}$ is non-zero(5.2.6.11) normal open subgroup of $\mathcal{G}_{k(\mathfrak{m})}$, and $k(\mathfrak{m}) \cong k$ as $k = \overline{k}$, contradiction. □

Prop. (9.3.3.7). If k'/k is a separable algebraic extension, then $R(G_{k'}) = R(G)_{k'}$. ⌟

Proof: $R(G)_{k'} \subset R(G_{k'})$ by definition, and it suffices to prove they are the same when k'/k is Galois. But then this follows from Galois descent(6.1.5.19) and the fact connectedness, smoothness, normality and solvability is reflexive(9.1.5.21). □

Cor. (9.3.3.8). Let G be a group variety over a perfect field k, then G is semisimple iff $R(G) = e$. In particular, $G/R(G)$ is semisimple, by(9.1.5.30). ⌟

Cor. (9.3.3.9). Let G be a group variety over a perfect field k, then G is semisimple iff it contains no non-trivial commutative normal subgroup varieties. ⌟

Def. (9.3.3.10)[Simple Groups]. A **simple algebraic group** is a semisimple non-commutative group with no non-trivial normal algebraic subgroups.

An **almost-simple algebraic group** is a semisimple non-commutative group s.t. every non-trivial normal algebraic subgroup is finite.

A **geometrically (almost-)simple algebraic group** is an algebraic group G s.t. $G_{\overline{k}}$ is (almost-)simple.

A(n) **(almost-)pseudo simple algebraic group** is a non-commutative group variety G s.t. every non-trivial normal algebraic subgroup is trivial(finite). (May not by semisimple). ⌟

Reductive Groups

Def. (9.3.3.11)[Unipotent Radicals]. By(9.1.5.29) and(9.1.5.30), any algebraic group G has a maximal connected smooth normal unipotent subgroup $R_u(G)$, which is called the **unipotent radical** of G, denoted by $R_u(G)$.

Let G be an affine group variety over k, then G is called a **reductive group** iff $R_u(G_{\overline{k}}) = e$.

G is called a **pseudo-reductive group** if $R_u(G) = e$. ⌟

Prop. (9.3.3.12). Let k'/k be a field extension, then an algebraic group G over k is reductive iff $G_{k'}$ is reductive. ⌟

Proof: The proof is verbatim as that of(9.3.3.6). □

Prop. (9.3.3.13). If k'/k is a separable algebraic extension, then $R_u(G_{k'}) = R_u(G)_{k'}$. ⌟

Proof: $R(G)_{k'} \subset R(G_{k'})$ by definition, and it suffices to prove they are the same when k'/k is Galois. But then this follows from Galois descent(6.1.5.19) and the fact connectedness, smoothness, normality and unipotency is reflexive(18.5.3.2). □

Cor. (9.3.3.14). Let G be a group variety over a perfect field k, then G is reductive iff $R_u(G) = e$. In particular, $G/R_u(G)$ is reductive, by(9.1.5.30). ⌟

Prop. (9.3.3.15). Let G be a reductive group, then

- the center $Z(G)$ is of multiplicative type.
- $R(G)$ is the largest subtorus of $Z(G)$.
- $R(G_{k'}) = R(G)_{k'}$ for any field extension k'/k.
- $G/R(G)$ is semisimple.
- $G/Z(G)$ has trivial center.

- $Z(G) \cap [G, G]$ is finite.

⌟

Proof: Cf.[Mil17]P372.
4: This is because $(G/R(G))_{k'} = G_{k'}/R(G)_{k'} = G_{k'}/R(G_{k'})$ is semisimple.
5: Cf.[Mil17]P402. □

Cor. (9.3.3.16). Central and multiplicative isogenies from a group variety are the same thing, by(9.1.5.18). ⌟

Prop. (9.3.3.17) [Reductive Groups and Semisimple Groups]. A semisimple group is reductive, because $R_u(G) \subset R(G)$ as a unipotent group is solvable. Conversely, if G is a reductive group, then the following are equivalent:

- G is semisimple.
- $R(G) = e$.
- $Z(G)$ is finite.
- $G/[G, G]$ is finite.

⌟

Proof: 1 $\iff$ 2 follows from(9.3.3.15).
2 $\iff$ 3: As $R(G)$ is the maximal subtorus of the group $Z(G)$ of multiplicative type, $Z(G)/R(G)$ is finite(9.2.3.17). So if $R(G) = e$, $Z(G)$ is finite. And if $Z(G)$ is finite, $R(G) = e$ because it is a torus. □

Prop. (9.3.3.18). Let G be a group variety over a field k, then if G is reductive, then every commutative normal subgroup variety of G is a torus, and the converse is also true if k is perfect. ⌟

Proof: If N is a commutative normal subgroup variety of G, then $N \subset R(G)$, which is a torus by(9.3.3.15) and(9.2.3.6). The converse follows from the fact $R_u(G) = e$ because $\mathrm{U}(n)$ has no non-zero subtorus by(9.3.5.4). □

Prop. (9.3.3.19). If G is reductive, then $[G, G]$ is semisimple of rank equal to the semisimple rank of G. ⌟

Proof: Cf.[Mil17]P402. □

Prop. (9.3.3.20) [Maximal Central Torus]. If G is a reductive group over a perfect field k, then $R(G) = Z(G)^0_{\mathrm{red}}$, which is the maximal central torus by(9.3.3.21). In particular, G is semisimple if and only if $Z(G)$ is finite. ⌟

Proof: □

Prop. (9.3.3.21). Any commutative affine group variety G is of the form $U \times T$ where U is unipotent and T is a torus. ⌟

Proof: ? □

Prop. (9.3.3.22). Let $\varphi : G' \to G$ be an isogeny of group varieties. If G is reductive or semisimple, then so is G'. ⌟

Proof: It suffices to assume $k = \overline{k}$. Let U be a normal unipotent/solvable subgroup variety of G, then $\varphi(U)$ is also a unipotent/solvable group variety by(9.1.5.29), and it is normal because φ is a quotient map(9.1.5.29). Thus $\varphi(U) = e$, which implies U is a finite group variety, thus trivial. □

Prop. (9.3.3.23) [Matsushima's Criterion]. If G is a reductive group and H a smooth algebraic subgroup, then G/H is affine iff H^0 is reductive. ⌟

Proof: Cf. [Borel, On affine algebraic homogeneous spaces]. □

Def. (9.3.3.24) [Ranks]. The **rank of a group variety** G over k is the dimension of the maximal torus in $G_{\overline{k}}$. The **semisimple rank** is the rank of $G_{\overline{k}}/R(G_{\overline{k}})$.

The **k-rank** is the dimension of a maximal split torus in G. The **semisimple k-rank** of G is is k-rank of $G/R(G)$.

These are well-defined by(9.3.1.5). ⌟

Prop. (9.3.3.25). Let G be a reductive group, then the semisimple rank of G equals $\dim G - \dim Z(G)$. ⌟

Proof: Cf.[Mil17]P402. □

Parabolic Subgroups of Reductive Groups

Prop. (9.3.3.26)[Levi Factors]. Let P be a group variety over k, a **Levi subgroup** of P is a subgroup variety L of P s.t. $L_{\overline{k}} \to P_{\overline{k}}/R_u(P_{\overline{k}})$ is an isomorphism. In other words, L is a reductive subgroup of P s.t. $P_{\overline{k}} = R_u(P_{\overline{k}}) \ltimes L_{\overline{k}}$. ⌟

Prop. (9.3.3.27). Let P be a parabolic subgroup of a reductive group G, then P has Levi subgroups, and any two Levi subgroups of P are conjugate by a unique element of $R_u(P)(k)$. ⌟

Proof: Cf.[Mil17]P559. □

4 Split Reductive Groups

Def. (9.3.4.1) [Split Reductive Groups]. For $k \in \texttt{Field}$, a **split reductive pair** is a pair (G, T) where G is a reductive group over k and T is a split maximal torus. A reductive group is called **split reductive** if it is contained in some reductive pair. By(9.2.3.7), any reductive group is reductive after a finite separable change of fields. ⌟

Def. (9.3.4.2) [Anisotropic Reductive Groups]. For $k \in \texttt{Field}$, a reductive group is isotropic if it contains a non-central split torus; otherwise, it is anisotropic. Notice for semisimple groups, any split torus is central**?**. ⌟

Reductive Groups of Semisimple Rank≤ 1

Prop. (9.3.4.3) [Classifying Reductive Groups of Semisimple Rank$\leq$ 1]. Any reductive group over k of semisimple rank 1 is isomorphic to exactly one of the groups

$$\mathbb{G}_m^r \times \mathrm{SL}(2), \quad \mathbb{G}_m^r \times \mathrm{PGL}(2), \quad \mathbb{G}_m^r \times \mathrm{PGL}(2), \quad r \in \mathbb{N}.$$

⌟

Proof: Cf.[Mil17]P419. □

5 Classical Groups

Def. (9.3.5.1) [Examples of Classical Groups].

- the **general linear group** $\mathrm{GL}(n) = \mathbb{Z}[T_{ij}][1/\det]$ representing the group functor $\mathcal{CA}\mathrm{lg}_{\mathbb{Z}} \to \mathcal{G}\mathrm{rp} : R \mapsto GL(n,R)$.
- the **multiplicative group** $\mathbb{G}_m = \mathrm{Spec}\,\mathbb{Z}[T,T^{-1}]$, which is just GL(1).
- the **special linear group** $\mathrm{SL}(n)$ is the algebraic subgroup scheme of $\mathrm{GL}(n)$ defined by the ideal $(\det -1)$, representing the group functor $\mathcal{CA}\mathrm{lg}_{\mathbb{Z}} \to \mathcal{G}\mathrm{rp} : R \mapsto SL(n,R)$.
- the **orthogonal group** $\mathrm{O}(n)$ is the algebraic subgroup of $\mathrm{GL}(2n)\times\mathbb{G}_m \subset \mathrm{GL}(2n+1)$ generated by the n^2 entries of the equation $(T_{ij})^t C_n (T_{ij}) = TC_n$, where $C_n = \begin{bmatrix} 0 & I_k & 0 \\ I_k & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ if $n = 2k+1$ and $\begin{bmatrix} 0 & I_k \\ I_k & 0 \end{bmatrix}$ if $n = 2k$, representing the functor $\mathcal{CA}\mathrm{lg}_{\mathbb{Z}} \to \mathcal{G}\mathrm{rp} : R \mapsto \{g \in GL(2n,R)\times\mathbb{R}^\times | g^t C_n g = rC_n\}$.
- the **special orthogonal groups** $\mathrm{SO}(n) = \mathrm{O}(n) \cap \mathrm{SL}(n)$.
- the **symplectic group** $\mathrm{Sp}(2n)$ is the algebraic subgroup of $\mathrm{GL}(n)$ defined by the ideal generated by the n^2 entries of the equation $(T_{ij})^t J_{2n} (T_{ij}) = J_{2n}$, where $J_{2n} = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$, representing the functor
$$\mathcal{CA}\mathrm{lg}_{\mathbb{Z}} \to \mathcal{G}\mathrm{rp} : R \mapsto \{g \in GL(2n,R) | g^t J_{2n} g = J_{2n}\} = \{\begin{bmatrix} A & B \\ C & D \end{bmatrix} | A^tC = C^tA, A^tD - C^tB = I, B^tD = D^tB\}.$$
- $\mathrm{PGL}(n)$ is the quotient group of $\mathrm{GL}(n)$ by its center.
- $\mathrm{PSL}(n)$ is the quotient group of $\mathrm{SL}(n)$ by its center.
- $\mathrm{PSO}(n)$ is the quotient group of $\mathrm{SO}(n)$ by its center.
- the **general symplectic group** $\mathrm{GSp}(2n)$ is the algebraic subgroup of $\mathrm{GL}(2n)\times\mathbb{G}_m \subset \mathrm{GL}(2n+1)$ generated by the entries of the equation $(T_{ij})^t J_n (T_{ij}) = TJ_n$, representing the functor $\mathcal{CA}\mathrm{lg}_{\mathbb{Z}} \to \mathcal{G}\mathrm{rp} : R \mapsto \{(g,r) \in GL(2n,R) \times \mathbb{R}^\times | g^t J_n g = rJ_n\}$.
- the **standard Borel subgroup** $\mathrm{B}(n)$ is the algebraic subgroup of $\mathrm{GL}(n)$ representing the upper-triangular matrices.
- the **standard unipotent subgroup** $\mathrm{Unip}(n)$ is the algebraic subgroup of $\mathrm{B}(n)$ representing the unipotent matrices.
- the **diagonal group** $\mathrm{D}(n)$ is the algebraic subgroup of $\mathrm{B}(n)$ representing the diagonal matrices.
- **unitary groups**.
- **special unitary groups**.

⌟

Proof: By(9.1.1.3), it suffices to show $\mathrm{Hom}(-,G)$ is a group functor when restricted to affine schemes. □

Prop. (9.3.5.2) [Amplitude Character]. There is an **amplitude character** $\mathrm{GSp}_{2n} \to \mathbb{G}_m : T \mapsto T$, which represents the natural transformation $R \mapsto ((g,r) \mapsto r)$. ⌟

Prop. (9.3.5.3) [Borel Subgroups of $\mathrm{GL}(n)$**].** If $k = \overline{k}$ and $G = \mathrm{GL}(n)$, then by Lie-Kolchin(9.2.5.5), the Borel subgroups of G are exactly the conjugates by $G(k)$ of $\mathbb{B}(n)$. ⌟

Proof: Cf.[Mil17]P354. □

Prop. (9.3.5.4). $\mathrm{B}(n)$ is split solvable and $\mathrm{Unip}(n)$ is split nilpotent.

Moreover, $\mathrm{Unip}(n)$ has no non-zero subtorus, by successively using(9.1.1.8). ⌟

Proof: Cf.[Mil17]P137. □

Prop. (9.3.5.5). Let $G = \mathrm{SO}(2n), \mathrm{SO}(2n+1)$ or $\mathrm{Sp}(2n)$, then the maximal Borel subgroup of G are the stabilizers of the maximal totally anisotropic flags in G(of length n). ⌟

Proof: Cf.[Mil17]P354. □

Prop. (9.3.5.6) [Reductive and Semisimple Groups]. $\mathrm{GL}(n), \mathrm{SL}(n), \mathrm{SO}(n), \mathrm{Sp}(2n)$ are reductive, as they are connected, and their standard representation is simple, by(18.5.4.1).

$\mathrm{SL}(n), \mathrm{SO}(n), \mathrm{Sp}(2n)$ are semisimple, as they have finite centers(9.3.3.17). ⌟

6 Real Reductive Groups

Main references are [Gaitsgory, Real Reductive Groups] and [Mil17b].

Def. (9.3.6.1) [Real Forms]. Let G be a connected complex Lie group, then a **real form** of G is a connected real Lie subgroup $K \subset G$ that $\mathfrak{k} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathfrak{g}$. ⌟

Prop. (9.3.6.2) [Real Lie Groups and Algebraic Groups]. Let $(H, \mathfrak{h})$ be a connected Lie group in $\mathrm{Lie}\,\mathcal{G}\mathrm{rp}/\mathbb{C}$, then there needs not be an algebraic group G over $\mathbb{R}$ that $G(\mathbb{R})^0 = H$. For example, the topological fundamental group of $SL(2, \mathbb{R})$ is $\mathbb{Z}$, so it has many coverings of finite degree, none of which is algebraic, because SL_2 as an algebraic group is simply connected**?**.

However, if H admits a f.d. representation $H \hookrightarrow GL(V)$, then there exists an algebraic group $G \subset GL(V)$ that $\mathrm{Lie}(G) = [\mathfrak{h}, \mathfrak{h}]$. So if H is semisimple, then there exists an algebraic group $G \subset GL(V)$ s.t. $\mathrm{Lie}(G) = [\mathfrak{h}, \mathfrak{h}]$. When H is semisimple, this means $G^0 = H$. ⌟

Compact Real Algebraic Groups

Def. (9.3.6.3) [Compact Real Algebraic Groups]. A **compact real algebraic group** is an algebraic group $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/\mathbb{R}$ s.t. $G(\mathbb{R})$ is a compact Lie group. ⌟

Prop. (9.3.6.4) [Compactness and Representations]. Let $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}_{\mathrm{cntd}}/\mathbb{R}$. If G is compact, then every f.d. real representation $\rho : G \to \mathrm{GL}(V)$ carries a $G(\mathbb{R})$-invariant inner form. Conversely, if a faithful f.d. real representation carries such a form, then G is compact. ⌟

Proof: If G is compact, then $H = \rho_{\mathbb{R}}(G(\mathbb{R}))$ is compact, so we can take an arbitrary inner form on V and take average on H. The converse is easy. □

Def. (9.3.6.5) [Relevant Groups]. A compact real algebraic group is called **relevant** iff the map $\pi_0(G(\mathbb{R})) \to \pi_0(G)(\mathbb{R})$ is surjective. ⌟

Lemma (9.3.6.6). Let Z be an affine variety over $\mathbb{R}$, let X be a subset of $Z(\mathbb{R})$, and let I_X be the ideal of regular functions on Z that vanishes at X, then $X' = V(I_X)$ satisfies $X \subset X'(\mathbb{R})$. Also by construction, X' is relevant and X intersects real points of every connected components of X'.

Now if Z is acted on by a compact Lie group K and X is a single K-orbit, then $X \cong X'(\mathbb{R})$. ⌟

Proof: Cf.[Gaitsgory P17]. □

Prop. (9.3.6.7) [Compact Relevant Groups and Compact Real Lie Groups]. The functor $G \mapsto G(\mathbb{R})$ is an equivalence of categories from the category of relevant real compact algebraic groups to the category of compact real Lie groups. ⌟

Proof: For the fully faithfulness: given a map $\varphi : G_1(\mathbb{R}) \to G_2(\mathbb{R})$, we need to show it comes from a unique algebraic group homomorphism. Let $K \subset G_1(\mathbb{R}) \times G_2(\mathbb{R})$ be the graph of φ, then let Γ be the subgroup of $G_1 \times G_2$ corresponding to K in(9.3.6.6), then it suffices to prove that the map $\Gamma \to G_1$ is an isomorphism. It is an isomorphism after passing to real points, so isomorphism on the level of Lie algebras. And then it is an isomorphism, because both groups are relevant?. □

Cor. (9.3.6.8). The proof actually works only if G_1 is relevant compact real group. So if we choose $G_2 = GL(n, \mathbb{C})_{\mathbb{R}}$, then by adjointness there is a bijection

$$\mathrm{Hom}_{\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/\mathbb{C}}(G_{\mathbb{C}}, \mathrm{GL}(n)_{\mathbb{C}}) \cong \mathrm{Hom}_{\mathcal{L}\mathrm{ie}\mathcal{G}\mathrm{rp}}(G(\mathbb{R}), GL_n(\mathbb{C})).$$

That is, their complex representations correspond. ⌟

Complex Reductive Algebraic Groups

Prop. (9.3.6.9). If G is a real reductive group, then its complexification $G_{\mathbb{C}}$ is complex reductive. ⌟

Proof: It suffices to show that $\mathrm{Rep}(G(\mathbb{C}))$ is semisimple. For this, notice $\mathrm{Rep}(G)$ is semisimple by definition, so it suffices to show for any representation V of $G_{\mathbb{C}}$, if W is a G-invariant subspace, then W is also W is $G_{\mathbb{C}}$-invariant. But the invariance condition is a vanishing of some matrix coefficients, they vanish on G so also vanish on $G_{\mathbb{C}}$. □

Def. (9.3.6.10) [Real Form]. A **real form** on a complex reductive algebraic group is an anti-linear group isomorphism $\sigma : G \to G$ that $\sigma^2 = 1$. It is called **compact** iff G^σ is compact real, and it is called **relevant** iff G^σ is relevant compact(9.3.6.5). ⌟

Prop. (9.3.6.11) [Polar Decomposition]. If G is a complex algebraic group and $K \in G(\mathbb{C})$ is a compact Lie subgroup. Assume that

- $\mathfrak{g} \cong \mathfrak{k} \otimes_{\mathbb{R}} \mathbb{C}$.
- K intersects non-trivially every connected components of $G(\mathbb{C})$.

Then the group G contains a unique real structure σ that $K = G(\mathbb{C})^\sigma$. And if $\mathfrak{p} \subset \mathfrak{g}$ be the subspace $\{\xi \in \mathfrak{g} | \sigma(\xi) = -\xi\}$, then the map

$$k \times \mathfrak{p} \to G(\mathbb{C}) : (k, p) \mapsto k \cdot \exp(p)$$

is a diffeomorphism. ⌟

Proof: Cf.[Gaitsgory P18]. □

Cor. (9.3.6.12). If we denote $P = \exp(\mathfrak{p})$, then $P \subset \widetilde{P} = \{g \in G(\mathbb{C}) | \sigma(g) = g^{-1}\}$, and there is a diffeomorphism:

$$\coprod_{k \in K, k^2 = 1} \{k\} \times P \cong \widetilde{P}.$$

⌟

Cor. (9.3.6.13). In the situation of(9.3.6.11), G is reductive, by(9.3.6.9). ⌟

Cor. (9.3.6.14). $K \to G(\mathbb{C})$ is a homotopy equivalence. ⌟

Cartan Involutions

Def. (9.3.6.15)[Cartan Involutions]. Let $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}_{\mathrm{cntd}}/\mathbb{R}$, an **involution on** G is an isomorphism $\theta : G \cong G$ s.t. $\theta^2 = \mathrm{id}$.

A **Cartan involution** is an involution s.t. $G^{(\theta)}(\mathbb{R}) = \{g \in G(\mathbb{C}) | g = \theta(\overline{g})\}$ is compact. ⌟

Prop. (9.3.6.16). Cartan involution and compactness. ⌟

Example (9.3.6.17). Let $G = \mathrm{SL}(2)_{\mathbb{R}}$ and $\theta = \mathrm{ad}(\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix})$, then $\mathrm{SL}(2)^{(\theta)}(\mathbb{R}) = SU(2)$ is compact, so this is a Cartan involution on G. ⌟

Thm. (9.3.6.18)[Satake]. Let $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}_{\mathrm{cntd}}/\mathbb{R}$, then G admits a Cartan involution iff G is reductive. And in this case, any two Cartan involutions differ by a conjugation by elements in $G(\mathbb{R})$, i.e. $(\tau = \mathrm{ad}(g_0)^{-1} \circ \theta \circ \mathrm{ad}(g_0))$. ⌟

Proof: Cf.[Satake, Algebraic structures of symmetric domains, volume 4 of Kano Memorial Lectures, 1980]I.4.3. □

Cor. (9.3.6.19) [Satake].

- G is a connected algebraic group, then G is compact iff id is a Cartan involution on G. And in this case, this is the only Cartan involution of G. In particular, a compact connected algebraic group is reductive.
- If V is a f.d. real vector space and $G = \mathrm{GL}(V)$, then the choice of a basis for V determines a Cartan involution $M \mapsto M^t$, and by(9.3.6.18), any Cartan involution is of this form.
- If $G \subset \mathrm{GL}(V)$, then G is reductive iff g is stable under a Cartan involution of $\mathrm{GL}(V)$. And any Cartan involutions of G is of this form.

⌟

Proof: Cf.[Satake, Algebraic structures of symmetric domains, volume 4 of Kano Memorial Lectures, 1980]I.4.4. □

Prop. (9.3.6.20)[c-Polarizations]. Let $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/\mathbb{R}$ and $c \in G(\mathbb{R})$(equivalently $c^2 \in Z(G(\mathbb{R}))$, and $\mathrm{ad}(c)^{-1} = \mathrm{ad}(c^{-1})$). Then for a real representation V of G, a **c-polarization** is a $G(\mathbb{R})$-invariant bilinear form φ s.t. the form $(u, v) \mapsto \varphi(u, cv)$ is symmetric and positive-definite.

Then for such c, if $\mathrm{ad}(c)$ is a Cartan involution, then any f.d. real representation of G admits a c-polarization. Conversely, if a faithful real representation of G admits a c-involution, then $\mathrm{ad}(c)$ is a Cartan involution. ⌟

Proof: Cf.[Mil17b]P16. □

Maximal Compact Subgroup

Cor. (9.3.6.21). For any compact subgroup $K' \subset G(\mathbb{R})$, there exists an element $g \in P^\tau$ s.t. $Ad_g(K') \in K^\tau$. ⌟

Proof: Cf.[Gaitsgory P25]. □

Complex Reductive Lie Groups

Def. (9.3.6.22) [Complex Reductive Lie Groups]. A **connected complex reductive Lie group** is a connected complex Lie group G of the form $((\mathbb{C}^\times)^r \times G_{ss})/Z$ where G_{ss} is semisimple and Z is a finite central subgroup. A **complex reductive Lie group** is a complex Lie group G that G^0 is connected reductive and G/G^0 is finite. ⌟

Def. (9.3.6.23) [Compact Part]. If $G = ((\mathbb{C}^\times)^r \times G_{ss})/Z$ is a connected complex reductive Lie group, then $Z \subset (S^1)^r \times G^c_{ss}$(the compact part), then we denote $G^c = (S^1)^r \times G^c_{ss}/Z$ the compact subgroup of G. Then the restriction of f.d. representations of G to G^c is an equivalence by(12.11.6.3). ⌟

Example (9.3.6.24). $GL(n, \mathbb{C}) = (\mathbb{C}^* \times SL(n, \mathbb{C}))/\mu_n$ is a complex reductive Lie group. ⌟

Prop. (9.3.6.25) [Abstract Jordan Decomposition]. Let G be a connected reductive complex Lie group. A **semisimple/unipotent element** of G is an element that acts on every f.d. representation of G by a semisimple/reductive operator. By(12.11.4.5), it suffices to check for one faithful representation of G by(12.11.4.5) and(9.3.6.23)(faithful representations exist by(9.3.6.23) and(12.11.4.4)).

Then every element $g \in G$ has a decomposition $g = g_s g_u$ where g_s is semisimple, g_u is unipotent, and $g_s g_u = g_u g_s$. ⌟

Proof: Cf.[Etingof, P210]. □

7 Reductive Group Schemes

9.4 Topics in Group Schemes

Thm. (9.4.0.1) [Lang-Steinberg]. Let $k \in \texttt{Field}, k = \overline{k}, G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}_{\mathrm{cntd}}/k, F \in \mathrm{End}(G) \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/k$ s.t. the fixed point of $F(\overline{k})$ is finite, then the **Lang map**

$$\mathcal{L} : G \to G : g \mapsto g^{-1}F(g)$$

is surjective. ⌟

Proof: Cf.[Steinberg, Endomorphisms of Linear Algebraic Groups, P67].**?**

We only prove for the case $\#k < \infty$ and some Power of F is given by a standard Frobenius of G.

By(9.1.4.3), we can assume G is smooth. G acts on itself as $g(x) = gxF(g)^{-1}$. By(9.2.1.15), it has a closed orbit Ω. Thus it suffices to show that $\dim \Omega = \dim G$. Take $x \in \Omega(k)$, by(9.2.1.12) and(9.1.1.28), it suffices to show there exists only f.m. $g \in G(k)$ s.t. $gxF(g)^{-1} = x$. Let $F^m(x) = x, f : G \to G : f(g) = xF(g)x^{-1}$. Notice $xF(x) \cdot F^2(x) \cdot \ldots \cdot F^{m-1}(x)$ is contained in $\ker(F^m)$, so it is of finite order, let's say r. Then $f^{mr} = F^{mr}$, which has only f.m. solutions, thus there are only f.m. g s.t. $gxF(g)^{-1} = x$. □

1 over Finite Fields

Main references are [Representations of Finite Groups of Lie Type, Digne and Michel].

Notation (9.4.1.1).

- $p \in \mathbf{P}, r \in \mathbb{Z}_+, q = p^r, k \in \texttt{Field}^p, \#k = q.$

⌟

Prop. (9.4.1.2) [Orbits Contains a Rational Point]. Let $V \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}}/k, G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}_{\mathrm{cntd}}/k$, G acts on V, then any G-orbits O contains a rational point. ⌟

Proof: Let $v \in O(\overline{k})$, then $F(v) = gv$ for some $g \in G(\overline{k})$. Then by Lang's theorem(9.4.0.1), $g = F(h)^{-1}h$ for some $h \in G(\overline{k})$. Then $F(h(v)) = h(v)$, so $h(v) \in O$ is a rational point. □

Cor. (9.4.1.3). If $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/k$, $H \leq G$ is a connected subgroup, then $G(k)/H(k) = G/H(k)$. ⌟

9.5 Formal Groups and p-Divisible Groups

Main References are [Zin84].

1 Formal Power Series

Def. (9.5.1.1) [Notations]. Let $\underline{X} = \{X_1, \ldots, X_n\}$, $\underline{Y} = \{Y_1, \ldots, Y_n\}$.

Let R be a commutative unital ring, $R[[\underline{X}]]$ be the power series ring. It is a local ring with the maximal ideal $(\underline{X})$.

Let $i_1 : R[[\underline{X}]] \to R[[\underline{X}, \underline{Y}]]$ and $i_2 : R[[\underline{Y}]] \to R[[\underline{X}, \underline{Y}]]$ be the natural embeddings.

Let $\Omega^1_{R[[\underline{X}]]/R}$ be the free $R[[X]]$-module with basis given by $dX_1, \ldots, dX_n$. And there is a universal derivative $D : R[[\underline{X}]] \to \Omega^1_{R[[\underline{X}]]/R}$ given by $D(f) = \sum_i \frac{\partial f}{\partial X_i} dX_i$. It satisfies the usual universal property of Kähler differentials, but with morphisms changed to continuous morphisms. ⌟

Prop. (9.5.1.2) [Formal Sums and Products].

- Let $f_n \in R[[\underline{X}]]$ for any $n \in \mathbb{N}$ s.t. for any $m \in \mathbb{N}$, there exists a $N(m) \in \mathbb{N}$ s.t. $f_n \in (\underline{X})^m$ for any $n \geq N(m)$, then define the **formal sum**

$$\sum_n f_n = \varinjlim_{n\to\infty} \sum_{k=0}^n f_k.$$

  In this case, we say $\sum_n f_n$ is well-defined.

- Let $g_n \in R[[\underline{X}]]$ for any $n \in \mathbb{N}$ s.t. for any $m \in \mathbb{N}$, there exists a $N(m) \in \mathbb{N}$ s.t. $g_n \in 1 + (\underline{X})^m$ for any $n \geq N(m)$, then define the **formal product**

$$\prod_n g_n = \varinjlim_{n\to\infty} \prod_{k=0}^n g_k.$$

  In this case, we say $\prod_n g_n$ is well-defined.

⌟

Prop. (9.5.1.3) [Automorphisms]. If F_i are power series without constant terms that the matrix degree 1 terms of (F_i)(the Jacobi matrix) is invertible in R, then there are unique power series G_i without constant terms that $G \circ F = \mathrm{id}$ and $F \circ G = \mathrm{id}$. ⌟

Proof: It F_i induces a map $F : R[[X_1, \ldots, X_n]] \to R[[X_1, \ldots, X_n]]$ which in turn induces a graded map $K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]$. It is clear that $(\frac{\partial F_i}{\partial X_j})_{ij}$ is invertible iff the induced graded ring map is an isomorphism, and because $K[[X_1, \ldots, X_n]]$, a map is an isomorphism iff its induced graded map is an isomorphism. □

Prop. (9.5.1.4). If R be a torsion-free algebra, and let

$$f(T) = \sum_{n\geq 1}^{\infty} \frac{a_n}{n!} T^n \in (R \otimes \mathbb{Q})[[T]], \quad a_1 \in R^*.$$

Then the unique $g(T)$ s.t. $f(g(T)) = T$ is of the form

$$g(T) = \sum_{n\geq 1}^{\infty} \frac{b_n}{n!} T^n \in (R \otimes \mathbb{Q})[[T]], \quad b_1 \in R^*.$$

⌟

Proof: Repeatedly differentiating the equation $f(g(T)) = T$, we get that $f\prime(g(T))g^{(n)}(T)$ can be expressed as integral polynomials in the variables

$$f^{(i)}(g(T)), 1 \le i \le n, \quad g^{(j)}(T), 1 \le j \le n-1.$$

Then evaluating at $T = 0$, we get that $b_n \in R$ and $b_1 \in R^*$, as $a_1 \in R^*$. □

1**-Dimensional Formal Power Series**

Def. (9.5.1.5) [Formal Exponential and Logarithm]. The **formal exponential** and **formal logarithm** is defined to be elements in $\mathbb{Q}[[x]]$:

$$\exp(x) = \sum_{n\ge 0} \frac{x^n}{n!}, \quad \log(1+x) = -\sum_{n>0} \frac{(-x)^n}{n}.$$

They satisfies $\exp(\log(1+x)) = 1+x, \log(\exp(x)) = x$. ⌟

Remark (9.5.1.6). WARNING: It should be made clear that $\log(1+f)$ is defined only for $f \in xK[[x]]$, and $\log(1+x)$ is a symbol for the function $\mathrm{Log}(x) = \log(1+x)$. $\log(x)$ is not defined. ⌟

Proof: It suffices to prove $\mathrm{Exp}(x) = \exp(x) - 1$ and $\mathrm{Log}(x) = \log(1+x)$ are inverse to each other. It suffices to show $\log(\exp(x)) = x$, because then by(9.5.1.3) the inverse of Log must be just Exp by(9.5.1.3).

We notice Exp are the unique formal power series without constant term that satisfied $d(\mathrm{Exp}) = \mathrm{Exp}+1$, and Log is the unique formal power series that satisfies $d(\mathrm{Log}(x)) = \frac{1}{1+x}$. Thus

$$d(\log(\exp(x))) = \frac{\exp(x)}{\exp(x)} = 1,$$

so $\log(\exp(x)) = x$, because it has no constant term. □

Prop. (9.5.1.7) [Multiplicative Properties]. Suppose $\mathbb{Q} \subset R$, then

- for any $f, g \in R[[\underline{X}]]$, $\exp(f+g) = \exp(f)\exp(g)$.
- If $\sum_n f_n$ is well-defined(9.5.1.2), then $\prod_n \exp(f_n)$ is well-defined and
$$\exp(\sum_n f_n) = \prod_n \exp(f_n).$$
- for any $f, g \in 1 + (\underline{X})$, $\log(f) + \log(g) = \log(fg)$.
- If $g_n \in 1 + (\underline{X})$ and $\prod_n g_n$ is well-defined(9.5.1.2), then $\sum_n \log(f_n)$ is well-defined and
$$\log(\sum_n f_n) = \prod_n \log(f_n).$$

⌟

Proof: Brutal force calculation.**?** □

Def. (9.5.1.8) [Formal Powers]. Let $f \in 1 + xR[[x]], g \in R[[x]]$, f^g is defined to be

$$\exp(g\log(f)).$$

In particular, $\log(f^g) = g\log(f)$ by(9.5.1.5). ⌟

Prop. (9.5.1.9). In $\mathbb{Q}[[x]]$, if $p \in \mathbf{P}$, $m, n \in \mathbb{Z}$, $(n,p) = 1$, and $f(x) \in 1 + x\mathbb{Z}_{(p)}[[x]]$, then $f(x)^{m/n} \in 1 + x\mathbb{Z}_{(p)}[[x]]$. ⌟

Proof: If $g(x) = f(x)^{m/n}$, it is easy to see $g(x)^n = f(x)^m$ and $g(x) \in 1 + x\mathbb{Q}[[x]]$. Let

$$f(x)^m = 1 + \sum_{m\geq 1} a_m x^m, \quad g(x) = 1 + \sum_{m\geq 1} b_m x^m,$$

Then it is easy to use induction to show $b_m \in \mathbb{Z}_{(p)}$ for any $m \in \mathbb{Z}_+$. □

Prop. (9.5.1.10). In $\mathbb{Q}[[x]]$,

$$\exp(x) = \prod_{d>0} (\frac{1}{1-x^d})^{\frac{\mu(d)}{d}}.$$

⌟

Proof: Taking log, we prove its convergence and equality at once:

$$\sum_{d>0} \log((\frac{1}{1-x^d})^{\frac{\mu(d)}{d}}) = \sum_{d>0} \frac{\mu(d)}{d} \log(\frac{1}{1-x^d}) = \sum_{d>0} \frac{\mu(d)}{d} \sum_{d'>0} \frac{x^{dd'}}{d'} = \sum_{n>0} \frac{x^n}{n} \sum_{d|n} \mu(d) = x(2.6.3.22).$$

□

Prop. (9.5.1.11) [Artin-Hasse Exponential]. For $p \in \mathbf{P}$, the **Artin-Hasse exponential** is the power series $\mathrm{hexp}(x)$ defined to be

$$\mathrm{hexp}(x) = \exp(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \ldots) \in \mathbb{Q}[[x]].$$

Then it satisfies

$$\mathrm{hexp}(x) = \prod_{d>0, p\nmid d} (\frac{1}{1-x^d})^{\frac{\mu(d)}{d}}.$$

and in fact $\mathrm{hexp}(x) \in \mathbb{Z}_{(p)}[[x]]$. ⌟

Proof: Taking log, we prove its convergence and equality at once:

$$\sum_{d>0,p\nmid d} \log((\frac{1}{1-x^d})^{\frac{\mu(d)}{d}}) = \sum_{d>0,p\nmid d} \frac{\mu(d)}{d} \log(\frac{1}{1-x^d}) = \sum_{d>0,p\nmid d} \frac{\mu(d)}{d} \sum_{d'>0} \frac{x^{dd'}}{d'} = \sum_{n>0} \frac{x^n}{n} \sum_{d|n,p\nmid d} \mu(d) = \sum_{k\in\mathbb{N}} \frac{x^{p^k}}{p^k} (2.6.3.22).$$

Then the last assertion follows from(9.5.1.9). □

Def. (9.5.1.12) [Bernoulli Numbers]. The **Bernoulli numbers** $B_k, k \geq 0$ are defined to be

$$\frac{X}{e^X - 1} = \sum_{k=0}^{\infty} B_k \frac{X^k}{k!} \in \mathbb{Q}[[X]].$$

Then B_k are all rational numbers, and

$$B_0 = 1, B_1 = -\frac{1}{2}, B_{2k+1} = 0 (k \geq 1), B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}.$$

More numbers can be found at`https://oeis.org/wiki/Bernoulli_numbers`.

For simplicity, for $k \in \mathbb{Z}_{<0}$, denote $B_k = 0$. ⌟

Def. (9.5.1.13)[Hankel Determinants]. Let K be a field and $f = \sum a_i T^i \in K[[T]]$, then for $k, M > 0$, define the **Hankel determinants** to be

$$H_k = \det(a_{i+j+k}), 1 \le i, j \le M$$

⌟

Prop. (9.5.1.14) [Characterizing Rational Functions]. Let $f \in K[[T]]$, then $f \in K[T]$ iff the Hankel determinants H_k of f vanishes for k, M large. ⌟

Proof: □

Cor. (9.5.1.15). If $K \subset L$ are fields, then $K[[T]] \cap L[T] = K[T]$. ⌟

Prop. (9.5.1.16). Let $P, Q \in \mathbb{Q}[T]$ be prime to each other with constant coefficient 1. if $P/Q = Z \in \mathbb{Z}[[T]]$, then we have $P, Q \in \mathbb{Z}[T]$. ⌟

Proof: Let λ be a root of $Q(T)$, we prove that $|\lambda^{-1}|_p \le 1$ for any $p \in \mathbf{P}$: If $|\lambda|_p < 1$, then $Z(\lambda)$ converges in $\mathbb{Q}_p$ because it has integral coefficients, and then

$$P(\lambda) = Q(\lambda)Z(\lambda) = 0.$$

This contradicts the fact that P, Q are coprime. So $\lambda^{-1} \in \mathbb{Z}$, and $Q \in \mathbb{Z}[T]$. Consequently, $P(T) = Q(T)Z(T) \in \mathbb{Z}[[T]] \cap \mathbb{Q}[T] = \mathbb{Z}[T]$. □

Geometric Objects

Def. (9.5.1.17) [Differential Operators]. A continuous R-linear mapping $D : R[[\underline{X}]] \to R[[\underline{X}]]$ is called a **formal differential operator** of order $N \ge -1$ iff

$$L_D : R[[\underline{X}, \underline{Z}]] \to R[[\underline{X}]] : \sum p_\alpha(\underline{X}) Z^\alpha \to \sum p_\alpha(X) D(X^\alpha)$$

vanish on J^{N+1}, where $J = (X_i - Z_i)$.

Then D is an operator of order N if $fD - Df$ has order $N - 1$ for any $f \in R[[X]]$. ⌟

Proof: Let D be a differential operator of order N, since $f(\underline{X}) - f(\underline{Z}) \in J$, for all $g(\underline{X}, \underline{Z}) \in J^N$, we have $L_D((f(\underline{X}) - f(\underline{Z}))g(\underline{X}, \underline{Z})) = 0$, which is equivalent to $L_{D\circ f - f \circ D}(g) = 0$, so $D \circ f - f \circ D$ is an operator of order $N - 1$. Conversely, if $D \circ f - f \circ D$ is an operator of degree $N - 1$, then $L_D((f(\underline{X}) - f(\underline{Z}))g) = 0$ for all $g \in J^N$, then D is an operator of order N. □

Cor. (9.5.1.18). A differential operator $D : R[[\underline{X}]] \to R[[\underline{X}]]$ of order 1 is a linear map that satisfies $D(fg) = D(f)g + fD(g)$, which is just a derivative on $R[[\underline{X}]]$. Equivalently, $D = \sum_i u_i(\underline{Z}) \frac{\partial}{\partial Z_i}$. ⌟

Prop. (9.5.1.19) [Graded Module of Differential Operators]. Let D_1, D_2 be differential forms of order N_1, N_2, then $D_1 \circ D_2$ is a differential form of order $N_1 + N_2$, and $[D_1, D_2]$ is a differential form of order $N_1 + N_2 - 1$. The R-algebra of differential operators on $R[[\underline{X}]]$ is denoted by $\mathcal{DO}$.

In particular, the graded module of differential operators

$$\operatorname{gr} \mathcal{DO} = \oplus\, \mathcal{DO}_N \,/\, \mathcal{DO}_{N-1}$$

is a commutative graded ring. ⌟

Proof:

□

Prop. (9.5.1.20) [Basis of Differential Operators]. There is a representation $g(X+Y) = \sum_\alpha D_\alpha g(X) Y^\alpha$ for any $g \in R[[\underline{X},\underline{Y}]]$, where D_α is a differential operator of degree $|\alpha|$. And $\{D_\alpha\}$ form a free $K[[\underline{X}]]$-basis for the module of differential operators(9.5.1.19).

In fact, D_α is just mimicking $\frac{\partial^\alpha}{\alpha!}$ in all fields. ⌟

Proof: $g(\underline{Z}) = \sum_\alpha D_\alpha g(\underline{X})(\underline{Z}-\underline{X})^\alpha$, thus if D is a differential operator of order N, then

$$D(g)(\underline{X}) = L_D(g(\underline{Z})) = \sum_{|\alpha|\leq N} L((\underline{Z}-\underline{X})^\alpha) D_\alpha g(\underline{X}),$$

which means $D = \sum_{|\alpha|\leq N} a_\alpha(\underline{X}) D_\alpha$, where $a_\alpha = L((\underline{Z}-\underline{X})^\alpha)$. □

Def. (9.5.1.21)[Tangent Space]. The tangent space of $K[[\underline{X}]]$ is the K-module $\mathrm{Hom}_K((\underline{X})/(\underline{X})^2, K)$. ⌟

Def. (9.5.1.22) [Formal Curves]. A **formal curve** in $K[[\underline{X}]]$ is an n-tuple $(\gamma_1(T),\ldots,\gamma_n(T))$ of elements in $K[[T]]$. The **tangent space of formal curve** is the map $\mathrm{Hom}_K((\underline{X})/(\underline{X})^2, K)$ given by $X_i \mapsto \gamma_i(T) \in (T)/(T^2) \cong K$. ⌟

Prop. (9.5.1.23)[Integral Curves]. For any ⌟

2 Formal Identities

Prop. (9.5.2.1). In $\mathbb{Z}[[T]]$,

$$\frac{1}{(1-T)^2} = \sum_{n\geq 0}(n+1)z^n$$

⌟

Proof:

$$(1-T)^2\sum_{n\geq 0}(n+1)z^n = (1-T)\sum_{n\geq 0} z^n = 1.$$

□

Prop. (9.5.2.2). In $\mathbb{Z}[[T]]$,

$$\sum_{n\geq 1}\frac{nT^n}{1-T^n} = \sum_{n\geq 1}\frac{T^n}{(1-T^n)^2}$$

⌟

Proof: □

Prop. (9.5.2.3). In $R[[z]]$, if

$$\sum_{r=0}^\infty A(r)z^r = \frac{1}{(1-\alpha_1 z)(1-\alpha_2 z)}, \quad \sum_{r=0}^\infty B(r)z^r = \frac{1}{(1-\beta_1 z)(1-\beta_2 z)},$$

then

$$\sum_{r=0}^\infty A(r)B(r)z^r = (1-\alpha_1\alpha_2\beta_1\beta_2 z^2)\prod_{i=1}^2\prod_{j=1}^2\frac{1}{(1-\alpha_i\beta_j z)}.$$

⌟

Proof: $A(n)B(n) = \sum_{0\leq k,j\leq n}\alpha_i^k\alpha_2^{n-k}\beta_1^j\beta_2^{n-j}$, and the coefficients in the z^n term of $\prod_{i=1}^2\prod_{j=1}^2\frac{1}{(1-\alpha_i\beta_j z)}$ is

$$\sum_{0\leq k,j\leq n}\#\{(r_1,r_2,r_3,r_4)|0\leq r_i\leq n, r_1+r_2=a, r_1+r_3=b, r_1+r_2+r_3+r_4=n\}\alpha_i^k\alpha_2^{n-k}\beta_1^j\beta_2^{n-j}.$$

Notice

$$\#\{(r_1,r_2,r_3,r_4)|0\leq r_i\leq n, r_1+r_2=a, r_1+r_3=b, r_1+r_2+r_3+r_4=n\}=\min(a,b)-(a+b-n).$$

Thus the effect of multiplying $(1-\alpha_1\alpha_2\beta_1\beta_2 z^2)$ reduces the coefficients of $\alpha_i^k\alpha_2^{n-k}\beta_1^j\beta_2^{n-j}z^n$ to 1. So the assertion follows. □

Prop. (9.5.2.4) [Euler Identities].

- In $\mathbb{Z}[x][[q]]$,
$$\prod_{n\geq 0}(1+xq^n)=\sum_{n=0}^{\infty}\frac{q^{n(n-1)/2}x^n}{(1-q)\dots(1-q^n)}.$$
- In $\mathbb{Z}[[x,q]]$,
$$\prod_{n\geq 0}(1-xq^n)^{-1}=\sum_{n=0}^{\infty}\frac{x^n}{(1-q)\dots(1-q^n)}.$$

⌟

Proof: These follow from interesting combinatorial identies. □

Prop. (9.5.2.5) [Jacobi's Triple Product Formula, [And65]]. in $\mathbb{Z}[x][[x^{-1}q]]$,

$$\sum_{n=-\infty}^{\infty}x^nq^{n^2}=\prod_{n=1}^{\infty}(1-q^{2n})(1+xq^{2n-1})(1+x^{-1}q^{2n+1}).$$

⌟

Proof: By substituting $q=q^2, x=xq$ in Euler identities1(9.5.2.4), in $\mathbb{Z}[x][[x^{-1}q]]$,

$$\begin{aligned}
\prod_{n\geq 0}(1+xq^{2n+1}) &= \sum_{n=0}^{\infty}\frac{q^{n^2}x^n}{(1-q^2)(1-q^4)\dots(1-q^{2n})}\\
&=(\prod_{j\geq 0}(1-q^{2j+2}))^{-1}\sum_{n=0}^{\infty}q^{n^2}x^n\prod_{j=0}^{\infty}(1-q^{2n+2+2j})\\
&=(\prod_{j\geq 0}(1-q^{2j+2}))^{-1}\sum_{n=-\infty}^{\infty}q^{n^2}x^n\prod_{j=0}^{\infty}(1-q^{2n+2+2j})\\
(q=q^2, x=q^{2n+2}\text{ in}(9.5.2.4)) &=(\prod_{j\geq 0}(1-q^{2j+2}))^{-1}\sum_{n=-\infty}^{\infty}q^{n^2}x^n\sum_{m=0}^{\infty}\frac{(-1)^mq^{m^2+m+2nm}}{(1-q^2)(1-q^4)\dots(1-q^{2n})}\\
&=(\prod_{j\geq 0}(1-q^{2j+2}))^{-1}\sum_{m=0}^{\infty}\frac{(-x^{-1}q)^m}{(1-q^2)\dots(1-q^{2n})}\sum_{n=-\infty}^{\infty}q^{(m+n)^2}x^{m+n}\\
(q=q^2, x=-x^{-1}q\text{ in}(9.5.2.4)) &=(\prod_{j\geq 0}(1-q^{2j+2}))^{-1}\prod_{j=0}^{\infty}(1+x^{-1}q^{2j+1})^{-1}\sum_{n=-\infty}^{\infty}q^{n^2}x^n.
\end{aligned}$$

□

Cor. (9.5.2.6) [Dedekind Eta Function]. Substitute $q = q^{3/2}$ and $x = q^{-1/2}$, we get:

$$\sum_{n=-\infty}^{\infty}(-1)^n q^{(3n^2+n)/2} = \prod_{n=1}^{\infty}(1-q^{3n})(1-q^{3n-1})(1-q^{3n-2}) = \prod_{n=1}^{\infty}(1-q^n) \in \mathbb{Z}[[q]].$$

By completing the square,

$$\sum_{n=-\infty}^{\infty}(-1)^n q^{(6n+1)^2/24} = q^{1/24}\prod_{n=1}^{\infty}(1-q^n) \in \mathbb{Z}[[q^{1/24}]].$$

the last term is known as the **Dedekind eta function** $\eta(q) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n) \in \mathbb{Z}[[q^{1/24}]]$. ⌟

3 Formal Group Law

In this subsection, the local structure of an algebraic group scheme at the origin is studied.

Def. (9.5.3.1) [Formal Group Laws]. A **formal group law** $\mathcal{G}$ of dimension n over $R \in \mathcal{CA}\mathrm{lg}$ is a continuous local map $\mu_{\mathcal{G}} : K[[\underline{X}]] \to K[[\underline{X}, \underline{Y}]]$ given by an n-tuple of power series $G = (G_1, \ldots, G_n)$ in $R[[\underline{X}, \underline{Y}]]$ that

$$G(X, Y) \equiv X + Y \mod (\underline{X}, \underline{Y})^2, \quad G(G(\underline{X}, \underline{Y}), Z) = G(X, G(Y, Z)).$$

A **formal R-module** is a formal group law $\mathcal{G}$ over R together with a ring homomorphism $R \to \mathrm{End}_R(G)$ that $[a](X) = aX + \ldots$.

A morphism of formal groups laws $\mathcal{G} \to \mathcal{H}$ is a continuous local map $\varphi^* : R[[\underline{X}']] \to R[[\underline{X}]]$ given by an n'-tuple of power series $\varphi = (\varphi_1, \ldots, \varphi_{n'})$ in $R[[\underline{X}]]$ that satisfies

$$\mu_{\mathcal{G}} \circ \varphi^* = (\varphi^* \otimes \varphi^*) \circ \mu_{\mathcal{H}}.$$

Or equivalently, $\varphi(G(\underline{X}, \underline{Y})) = H(\varphi(\underline{X}), \varphi(\underline{Y}))$. ⌟

Prop. (9.5.3.2). For a formal group Law G,

- $G(0, \underline{Y}) = \underline{Y}, G(\underline{X}, 0) = \underline{X}$.
- There exists a unique inverse $i(\underline{X})$ that $G(\underline{X}, i(\underline{X})) = 0$. And this $i(\underline{X})$ satisfies $G(i(\underline{X}), \underline{X}) = 0$, and $i^2 = \mathrm{id}$.

⌟

Proof: ? □

Cor. (9.5.3.3) [Formal Group Laws and Group Schemes]. WARNING: A formal group law of dimension n is not equivalent to a group scheme structure on $\mathrm{Spec}\,\mathbb{Z}[[X_1, \ldots, X_n]]$(9.1.1.1), as here we are taking a completion. ⌟

Def. (9.5.3.4) [Multiplication Map]. Let G be a commutative formal group law over R and $m \in \mathbb{Z}$, then we can define a group homomorphism $[m] : G \to G$ inductively as follows:

$$[0](\underline{X}) = 0, \quad [m+1](\underline{X}) = G([m](\underline{X}), \underline{X}), \quad [m-1](\underline{X}) = G([m](\underline{X}), i(\underline{X})).$$

Then it can be verified that this is well-defined and $[m]$ is a group homomorphism. ⌟

Prop. (9.5.3.5) [Multiplications as Automorphisms]. Let $\mathcal{G}$ be a commutative formal group law over R and $m \in \mathbb{Z}$, then $[m](\underline{X}) = m\underline{X} + o(\underline{X})$. In particular, if m is invertible in R, then $[m]$ is an automorphism of G, by(9.5.1.3). ⌟

Prop. (9.5.3.6). $\mathbb{G}_a$ is the one-dimensional formal group with $\mathbb{G}_a(\underline{X},\underline{Y}) = X + Y$, $\mathbb{G}_m$ is the one-dimensional formal group with $\mathbb{G}_m(\underline{X},\underline{Y}) = X + Y + XY$. Over a $\mathbb{Q}$-algebra K, there is an isomorphism between $\mathbb{G}_a$ and $\mathbb{G}_m$ giving by $X \to \exp(X) - 1$. ⌟

Def. (9.5.3.7) [Invariant Differential Forms]. An **invariant differential form** on a formal group law G over R is an element $\omega = \sum a_i(\underline{X})dX_i \in \Omega^1_{R[[X]]/R}$ that satisfies $(\underline{Y} \mapsto G(\underline{X},\underline{Y}))_*\omega = \omega$, i.e.

$$\sum_j a_j(\underline{Y})dY_j = \sum_i a_i(G(\underline{X},\underline{Y}))\frac{\partial G_i}{\partial Y_j}(\underline{X},\underline{Y})dY_j.$$

If G is commutative, then this is equivalent to $\mu_*\omega = i_{1*}\omega + i_{2*}\omega$. ⌟

Prop. (9.5.3.8). The mapping $\omega \mapsto (u_1(0),\dots,u_n(0))$ is an isomorphism of the R-module of invariant differential forms and R^n. ⌟

Proof: Cf.[Zin84]P14. □

Prop. (9.5.3.9)[Pullback of Invariant Differential Forms]. Let $\varphi : G \to H$ be a homomorphism of formal group laws, then for any invariant differential form $\omega = \sum a_i(\underline{X})dX_i$ on H, $\varphi^*\omega$ is a differential form on G, given by expanding $\sum a_i(\varphi(\underline{X}))d(\varphi_i(\underline{X}))$. ⌟

Proof:

$$\begin{aligned}(\underline{Y} \mapsto G(\underline{X},\underline{Y}))^*\varphi^*\omega &= \sum a_i(\varphi(G(\underline{X},\underline{Y})))d(\varphi(G(\underline{X},\underline{Y})))\\ &= \sum a_i(H(\varphi(\underline{X}),\varphi(\underline{Y})))d(H(\varphi(\underline{X}),\varphi(\underline{Y})))\\ &= \sum_i a_i(\varphi(\underline{Y}))d(\varphi(\underline{Y}))\\ &= \varphi^*\omega\end{aligned}$$

□

Def. (9.5.3.10) [Invariant Differential Operators]. An **invariant differential operator** on a formal group G of dimension n is a differential operator D s.t.

$$\mu \circ D = (1 \otimes D) \circ \mu.$$

Equivalently, if $D = \sum_i u_i(\underline{Z})\frac{\partial}{\partial Z_i}$, it satisfies

$$\sum_j u_j(\underline{Y})\frac{\partial G_i}{\partial Y_j} = u_i(G(\underline{X},\underline{Y})).$$

The space of invariant operators is stable under composition. The R-algebra of invariant differential operators on G is denoted by $\mathcal{DO}_G$. ⌟

Prop. (9.5.3.11). The space of invariant differential operators on G of order$\leq N$ are in bijection with the space of K-linear maps $l : K[[\underline{X}]] \to K$ s.t. $l((\underline{X})^{N+1}) = 0$ via

$$Df(\underline{X}) = (1 \otimes l)f(G(\underline{X},\underline{Y})).$$

⌟

Proof: Cf.[Zin84]P22. □

Cor. (9.5.3.12) [Basis of Invariant Differential Operators]. For any $f \in K[[\underline{X}]]$, write $f(G(\underline{X},\underline{Y})) = \sum_\alpha (H_\alpha f)(\underline{X})Y^\alpha$.

Then H_α are differential operators of order $|\alpha|$, and the space of invariant differential operators of order N form a free R-module with basis H_α. In particular, the space of invariant derivatives is isomorphic to R^n. ⌟

Proof: By(9.5.3.11),

$$Df(\underline{X}) = (1\otimes l)f(G(\underline{X},\underline{Y})) = (1\otimes l)(\sum_\alpha (H_\alpha f)(\underline{X})Y^\alpha) = \sum_\alpha l(\underline{Y}^\alpha)(H_\alpha f)(\underline{X}).$$

□

Cor. (9.5.3.13) [Composition of Invariant Differential Operators]. Let $D_1, D_2 \in \mathcal{DO}_G$, then

$$(D_1\circ D_2)f(\underline{Z}) = (1\otimes l_1\otimes l_2)f(G(\underline{Z},G(\underline{X},\underline{Y}))),$$

in particular,

$$l_{D_1\circ D_2}(f) = (l_1\otimes l_2)f(G(\underline{X},\underline{Y})).$$

⌟

Proof:

$$(D_1\circ D_2)f(\underline{Z}) = D_1(1\otimes l_1)f(G(\underline{Z},\underline{Y})) = (1\otimes l_2\otimes 1)(1\otimes 1\otimes l_1)f(G(G(\underline{Z},\underline{X}),\underline{Y})) = (1\otimes l_1\otimes l_2)f(G(\underline{Z},G(\underline{X},\underline{Y}))).$$

□

Prop. (9.5.3.14) [Pushforward of Invariant Differential Operators]. A homomorphism φ of formal groups $G\to H$ induces a map from the linear maps $l : K[[\underline{X}]]\to K$ to linear maps $l\circ\varphi^* : K[[\underline{X}']]\to K$, which induces a K-homomorphism of algebras $\varphi_* : \mathcal{DO}_G \to \mathcal{DO}_H$. ⌟

Proof: To show preserves algebra structure, notice for any $f \in R[[\underline{X}']]$, by(9.5.3.13),

$$\begin{aligned}\varphi_*(D)\circ\varphi_*(D')f(0) &= (l\circ\varphi^*)\otimes(l'\circ\varphi^*)f(H(\underline{X}',\underline{Y}'))\\ &= (l\otimes l')f(H(\varphi(\underline{X}),\varphi(\underline{Y})))\\ &= (l\otimes l')f(\varphi(G(\underline{X},\underline{Y})))\\ &= [(l\otimes l')\circ\varphi^*]f(G(\underline{X},\underline{Y}))\\ &= \varphi_*(D\circ D')f(0).\end{aligned}$$

Thus $\varphi_*(D)\circ\varphi_*(D') = \varphi_*(D\circ D')$, by(9.5.3.11). □

Prop. (9.5.3.15) [$\mathbb{Q}$-Theorem]. Any commutative connected formal group over a $\mathbb{Q}$-algebra R is a direct sum of $\widehat{\mathbb{G}}_a$. ⌟

Proof: Cf.[Zin84]P19. □

1-dimensional Formal Groups

Def. (9.5.3.16) [Normalized Invariant Differential Form]. For a 1-dimensional formal group G over $R[[X]]$, the module of invariant differentials is isomorphic to R(9.5.3.10). An invariant differential form $\omega = P(T)dT$ is called **normalized** if $P(0) = 1$.

Then the unique normalized invariant differential form on G is given by $\omega_G = G_X(0,T)^{-1}dT$. ⌟

Proof: We need to check $G_X(0, G(T,S))^{-1}G_X(T,S) = G_X(0,T)^{-1}$, and this is just $G(U, G(T,S)) = G(G(U,T),S)$ differentiated at U and let $U = 0$. □

Prop. (9.5.3.17). For a morphism $\varphi : \mathcal{F} \to \mathcal{G}$ of 1-dimensional formal groups laws over R, $\varphi^*\omega_{\mathcal{G}} = \varphi'(0)\omega_{\mathcal{F}}$. ⌟

Proof: By(9.5.3.9), $\varphi^*\omega_{\mathcal{G}}$ is an invariant differential form, and compare their constant coefficients. □

Cor. (9.5.3.18). Let p be a prime, then for any formal group law of dimension 1,

$$[p](T) = pf(T) + g(T^p)$$

for some $f(0) = g(0) = 0$. ⌟

Proof: If suffices to show that $[p]'(T) \subset pR[[T]]$. But by(9.5.3.17) and(9.5.3.5),

$$p\omega(T) = [p]^*\omega(T) = G_X(0, [p](T))^{-1}[p]'(T)dT$$

so this is true. □

Def. (9.5.3.19) [Formal Logarithm]. When R is torsion-free, the **formal logarithm** $\log_{\mathcal{F}}$ for a 1-dimensional formal group is the integration of invariant differential

$$\int_0^T \omega_{\mathcal{F}} = T + \frac{c_1}{2}T^2 + \cdots \in (R \otimes \mathbb{Q})[[T]].$$

Then the **formal power exponential** is the the unique power series $\exp_{\mathcal{F}}$ that is the inverse of $\log_{\mathcal{F}}$. It exists uniquely by(9.5.1.3), and by(9.5.1.4), it is of the form

$$\exp_{\mathcal{F}} = \sum_{n\geq 1}^{\infty} \frac{b_n}{n!}T^n \in (R \otimes Q)[[T]], b_n \in R.$$

⌟

Prop. (9.5.3.20). For R is torsion-free and an 1 dimensional formal group $\mathcal{F}$ over R,

$$\log_{\mathcal{F}} : \mathcal{F} \to \mathbb{G}_a$$

is an isomorphism of formal groups laws over $R \otimes_{\mathbb{Z}} \mathbb{Q}$.

And if $\mathcal{F}$ is a formal R-module, then it is an isomorphism of R-modules, because from(9.5.3.17) that $\omega_{\mathcal{F}} \circ [a] = a\omega_{\mathcal{F}}$, thus $\log_{\mathcal{F}} \circ [a] = a \cdot \log_{\mathcal{F}}$. ⌟

Proof: From $\omega_{\mathcal{F}}(F(T,S)) = \omega_{\mathcal{F}}(T)$, we get that $\log_{\mathcal{F}}(F(T,S)) = \log_{\mathcal{F}}(S) + \log_{\mathcal{F}}(T)$. So it is a homomorphism. Now the inverse $\exp_{\mathcal{F}}$ is already given, so it is an isomorphism. □

Cor. (9.5.3.21) [1-Dimensional Formal Group Law is Commutative]. Any 1-dimensional formal group over a ring R that has no torsion nilpotents is commutative. ⌟

Proof: We only prove for R torsion free?. $F(T,S) = \exp_{\mathcal{F}}(\log_{\mathcal{F}}(T) + \log_{\mathcal{F}}(S))$. □

Lubin-Tate Formal Group Law

Notation (9.5.3.22).
- Let $(K, v, \mathcal{O}_K, \mathfrak{p}_v, k) \in p$-`LField`.

⌟

Def. (9.5.3.23) [Lubin-Tate Formal Group Law]. Let ϖ be a uniformizer for K, a **Lubin-Tate power series** for ϖ is a power series $\varphi(X) \in \mathcal{O}_K[[X]]$ s.t.

$$\varphi(X) \equiv \varpi X \mod X^2, \quad \varphi(X) \equiv X^q (\text{mod } \mathfrak{p}_v).$$

A **Lubin-Tate module** G over $\mathcal{O}_K$ is a formal $\mathcal{O}_K$-module(9.5.3.1) s.t. $[\pi_K](X)$ is a Lubin-Tate power series. ⌟

Prop. (9.5.3.24). Given a p-adic number field K with residue field $\mathbb{F}_q$, we consider the set ξ_π of all Lubin-Tate power series for π.

If $f, g \in \xi_\pi$ and $L(\underline{X}) = \sum a_i X_i$ be a linear form, then there exists a unique power series $F(\underline{X})$ that $F(X) \equiv L(X) \mod (\underline{X})^2$ and $f(F(\underline{X})) = F(g(\underline{X}))$. ⌟

Proof: Choose F consecutively, if $F_{r+1} = F_r + \Delta_r$, then must

$$\Delta \equiv \frac{f(F_r(X)) - F_r(g(X))}{\pi^{r+1} - \pi} \text{ mod degree } (r+2).$$

This has coefficient in $\mathcal{O}$ because $f \equiv g \equiv Z^q \mod \pi$. □

Cor. (9.5.3.25). If we let $f = g, L = X + Y$ to get F_f and $f, g, L = aX$ to get $a_{f,g}$, then
- $F_f(\underline{X}, \underline{Y}) = F_f(Y, X)$.
- $F_f(F_f(\underline{X}, \underline{Y}), Z) = F_f(X, F_f(Y, Z))$.
- $a_{f,g}(F_g(\underline{X}, \underline{Y})) = F_f(a_{f,g}(X), a_{f,g}(Y))$.
- $a_f b_f(Z) = (ab)_f(Z)$.
- $(a+b)_f(Z) = F_f(a_f(Z), b_f(Z))$.
- $\pi_f(Z) = f(Z)$.

all follow from the unicity of the last proposition. ⌟

Cor. (9.5.3.26) [Existence of Lubin-Tate Modules]. We get a commutative formal $\mathcal{O}$-module F_f for every f. And this group can act on $\mathfrak{p}_L$ for an alg.ext L/K. The set of zeros $\Lambda_{f,n}$ of f^n in L, as the elements annihilated by π^n, is a submodule of $\mathfrak{p}_L^{(f)}$.

And $u_{g,f}$ for any unit $u \in \mathcal{O}$ defines an isomorphism between F_f and F_g, thus this formal group only depends on π, called F_π. Hence $L_{f,n} = K(\Lambda_{f,n})$ only depends on π, with Galois group $G_{\pi,n}$. ⌟

Prop. (9.5.3.27) [Different Uniformizers]. For two uniformizers ϖ, ϖ', it is proven that F_ϖ and $F_{\varpi'}$ are isomorphic, but isomorphic over $\mathcal{O}_{\widehat{K^{\text{ur}}}}$.

Thus $L_{\varpi,n}$ and $L_{\varpi',n}$ may not be isomorphic, but $K^{\text{ur}}.L_{\pi,n} = K^{\text{ur}}.L_{\pi',n}$ since $\widehat{K^{\text{ur}}}.L_{\pi,n} = \widehat{K^{\text{ur}}}.L_{\varpi',n}$ and both of them is the algebraic closure of K in it. ⌟

Proof: Cf.[Neukirch CFT P105].? □

Lemma (9.5.3.28). The Newton polygon of $[\pi_K^n]/\pi_K^n$ has vertices

$$(1,0),(q,-1/e_K),(q^2,-2/e_K),\dots.$$

⌟

Proof: Notice $[\pi_K^n]$ has no infinite edge of negative slope because all its coefficient are in $\mathcal{O}_K$. Now look at its roots, it has a root 0, and $q-1$ roots of valuation $v_p(\pi_K)/(q-1)$, $q(q-1)$ roots of valuation $v_p(\pi_K)/q(q-1)$, and so on. So by factor out these roots, $[\pi_K^n]/\pi_K^n$ is left with a power series whose Newton polygon is a single line, which shows the desired result. □

Prop. (9.5.3.29). The formal logarithm(9.5.3.19) of the Lubin-Tate formal group F_π satisfies:

$$\log_{\mathcal{F}_\varpi}(T)=\lim_{n\to\infty}[\pi_{\mathcal{F}}^n]/\pi_{\mathcal{F}}^n.$$

⌟

Proof: By(9.5.3.20) we have

$$\log_{\mathcal{F}}(T)=\log_{\mathcal{F}}([\pi_{\mathcal{F}}^n])/\pi_{\mathcal{F}}^n=([\pi_K^n]+a_2/2[\pi_K^n]^2+\dots)/\pi_K^n$$

and for any degree n, the coefficient of $[\pi_K^{2n}]/\pi_K^{2n}$ is bounded below by a $c(n)$, so $[\pi_K^{2n}]/\pi_K^n$ converges to 0, thus the result. □

Cor. (9.5.3.30). The Newton polygon of $\log_{\mathcal{F}}(T)$ has vertices $(1,0),(q,-1/e_K),(q^2,-2/e_K),\dots$. ⌟

The discussion is continued at2.

4 Formal Groups

Prop. (9.5.4.1) [Formal Group Law as Functors]. Let $\mathcal{N}\mathrm{il}_R$ be the Abelian category of nilpotent commutative (non-unital)R-algebras, then the category of commutative formal group law are equivalent to Abelian functors on $\mathcal{N}\mathrm{il}$ whose underlying set-theoretic functor if $N\mapsto N^n$. ⌟

Proof: Each commutative formal group law G of dimension n defines a functor

$$\mathcal{N}\mathrm{il}_R\to\mathcal{A}\mathrm{b}:N\mapsto(N^n,G)$$

Conversely, if $\widetilde{G}:\mathcal{N}\mathrm{il}_R\to\mathcal{A}\mathrm{b}$ is a functor s.t. the underlying set-theoretic map is $N\mapsto N^n$, then $\widetilde{G}((\underline{X},\underline{Y})/(\underline{X},\underline{\ })^k)\cong[(\underline{X},\underline{\ })/(\underline{X},\underline{Y})^k]^n$ as sets. Suppose

$$(X_1,\dots,X_n)+(Y_1,\dots,Y_n)=(G_1^k(\underline{X},\underline{Y}),\dots,G_n^k(\underline{X},\underline{Y}))$$

in $\widetilde{G}((\underline{X},\underline{Y})/(\underline{X},\underline{Y})^k)$, then $G_i^{k+1}\equiv G_i^k\mod(\underline{X},\underline{Y})^k$, and their limit defines a commutative formal group law of dimension n. Because for any nilpotent algebra N and $(a_1,\dots,a_n),(b_1,\dots,b_n)\in N^n$, there is a surjective map $(\underline{X},\underline{Y})/(\underline{X},\underline{\ })^k\to N$ for some k that maps X_i to a_i, Y_i to b_i, thus by functoriality, $\widetilde{G}(N)\cong G(N)$. □

Def. (9.5.4.2) [Formal Groups]. A (commutative)**formal group** is an exact Abelian functors on $\mathcal{N}\mathrm{il}$ whose underlying set-theoretic functor if $N\mapsto N^n$ and commutes with infinite direct sums. ⌟

Remark (9.5.4.3). Don't confuse formal groups with formal schemes, they are totally different notions. ⌟

Example (9.5.4.4). Let $S \in \mathbb{N}\mathrm{il}$, then the functor $\mathrm{res}_{S/R}(\mathbb{G}_m)$ is a commutative formal group. ⌟

Prop. (9.5.4.5). Let G be a commutative formal group law defined over a complete local ring $(R, \mathfrak{m})$, then

- For each n, $G(\mathfrak{m}^n)/G(\mathfrak{m}^{n+1}) \cong \mathfrak{m}^n/\mathfrak{m}^{n+1}$ as groups.
- Let p be the characteristic of the residue field k (p may be 0), then $\mathcal{F}(\mathfrak{m})_{tor} = \mathcal{F}(\mathfrak{m})[p^\infty]$.

⌟

Proof: 1: This is because $F(x, y) \equiv x + y \mod \mathfrak{m}^n$.

2: This is because $[m]$ is an automorphism by(9.5.3.5) as m is invertible in R. □

1-Dimensional Commutative Formal Groups over DVR

Prop. (9.5.4.6). Let $(R, \mathfrak{m})$ be a CDVR with residue field k of characteristic p, $\mathcal{F}$ a formal group law over R. Then $\mathcal{F}(\mathfrak{m})_{\mathrm{tor}} = \mathcal{F}[p^\infty]$, and if $x \in \mathcal{F}(\mathfrak{m})$ has exact order p^n, then $v(x) \le \frac{v(p)}{p^n - p^{n-1}}$. ⌟

Proof: If $(m, p) = 1$, then $\mathcal{F}(\mathfrak{m})[m] = 0$ by(9.5.3.5).

By(9.5.3.18), $[p](x) = pf(x) + g(x^p)$, where $f(0) = 1$. Thus it is possible only if $pv(x) \ge v(p^x)$, which means $v(x) \le v(p)/(p-1)$.

Now if this is true for $n \ge 1$, let $x \in \mathcal{F}(\mathfrak{m})$ with order p^{n+1}, then $v([p](x)) = v(pf(x) + g(x^p)) \ge \min(v(px), pv(x))$. But $[p](x)$ has order p^n, thus $\frac{v(p)}{p^n - p^{n-1}} \ge \min(v(px), pv(x))$. But $n \ge 1$ and $v(x) > 0$, it is impossible that $\frac{v(p)}{p^n - p^{n-1}} \ge v(px)$, thus we have $\frac{v(p)}{p^n - p^{n-1}} \ge pv(x)$. □

Prop. (9.5.4.7). Let $(K, \mathcal{O}_K, \mathfrak{m}, \kappa)$ be a complete valued field of mixed characteristic $(0, p)$, $\mathcal{F}$ a formal group law over K, then

- the formal logarithm(9.5.3.19) induces an homomorphism $\log_{\mathcal{F}} : \mathcal{F}(\mathfrak{m}) \to K$.
- For $r > \frac{v(p)}{p-1}$, $\log_{\mathcal{F}}$ is an isomorphism $\log_{\mathcal{F}} : \mathcal{F}(\mathfrak{m}^r) \cong \mathfrak{m}^r$.

⌟

Proof: This follows from determining the convergence of $\log_{\mathcal{F}}$ and $\exp_{\mathcal{F}}$ by(14.2.5.9), after which it is a homomorphism by(9.5.3.20). □

Cor. (9.5.4.8) [Group Structure of CDVRs]. Take $F(X, Y) = (1 + X)(1 + Y) - 1$, then $\log_{\mathcal{F}}$ is given by $\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$, and it induces an isomorphism $(1 + \mathfrak{m}^r)^\times \cong \mathfrak{m}^r$ for $r > \frac{v(p)}{p-1}$. ⌟

Prop. (9.5.4.9) [$\mathbb{Z}_p$-Multiplication]. Let $(R, \mathfrak{m})$ be a CDVR with residue field k of characteristic p, F a formal group law over R, then for any $x \in \mathcal{F}(\mathfrak{m})$, $\lim_{n \to \infty} [p^n](x) \to 0$.

In particular, we can define $[\alpha](x)$ for any $\alpha \in \mathbb{Z}_p$. ⌟

Proof: By(9.5.3.18), $v([p](x)) = v(pf(x) + g(x^p)) \ge \min(v(x) + v(p), pv(x))$. □

5 Cartier Theory

Main References are[Zin84].

Isogenies of Formal Groups

Def. (9.5.5.1) [Heights over Positive Characterestic]. Let R be a ring of characteristic $p > 0$, $\varphi : F \to G$ be a homomorphism of formal group laws over R of dimension 1, the **height of homomorphism** $\mathrm{ht}(\varphi)$ is the largest integer h s.t. $\varphi(T) = g(T^{p^h})$ for some h.

For a formal group law F over R, the **height of formal group law** $\mathrm{ht}(F)$ is $\mathrm{ht}([p]_F)$. By(9.5.3.18), the height is always positive. ⌟

Prop. (9.5.5.2). Let R be a ring of characteristic $p > 0$, $f : F \to G$ be a homomorphism of formal group laws over R of dimension 1, then

- If $f'(0) \neq 0$, then $\mathrm{ht}(f) > 0$.
- If $f = g(T^{p^h})$ with $h = \mathrm{ht}(f)$, then $g'(0) \neq 0$.

In particular, the first non-zero term of $f(T)$ is T^{p^h}, where h is the height of f. ⌟

Proof: 1: Let ω_F, ω_G be the normalized invariant differential forms of F and G, then

$$0 = f'(0)\omega_F(T) = \omega_G(f(T)) = G_X(0,T)^{-1} f'(T)dT,$$

thus $f'(T) = 0$, which means $\mathrm{ht}(f) > 0$.

2: Let $q = p^h$ and $F^{(q)}(T) = F(X^{1/q}, Y^{1/q})^q$. Then it is easy to see $F^{(q)}$ is another formal group law, and g is a homomorphism from $F^{(q)}$ to F:

$$g(F^{(q)}(X^q, Y^q)) = g(F(X,Y)^q) = f(F(X,Y)) = F(f(X), f(Y)) = F(g(X^q), g(Y^q)).$$

Which means $g(F^{(q)}(X,Y)) = F(g(X), g(Y))$. Thus if $g'(T) = 0$, by item1, $g(T) = g_1(T^p)$, contradicting $h = \mathrm{ht}(f)$. □

Prop. (9.5.5.3). Let $F \xrightarrow{f} G \xrightarrow{g} H$ be homomorphisms of formal group laws over ring R of characteristic $p > 0$, then $\mathrm{ht}(g \circ f) = \mathrm{ht}(f) + \mathrm{ht}(g)$. ⌟

Proof: Let $f(T) = f_1(T^{p^{\mathrm{ht}(f)}})$, $g(T) = g_1(T^{p^{\mathrm{ht}(g)}})$, where $f_1(0) \neq 0, g_1(0) \neq 0$ by(9.5.5.2), then

$$g \circ f(T) = g_1(f_1(T^{p^{\mathrm{ht}(f)}})^{p^{\mathrm{ht}(g)}}) = g_1(\widetilde{f}_1(T^{p^{\mathrm{ht}(f)+\mathrm{ht}(g)}}))$$

where $g_1(0)\widetilde{f}_1(0) \neq 0$, thus by(9.5.5.2) again, $\mathrm{ht}(g \circ f) = \mathrm{ht}(f) + \mathrm{ht}(g)$. □

6 p-divisible Groups

Def. (9.5.6.1)[Λ-Formal Schemes]. Let Λ be a local complete Noetherian ring and A_Λ^f be the category of finite length(Artinian) Λ-algebra,

Then a **Λ-formal functor** is a functor $A_\Lambda^f \to \mathcal{S}\mathrm{et}$.

The **formal completion** of a functor $A_\Lambda \to \mathcal{S}\mathrm{et}$ is its restriction on A_Λ^f. We denote the formal completion of $\operatorname{Spec} A$ by $\operatorname{Spf} A$.

Then a **Λ-formal scheme** is a filtered colimits of functors $\varinjlim \operatorname{Spf} A_i$, or equivalently a profinite Λ-algebra $A = \varprojlim A_i$ with profinite topology. ⌟

Def. (9.5.6.2)[Λ-Formal Group Schemes]. A **Λ-formal group** is a Λ-formal scheme with values in groups. ⌟

Def. (9.5.6.3) [p-Divisible Formal Lie Group Schemes]. A **formal Lie group** $\mathcal{G}$ over Λ is a connected formally smooth Λ-formal group. It is necessarily isomorphic to $\mathcal{G} = \operatorname{Spf} \Lambda[[X_1, \ldots, X_n]]$ where $n = \dim \mathcal{G}$. The number n is called the **dimension** of $\mathcal{G}$.

A **p-divisible formal Lie group** is a commutative formal Lie group $\mathcal{G} = \operatorname{Spf} \Lambda[[X_1, \ldots, X_n]]$ that multiplication by $p : [p]^*$ is a finite flat morphism on $\Lambda[[X_1, \ldots, X_n]]$. ⌟

Def. (9.5.6.4) [p-Divisible Groups]. Let p be a prime and S a scheme, a **p-divisible group** is a commutative group functor on Sch_{fppf}/S that

- G is p-divisible: $[p]_G$ is an epimorphism.
- G is p-torsion: $G = \varinjlim_n G(n)$, where $G(n) = \ker([p]_G : G \to G)$.
- $G(n)$ are representable as sheaves on Sch_{fppf}/S.

The category of p-divisible groups over S is denoted by $pdiv(S)$. ⌟

Prop. (9.5.6.5) [Equivalent Definitions of p-Divisible Groups]. Let p be a prime and S a scheme, then a p-divisible group over S is an ind system (G_v, i_v) of finite commutative groups schemes over S s.t.

- $0 \to G_v \xrightarrow{i_v} G_{v+1} \xrightarrow{p^v} G_{v+1}$ is an exact sequence of group schemes over S.
- the rank of fiber of $G(n)$ at $s \in S$ is $p^{nh(s)}$ where h is a locally constant function on S.

and (G_v, i_v) is called a **p-divisible group of height** h over S. ⌟

Proof: Cf.[Shatz, P61], [P-Divisible Groups, Haoran Wang]. □

Prop. (9.5.6.6) [Connected p-Divisible Groups and Formal Lie Groups]. Cf.[Shatz, P62]. ⌟

Def. (9.5.6.7) [Tate Module]. Let G be a p-divisible group over an integral domain $\mathcal{O}$ with fraction field K of characteristic 0, then the **Tate module** of G is defined to be

$$T_p(G) = \varprojlim_n G_n(\overline{K}),$$

and the **Tate comodule** of G is defined to be

$$\Phi_p(G) = \varinjlim_n G_n(\overline{K}).$$

⌟

Hodge-Tate Decomposition

Prop. (9.5.6.8) [Hodge-Tate Decomposition]. If $\mathcal{O}$ is a CDVR of mixed characteristic with perfect residue field k and fraction field K, then there is an isomorphism of f.d. $\mathbb{Q}_p$-representation of G_K:

$$T_p(G) \otimes_{\mathbb{Z}_p} \widehat{\overline{\mathbb{Q}_p}} \cong \textit{tangent} \oplus \textit{cotangent spaces of } G.$$

⌟

Proof: Cf.[p-divisible Groups, Morrow]. □

9.6 Algebraic Stacks

Basic references are [Sta], [Ols16], [Vis08] and [Fibered Category to Algebraic Stacks, Lamb].

Notation (9.6.0.1).

- Use notations as in Sites, Sheaves, Topoi and Stacks.
- Fix $S \in \mathcal{S}\mathrm{ch}$. A fibered category/stack over S means a fibered category/stack over $\mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/S$(obsolete).

⌟

1 Schemes as Functors

Prop. (9.6.1.1) [Strong Yoneda Lemma]. For any $S \in \mathcal{S}\mathrm{ch}$, the functor

$$\mathcal{S}\mathrm{ch}_S \to \mathcal{S}\mathrm{h}_{\mathrm{fpqc}}/S \to \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{A}\mathrm{ff}_{\mathrm{fpqc}}/S) \to \mathcal{P}\mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{A}\mathrm{ff}_S) : X \mapsto (\text{よ}(X) : \operatorname{Spec} R \mapsto \operatorname{Mor}_S(\operatorname{Spec} R, X))$$

is a fully faithful embedding of the categories. ⌟

Proof: (6.1.2.25) applied to $\mathcal{A}\mathrm{ff}_{\mathrm{fpqc}}/S \to \mathcal{S}\mathrm{ch}_{\mathrm{fpqc}}/S$ implies the restriction map $\mathcal{S}\mathrm{h}_{\mathrm{fpqc}}/S \to \mathcal{S}\mathrm{h}(\mathcal{A}\mathrm{ff}_{\mathrm{fpqc}}/S)$ is an equivalence, thus the assertion follows from Yoneda lemma and the fact $\mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{A}\mathrm{ff}_{\mathrm{fpqc}}/S) \to \mathcal{P}\mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{A}\mathrm{ff}_S)$ is fully faithful. □

Def. (9.6.1.2) [Closed Subfunctors]. Let $S \in \mathcal{S}\mathrm{ch}$ and Z be a subfunctor of $X \in \mathcal{P}\mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{A}\mathrm{ff}_S)$. Z is called a **closed subfunctor** of X if for any $T \in \mathcal{A}\mathrm{ff}_S$, $f \in \operatorname{Mor}(h_T, X)$, the functor $Z \otimes_X h_T$ is represented by a closed subscheme of T. ⌟

Prop. (9.6.1.3) [Closed Subfunctor of Schemes]. Let $S \in \mathcal{S}\mathrm{ch}$ and $X \in \mathcal{S}\mathrm{ch}_S$, then the closed subfunctors of $\widetilde{X}$(9.6.1.2) are exactly of the form $\widetilde{Z}$ for a closed subscheme $\widetilde{Z}$ of $\widetilde{X}$. ⌟

Proof: If Z is a closed subscheme of X, then for any $f : h^A \to X$, $f^{-1}(Z)$ is the pullback of Z along $\operatorname{Spec} A \to X$, so it is a closed subscheme of $\operatorname{Spec} A$. Conversely, if Z is a closed subfunctor of X, then for each affine open subset U of X, $Z \cap h_U$ is represented by a quotient of $\mathcal{O}(U)$ by some ideal $\mathcal{I}(U)$. Because of the uniqueness, $\mathcal{I}(U)$ and $\mathcal{I}(U')$ coincides on the intersection $U \cap U'$, thus $U \mapsto \mathcal{I}(U)$ defines a sheaf of ideals $\mathcal{I}$ on X.

Now $Z = h_{Z'}$, where Z' is the closed subscheme of X defined by $\mathcal{I}$, because for any $\operatorname{Spec} R \to X$, the pullback of Z and Z' to R are the same, because they are all closed subschemes of $\operatorname{Spec} R$ and they are equal on an open covering of $\operatorname{Spec} R$(The pullback of the open coverings of X). Now if $\operatorname{Spec} R \to X$ is represented by an element $\alpha \in X(R)$, $Z \times_X h^R(R)$ is the set $\{\varphi \in \operatorname{Hom}(R, R) | X(\varphi)(\alpha) \in Z(R)\}$. So $\mathrm{id}_R \in Z \times_X h^R(R) \iff \alpha \in Z(R)$/ From this we see that $Z(R) = Z'(R)$ for any R. □

Def. (9.6.1.4) [Open Subfunctors]. Let $S \in \mathcal{S}\mathrm{ch}$ and Z be a subfunctor of $X \in \mathcal{P}\mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{A}\mathrm{ff}_S)$. Z is called an **open subfunctor** of X if for any $T \in \mathcal{A}\mathrm{ff}_S$, $f \in \operatorname{Mor}(h_T, X)$, the functor $U \otimes_X h_T$ is represented by an open subscheme of T. ⌟

Prop. (9.6.1.5) [Open Subfunctor of Schemes]. Let $S \in \mathcal{S}\mathrm{ch}$ and $X \in \mathcal{S}\mathrm{ch}_S$, then closed subfunctors of $\widetilde{X}$(9.6.1.2) are exactly of the form $\widetilde{U}$ for an open subscheme $\widetilde{Z}$ of $\widetilde{X}$. ⌟

Proof: The proof is exactly the same as that of(9.6.1.3). □

Def. (9.6.1.6) [Open Coverings by Functors]. Let $S \in \mathcal{S}\mathrm{ch}$, an **open covering of a functor** $X \in \mathcal{P}\mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{S}\mathrm{ch}_S)$ is a family of open subfunctors $\{U_i\}$ that for any $T \in \mathcal{A}\mathrm{ff}_S$, $h_T \times_X U_i$ is an open covering of T. ⌟

Prop. (9.6.1.7) [Open Coverings of Schemes]. Let $S \in \mathcal{S}\mathrm{ch}$ and $X \in \mathcal{S}\mathrm{ch}_S$, then open coverings of the functor $\widetilde{X}$ are exactly open coverings of X. ⌟

Proof: The proof is exactly the same as that of(9.6.1.3). □

Prop. (9.6.1.8). The pullback of a closed subfunctor is also a closed subfunctor. The intersection of closed subfunctors is a closed subfunctor. ⌟

Lemma (9.6.1.9). Let k be a field and $B \in \mathcal{CA}\mathrm{lg}_k$, $X \in \mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{CA}\mathrm{lg}_B)$, define

$$X_* \in \mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{CA}\mathrm{lg}_k) : X_*(R) = X(R \otimes_k B).$$

Then if Z is a closed subfunctor of X, Z_* is also a closed subfunctor of X_*. ⌟

Proof: Let A be a k-algebra, and $\alpha \in X_*(A)$. To prove Z_* is closed in X_*, we need to show there exists an ideal $\mathfrak{a} \subset A$ that for any homomorphism $\varphi : A \to R$,

$$X_*(\varphi)(\alpha) \in Z_*(R) \iff \varphi(\mathfrak{a}) = 0.$$

Because Z is closed in X, there exists an ideal $\mathfrak{b}$ of $A \otimes_k B$ that for any $\varphi : A \to R$,

$$X(\varphi \otimes B)(\alpha) \in Z_*(R) \iff (\varphi \otimes B)(\mathfrak{b}) = 0.$$

Now by(5.1.1.27), there is an ideal $\mathfrak{a} \subset A$ that an ideal I of A satisfies $\mathfrak{b} \subset I \otimes B \iff \mathfrak{a} \subset I$, thus we are done. □

Prop. (9.6.1.10). Let $S \in \mathcal{S}\mathrm{ch}$, $X \in \mathcal{PS}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{A}\mathrm{ff}/S)$ and Z a closed subfunctor of X. If $Y \in \mathcal{S}\mathrm{ch}_R$, then $\underline{\mathrm{Mor}}(よ(Y), Z)$ is a closed subfunctor of $\underline{\mathrm{Mor}}(よ(Y), X)$. ⌟

Proof: If $Y = h^B$, then $\underline{\mathrm{Mor}}(Y, X)(R) = X(B \otimes R)$, thus the conclusion follows from(9.6.1.9). For a general Y, let Y_i be an affine open covering of Y, then there are maps $\rho_i : \underline{\mathrm{Hom}}(Y, X) \to \underline{\mathrm{Hom}}(Y_i, X)$. Now $\underline{\mathrm{Hom}}(Y_i, Z)$ is closed subfunctor of $\underline{\mathrm{Hom}}(Y_i, X)$, thus we are done if we can show that $\underline{\mathrm{Hom}}(Y, Z) = \cap_i \rho_i^{-1}(\underline{\mathrm{Hom}}(Y_i, Z))$. But this is equivalent to any map $Y_R \to X_R$ that maps $(Y_i)_R$ into Z_R maps Y_R into Z_R, which is clear. □

Def. (9.6.1.11) [Fat Subfunctors]. Let $S \in \mathcal{S}\mathrm{ch}$ and $\mathcal{F} \in \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{A}\mathrm{ff}_{\mathrm{fppf}}/S)$, then a subfunctor D of $\mathcal{F}$ is called a **fat subfunctor** if the shification of D w.r.t. the fppf topology is just $\mathcal{F}$. ⌟

Prop. (9.6.1.12) [Extending Group Structures]. Let $S \in \mathcal{S}\mathrm{ch}$, $\mathcal{F} \in \mathcal{S}\mathrm{h}^{\mathcal{G}\mathrm{rp}}(\mathcal{A}\mathrm{ff}_{\mathrm{fppf}}/S)$ and D a fat subfunctor of $\mathcal{F}$, then every group structure on D extends uniquely to a group structure on $\mathcal{F}$ by shification. ⌟

2 Algebraic Spaces

Def. (9.6.2.1) [Schematic Morphism]. A **schematic morphism** of fibered categories $\mathcal{X} \to \mathcal{Y} \in \mathcal{F}\mathrm{ib}\mathcal{C}\mathrm{at}^{\mathcal{G}\mathrm{rpd}}(\mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/S)$ over S is a representable morphism of fibered categories over $\mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/S$(4.2.3.36). ⌟

Def. (9.6.2.2) [Properties of Schematic Morphisms]. For a property $\mathscr{P}$ of maps of schemes that is fppf-local on the target and stable under base change, we say that $\mathscr{P}$ holds for a schematic map(9.6.2.1) $\mathcal{X} \to \mathcal{Y} \in \mathcal{F}\mathrm{ib}\mathcal{C}\mathrm{at}(\mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/S)$ if for any $S \in \mathcal{S}\mathrm{ch}$, $\mathscr{P}$ holds for the map $S \times_{\mathcal{Y}} \mathcal{X} \to S$.

It is easy to show that this definition is compatible with that of schemes when $\mathcal{X}, \mathcal{Y} \in \mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/S$. ⌟

Prop. (9.6.2.3) [Descent for Properties]. Let $f : \mathcal{X} \to \mathcal{Y} \in \mathcal{PSh}^{\mathcal{Set}}(\mathcal{Sch}_{\mathrm{fppf}}/S)$ be a schematic morphism and $g : \mathcal{Z} \to \mathcal{Y} \in \mathcal{PSh}^{\mathcal{Set}}(\mathcal{Sch}_{\mathrm{fppf}}/S)$. If $g^{\#}$ is an epimorphism, then f has $\mathscr{P}$ iff $\mathcal{X} \times_{\mathcal{Y}} \mathcal{Z} \to \mathcal{Z}$ has $\mathscr{P}$. ⌟

Proof: Cf.[Sta]03KD. □

Prop. (9.6.2.4) [Properties of Diagonals]. For $\mathcal{F} \in \mathcal{PSh}^{\mathcal{Set}}(\mathcal{Sch}_{\mathrm{fppf}}/S)$, the following are equivalent:

- $\Delta_{\mathcal{F}}$ is schematic.
- For any $U \in \mathcal{Sch}_{\mathrm{fppf}}/S$ and $a \in \mathcal{F}(U)$, the map $a : よ(U) \to \mathcal{F}$ is representable.
- For any $U, V \in \mathcal{Sch}_{\mathrm{fppf}}/S$ and $a \in \mathcal{F}(U), b \in \mathcal{F}(V)$, the fiber product $よ(U) \times_{a,\mathcal{F},b} よ(V)$ is representable.

Moreover, $\Delta_{\mathcal{F}}$ has a property $\mathscr{P}$ iff for any $U, V \in \mathcal{Sch}_{\mathrm{fppf}}/S$ and $a \in \mathcal{F}(U), b \in \mathcal{F}(V)$, the map $よ(U) \times_{a,\mathcal{F},b} よ(V) \to U \times V$ has property $\mathscr{P}$. ⌟

Proof: Cf.[Sta]025W, 0CBT. □

Prop. (9.6.2.5). If a schematic morphism $f : \mathcal{X} \to \mathcal{Y} \in \mathcal{PSh}^{\mathcal{Set}}(\mathcal{Sch}_{\mathrm{fppf}}/S)$ is flat, loc.p. and surjective, then f is an epimorphism. ⌟

Proof: Cf.[Sta]05VM. □

Algebraic Spaces

Def. (9.6.2.6) [Algebraic Space]. An **algebraic space** is a sheaf $\mathcal{F} \in \mathcal{Sh}_{\mathrm{fppf}}/S$ that the diagonal is schematic, and there exists some scheme $U \in \mathcal{Sch}/S$ with an étale surjective map $よ(U) \to \mathcal{F}$ in $\mathcal{Sch}_{\mathrm{fppf}}/S$, called an **atlas for the algebraic space** $\mathcal{F}$.

The category of algebraic spaces is the full subcategory of $\mathcal{Sh}_{\mathrm{fppf}}/S$, denoted by $\mathcal{AlgSp}/S$. ⌟

Prop. (9.6.2.7) [Schemes as Algebraic Spaces]. $よ : \mathcal{Sch}/S \to \mathcal{AlgSp}/S$ is a fully faithful embedding. ⌟

Proof: For $X \in \mathcal{Sch}/S$, h_X is a sheaf because fppf site is subcanonical by(6.1.4.34), its diagonal is representable, and the identity $\mathrm{id}_X : X \to X$ is surjective and étale. □

Remark (9.6.2.8). In general, the quotient of a scheme by a finite group action is an algebraic space that is not a scheme. Naively one can think of algebraic spaces as quotients of schemes by finite groups. ——Kollar. ⌟

Def. (9.6.2.9) [Sites over Algebraic Spaces]. The Zariski/étale/smooth/fppf/... sites over an algebraic space is defined verbatim as that of over algebraic schemes. ⌟

Prop. (9.6.2.10) [Algebraic Spaces and Étale Equivalence Relations]. Cf.[Sta]02WW. ⌟

Proof: □

Prop. (9.6.2.11). If $\mathcal{X}$ is an algebraic space over S, then the diagonal map $\Delta_{\mathcal{X}/S}$ is locally of finite type, locally quasi-finite, separated and is a monomorphism. ⌟

Proof: Cf.[Sta]02X4. □

Def. (9.6.2.12) [Underlying Space of Algebraic Spaces]. For $\mathcal{X} \in \mathcal{AlgSp}/S$, the underlying space $|\mathcal{X}|$ is a topological space whose points are the equivalence classes of morphisms $\operatorname{Spec} K \to \mathcal{X} \in \mathcal{Sh}_{\mathrm{fppf}}/S$, where $K \in \mathtt{Field}$. ⌟

Prop. (9.6.2.13). Let $\mathcal{X} \in \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}/S, T \in \mathcal{S}\mathrm{ch}/S, f : T \to \mathcal{X} \in \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}/S$, then f is surjective iff $|f| : |T| \to |X|$ is surjective. ⌟

Proof:

□

3 Morphisms between Algebraic Spaces

Remark (9.6.3.1). We need to define properties for not necessarily schematic morphisms, and it should be compatible with(9.6.2.2). ⌟

Open Morphisms

Def. (9.6.3.2) [Open Morphisms]. For a representable morphism $f : X \to Y \in \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}/S$, the following are equivalent:

- f is universally open(9.6.2.2).
- For any $Z \to Y \in \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}/S$, $|Z \times_Y X| \to |Z|$ is open.

Thus we can define an **open morphism of algebraic spaces** to be a morphism $f : X \to Y \in \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}/S$ s.t. $|f| : |X| \to |Y|$ is open. This is compatible with the definition before. ⌟

Proof: Cf.[Sta]. 03Z1. □

4 Algebraic Stacks

References are [Sta].

Def. (9.6.4.1)[Representable by Algebraic Spaces]. A morphism $f : \mathcal{X} \to \mathcal{Y} \in \mathcal{F}\mathrm{ib}\mathcal{C}\mathrm{at}^{\mathcal{G}\mathrm{rpd}}{}_{\mathrm{fppf}}/S$ is called **representable by algebraic spaces** if for any $T \in \mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/S$ and a morphism $(\mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/U) \to \mathcal{Y}$, the fibered category $(\mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/T) \times_{\mathcal{Y}} \mathcal{X}$ is equivalent to an algebraic space over T(9.6.2.6).(Notice it is a fibered category by(4.2.3.15) and(4.2.3.16)) ⌟

Def. (9.6.4.2) [Properties of Morphisms Representable by Algebraic Spaces]. For a property $\mathcal{P}$ of maps of schemes that is fppf-local and stable under base change, we say that $\mathcal{P}$ holds for a morphism $f : \mathcal{X} \to \mathcal{Y} \in \mathcal{F}\mathrm{ib}\mathcal{C}\mathrm{at}^{\mathcal{G}\mathrm{rpd}}(\mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/S)$ representable by algebraic spaces(9.6.4.1) iff for any $U \in \mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/S$, $\mathcal{P}$ holds for the map of algebraic spaces $U \times_{\mathcal{Y}} \mathcal{X} \to U \in \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}/S$(in the sense of Morphisms between Algebraic Spaces). ⌟

Prop. (9.6.4.3)[Properties Under Equivalences]. Having properties are stable under equivalences. Cf.[Sta]0459.**?** ⌟

Def. (9.6.4.4) [2-Category of Algebraic Stack]. An **algebraic stack** is a stack in groupoids $\mathcal{X} \in \mathcal{S}\mathrm{ta}^{\mathcal{G}\mathrm{rpd}}{}_{\mathrm{fppf}}/S$ that the diagonal is representable by an algebraic space(9.6.4.1), and there exists some scheme $U \in \mathcal{S}\mathrm{ch}/S$ with a smooth surjective map $\mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/U \to X$ in $\mathcal{S}\mathrm{ta}_{\mathrm{fppf}}/S$, called an **atlas for the algebraic stack** X.

It is called a **Deligne-Mumford stack** if moreover there exists some $U \in \mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/S$ with a smooth étale map $\mathcal{S}\mathrm{ch}_{\mathrm{fppf}}/U \to \mathcal{X}$ in $\mathcal{S}\mathrm{ta}_{\mathrm{fppf}}/S$.

The 2-category of algebraic(resp. Deligne-Mumford) stacks is the full sub-2-category of $\mathcal{S}\mathrm{ta}_{\mathrm{fppf}}/S$, denoted by $\mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{ta}/S$(resp. $\mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{ta}^{\mathrm{DM}}/S$). ⌟

Prop. (9.6.4.5). If $X, Y \in \mathcal{C}\mathrm{at}(\mathcal{S}\mathrm{ch}/S)$ are equivalent, then $\mathcal{X} \in \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}/S$(resp. $\mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{ta}^{\mathrm{DM}}/S$) iff so is $\mathcal{Y}$. ⌟

Proof: By(6.1.3.7), $\mathcal{Y}$ is also a stack in groupoid. And Δ_Y is equivalent to Δ_X, and notice that having property $\mathscr{P}$ is stable under equivalences(9.6.4.3). □

Prop. (9.6.4.6)[2-Fibered Products of Algebraic Stacks]. The 2-category $\mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}/S$ has 2-fibered products. ⌟

Proof: Cf.[Sta]04TF. □

Prop. (9.6.4.7) [Algebraic Stacks and Étale Groupoid Object]. There is a bijection of étale groupoid objects on a scheme with the category of algebraic stacks. ⌟

Proof: Cf.[Lamb, P39]. □

Prop. (9.6.4.8)[Algebraic Spaces and Étale Equivalence Relations]. There is a bijection of étale equivalence relations on a scheme with the category of algebraic spaces. ⌟

Proof: This is a corollary of(9.6.4.7). □

5 Sheaves on Algebraic Stacks

6 Representability

7 Artin's Axioms

8 Quot and Hilbert Stacks

9 Properties of Algebraic Stacks

10 Morphisms of Algebraic Stacks

11 Limits of Algebraic Stacks

12 Cohomology of Algebraic Stacks

13 Derived Categories of Stacks

9.7 Moduli Problems

References are [Sta]and [Stacks and Moduli, Alper].

Representability

Prop. (9.7.0.1) [A Representability Criterion]. Let $\mathcal{F} \in \mathcal{S}\mathrm{h}^{\mathcal{S}\mathrm{et}}(\mathcal{S}\mathrm{ch}_{\mathrm{Zar}})$ and there is a covering $F = \cup F_i$ by open subfunctors(9.6.1.4)(9.6.1.6) that are representable by schemes, then F is representable by a scheme. ⌟

Proof: Let (X_i, ξ_i) represents F_i, where $\xi \in F_i(X_i)$. Because $F_j \subset F$ is representable by open immersion, there are open subsets $U_{ij} \subset X_i$ that $T \to X_i$ factors through U_{ij} iff $\xi|_T \in F_j(T)$. In particular, $\xi_i|_{U_{ij}} \subset F_j(U_{ij})$, and therefore there is a canonical map $\varphi_{ij} : U_{ij} \to X_j$ that $\varphi_{ij}^*\xi_j = \xi_i|_{U_{ij}}$. By definition of U_{ji} this map factors through U_{ji}.

For the rest, Cf.[Sta]01JJ.**?** □

Cor. (9.7.0.2) [Representing Group Functors]. Let $S \in \mathcal{S}\mathrm{ch}$ and $\mathcal{G} \in \mathcal{S}\mathrm{h}^{\mathcal{G}\mathrm{rp}}(\mathcal{A}\mathrm{ff}_{\mathrm{Zar}}/S)$ and there is an open subfunctor $\mathcal{F} \subset \mathcal{G}$ s.t. for any $\mathrm{Spec}\, K \in \mathcal{A}\mathrm{ff}_S$ where K is a field and $g \in \mathcal{G}(K)$, there exists a $g' \in G(k)$ s.t. $gg' \in \mathcal{F}(K)$, then $\mathcal{G}$ is representable. ⌟

Proof: For any $g \in G(S)$, let $F_g = \tau_g^* F$, then $F_g \cong F$ and are also open subfunctors of $\mathcal{G}$. then $\{F_g \to G\}$ is an open covering because for any $T \in \mathcal{S}\mathrm{ch}$ and $\xi \in \mathrm{Mor}(h_T, \mathcal{G})$, $F_g \times_{\mathcal{G}} h_T$ is represented by open subschemes of T, and it must covers T because otherwise there are some map $\mathrm{Spec}\, k(x) \to T$ s.t. $F_g \times_{\mathcal{G}} h_{k(x)}$ are all empty, contradicting the hypothesis. Thus the assertion follows from(9.7.0.1). □

Prop. (9.7.0.3) [$\underline{\mathrm{Hom}}(\mathcal{E}, \mathcal{F})$ for Coherent Sheaves]. Let S be a locally Noetherian scheme and X a projective scheme over S. Let $\mathcal{E}, \mathcal{F}$ be coherent sheaves on X and $\mathcal{F}$ is flat, then the functor

$$\underline{\mathrm{Hom}}(\mathcal{E}, \mathcal{F}) : \mathcal{S}\mathrm{ch}_S \to \mathcal{S}\mathrm{et} : T \mapsto \mathrm{Hom}_T(\mathcal{E}_T, \mathcal{F}_T)$$

is representable by a vector bundle $\mathbf{V}$ over S(6.5.2.21). ⌟

Proof: Cf.[Kle05]P16. □

Cor. (9.7.0.4). For any $f \in \mathrm{Hom}(\mathcal{E}, \mathcal{F})$, f corresponds to a morphism $X \to \mathbf{V}$, then the inverse image of $\mathbf{V}_0 \subset \mathbf{V}$ in X is the closed subscheme X' with the universal property that for any $\varphi : T \to X$, $\varphi^* f = 0$ iff φ factors through X'. ⌟

Coarse Moduli Schemes

Def. (9.7.0.5) [Coarse Moduli Schemes]. For $k \in$ `Field` and $\mathcal{F} : \mathcal{S}\mathrm{ch}/k \to \mathcal{S}\mathrm{et}$, a **coarse moduli scheme** for $\mathcal{F}$ is a scheme $Z \in \mathcal{S}\mathrm{ch}/k$ with a morphism $\varphi : \mathcal{F} \to よ_Z$ satisfying the following universal property: for any $T \in \mathcal{S}\mathrm{ch}/k$,

$$\mathrm{Hom}(\mathcal{F}, よ_T) = \mathrm{Hom}(Z, T).$$

And Z is called a **fine moduli scheme** for $\mathcal{F}$ if φ is an isomorphism. ⌟

1 Hilbert & Quot Schemes

References are [Nit05]. For simplicity, we restrict to the category of locally Noetherian schemes over S, and assume X/S is separated.

Def. (9.7.1.1) [Hilbert Functors]. Let $X \in \mathcal{S}\mathrm{ch}_S$, then the **Hilbert functor** is the functor

$$\underline{\mathrm{Hilb}}_{X/S} : \mathcal{S}\mathrm{ch}_S \to \mathcal{S}\mathrm{et} : T \mapsto \{\text{closed subschemes of } X_T \text{ that is flat over } T\}.$$

⌟

Def. (9.7.1.2) [Quot Functors]. Let $S \in \mathrm{N}\,\mathcal{S}\mathrm{ch}$, $f : X \to S \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}}/S$ and $\mathcal{E} \in \mathcal{C}\mathrm{oh}(X)$, then for any $T \in \mathcal{S}\mathrm{ch}_S$, define a **family of quotients of $\mathcal{E}$ parametrized by T** to be a pair $(\mathcal{F}, q)$ where

- $\mathcal{F} \in \mathcal{C}\mathrm{oh}(X_T)$ s.t. $\mathrm{Supp}(\mathcal{F})$ is proper over T.
- $q : \mathcal{E}_T \to \mathcal{F}$ is a surjective homomorphism of sheaves.

Then the **Quot functor** is the functor

$$\underline{\mathrm{Quot}}_{\mathcal{E}/X/S} : \mathcal{S}\mathrm{ch}_S \to \mathcal{S}\mathrm{et} : T \mapsto \{\text{isomorphism classes of family of quotients of } \mathcal{E} \text{ parametrized by } T\}.$$

⌟

Cor. (9.7.1.3) [Hilbert Functors as Quot Functors]. $\underline{\mathrm{Hilb}}_{X/S} = \underline{\mathrm{Quot}}_{\mathcal{O}_X/X/S}$. ⌟

Prop. (9.7.1.4) [$\underline{\mathrm{Quot}}_{\mathcal{F}/X/S}$ are Fpqc Sheaves]. $\underline{\mathrm{Quot}}_{\mathcal{F}/X/S}$ is a fpqc sheaf over $\mathcal{S}\mathrm{ch}$. ⌟

Proof: This follows from the fact $\mathcal{QC}\mathrm{oh}/\mathcal{S}\mathrm{ch}$ is a fpqc sheaf(6.1.5.12). □

Prop. (9.7.1.5) [Stratification by Hilbert Polynomials]. Let $\mathcal{L} \in \mathrm{Pic}(X_T)$, then for any $t \in T$, the Hilbert polynomial of $\mathcal{F}_t$ w.r.t. the line bundle $\mathcal{L}_t$ on X_t is locally constant on T**?**, and is stable under extension of residue fields, thus we can define $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S}$ to represent the subfunctor of $\underline{\mathrm{Quot}}_{\mathcal{E}/X/S}$ consisting of pairs $(\mathcal{F}, q)$ s.t. $\mathcal{F}_t$ has Hilbert polynomial Φ w.r.t. $\mathcal{L}_t$ for all $t \in T$.

Thus if each $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S}$ is representable, $\underline{\mathrm{Quot}}_{\mathcal{E}/X/S}$ is also representable, and there is a decomposition

$$\underline{\mathrm{Quot}}_{\mathcal{E}/X/S} = \coprod_{\Phi \in \mathbb{Q}[\lambda]} \underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S}.$$

⌟

Prop. (9.7.1.6) [Valuation Criterion]. Let $X \to S$ be proper, then the morphism of functors $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S} \to h_S$ satisfies the discrete valuation criterion for properness. ⌟

Proof: The valuation criterion says if R is a valuation ring with fraction field K with a morphism $\mathrm{Spec}\, R \to S$, then any pairs $(\mathcal{F}_K, q_K)$ where $\mathcal{F}_K \in \mathcal{C}\mathrm{oh}(X_K)$ and $q_K : \mathcal{E}_K \to \mathcal{F}_K$ a surjection can extends uniquely to a surjective map $q_R : \mathcal{E}_R \to \mathcal{F}_R \in \mathcal{C}\mathrm{oh}(X_R)$ s.t. $\mathcal{F}_R$ is flat over R.

For this, let $j : X_K \to X_R$ be the open immersion, take $\mathcal{F}_R$ to be the image of the map $\mathcal{E}_R \to i_*\mathcal{E}_K \xrightarrow{i_* q_K} i_*\mathcal{F}_K$, then $i^*\mathcal{F}_R = \mathcal{F}_K$, and $\mathcal{F}_R$ is flat over R because it is torsion-free(5.4.1.12). Notice the properness of X/S is used to show that $\mathrm{Supp}(\mathcal{F}) \subset X_R$ is proper over R. □

Lemma (9.7.1.7) [Preliminary Reductions]. Situation as in(9.7.1.2), then

- Let $\nu \in \mathbb{Z}$, then tensoring $\mathcal{L}^\nu$ gives an isomorphism of functors $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S} \cong \underline{\mathrm{Quot}}^{\Psi,\mathcal{L}}_{\mathcal{E}(\nu)/X/S}$, where $\Psi(\lambda) = \Phi(\lambda + \nu)$.

- Let $\varphi : \mathcal{E} \to \mathcal{G}$ be a surjective homomorphism in $\mathfrak{Coh}(X)$, then the corresponding natural transformation $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{G}/X/S} \to \underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S}$ is a closed subfunctor.
- If X/S is proper, let $i : U \to X$ be an open subscheme, then $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{i^*\mathcal{E}/U/S}$ is an open subfunctor of $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S}$.

⌟

Proof: 1 is obvious.

2: It suffices to show for any locally Noetherian scheme $T \in \mathcal{S}\mathrm{ch}_S$ and a pair $(\mathcal{F}, q) \in \underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S}(T)$, there exists a closed subscheme T' of T s.t. for any locally Noetherian scheme U and $f : U \to T$, $q_U : \mathcal{E}_U \to \mathcal{F}_U$ factors through $\mathcal{G}_U$ iff f factors through T'. For this, just take T' to be the vanishing scheme of $\ker(\varphi_T) \to \mathcal{E}_T \to \mathcal{F}_T$(9.7.0.4)(or by direct verification).

3: Firstly the natural transformation $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{i^*\mathcal{E}/U/S} \to \underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S}$ is given by

$$\eta_T : (\mathcal{F}, i^*\mathcal{E}_T \to \mathcal{F}) \mapsto (\mathrm{Im}(\mathcal{E}_T \to i_*\mathcal{F}), \text{adjunction}).$$

Notice restriction is a left inverse to this transformation. Then by inspection, this is an open subfunctor iff for any locally Noetherian scheme $T \in \mathcal{S}\mathrm{ch}_S$ and a pair $(\mathcal{F}, q) \in \underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S}(T)$, for any locally Noetherian scheme Q and $f : Q \to T$, the restriction of $(\mathcal{F}, q)$ to Q is in $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{i^*\mathcal{E}/U/S}(Q)$ iff $\mathcal{F}_Q \to i_{Q*}i_Q^*\mathcal{F}_Q$ is injective.**?** □

Thm. (9.7.1.8) [Grothendieck]. Let $S \in \mathrm{N}\,\mathcal{S}\mathrm{ch}_{\mathrm{qc}}$ and $f : X \to S$ a (quasi-/strongly)projective morphism, $\mathcal{L}$ an f-ample line bundle on X, then for any $\mathcal{E} \in \mathfrak{Coh}(X)$ and $\Phi \in \mathbb{Q}[\lambda]$, the functor $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S}$(9.7.1.5) is representable by a (quasi-/strongly)projective S-scheme. ⌟

Proof: Cf.[Nit05]P24.

For the quasi-projective case, use(9.7.1.7) and the fact any coherent sheaf can be extended. □

Remark (9.7.1.9). Cf.[Hartshorne Appendix B, 3.4.1] has an example of a $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}^3/\mathbb{C}$ with a free $G = \mathbb{Z}/(2)$-action for which the quotient X/G is not a scheme. Which means that $\underline{\mathrm{Hilb}}_{X/\mathbb{C}}$ is not representable by a scheme. ⌟

Cor. (9.7.1.10). Let S be a locally Noetherian scheme and $f : X \to S$ be H-projective, $\mathcal{L} = \mathcal{O}_{\mathbb{P}_S(V)}(1)|_X$, $\mathcal{E}$ a coherent quotient sheaf of $\mathcal{O}_X^{\oplus p}(\nu)$ where $p > 0, \nu \in \mathbb{Z}$, and $\Phi \in \mathbb{Q}[\lambda]$, then he functor $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S}$ is representable by an H-projective S-scheme. ⌟

Lemma (9.7.1.11) [Altman-Kleinman]. Let S be a locally Noetherian scheme and $f : X \to S$ be a closed subscheme of some $\mathbb{P}_S(V)$ where V is a finite locally free sheaf on S, $\mathcal{L} = \mathcal{O}_{\mathbb{P}_S(V)}(1)|_X$, $\mathcal{E}$ a coherent quotient sheaf of $f^*(W)(\nu)$ where W is a finite locally free sheaf on S and $\nu \in \mathbb{Z}$, and $\Phi \in \mathbb{Q}[\lambda]$, then the functor $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S}$ is representable by a projective S-scheme that can be embedded in $\mathbb{P}_S(F)$ for some finite locally free sheaf F on S that is an exterior power of W with a symmetric power of V. ⌟

Proof: Cf.[Nit05]P24. □

Lemma (9.7.1.12). Let S be a locally Noetherian scheme and $f : X = \mathbb{P}_S(V) \to S$ where V is a finite locally free sheaf on S, $\mathcal{L} = \mathcal{O}_{\mathbb{P}_S(V)}(1)$, $\mathcal{E} = f^*(W)(\nu)$ where W is a finite locally free sheaf on S and $\nu \in \mathbb{Z}$, and $\Phi \in \mathbb{Q}[\lambda]$, then the functor $\underline{\mathrm{Quot}}^{\Phi,\mathcal{L}}_{\mathcal{E}/X/S}$ is representable by a projective S-scheme that can be embedded in $\mathbb{P}_S(F)$ for some finite locally free sheaf F on S that is an exterior power of W with a symmetric power of V. ⌟

Proof: Cf.[Nit05]P24. □

Examples of Quot Schemes

Prop. (9.7.1.13) [Projective Spaces]. $\underline{\mathrm{Quot}}^{1,\mathcal{O}_{\mathbb{Z}}}_{\mathcal{O}_{\mathbb{Z}}^{\oplus(n+1)}/\mathbb{Z}/\mathbb{Z}} \cong \mathbb{P}^n_{\mathbb{Z}}$, with the universal element the tautological quotient $\mathcal{O}_{\mathbb{P}^n}^{\oplus(n+1)} \to \mathcal{O}_{\mathbb{P}^n}(1)$.

Moreover, if $\mathcal{E} \in \mathfrak{Coh}^{\text{free}}(S)$, then $\underline{\mathrm{Quot}}^{1,\mathcal{O}_S}_{\mathcal{E}/S/S} \cong \mathbf{P}(\mathcal{E})$, with the universal element the tautological quotient $\pi^*(\mathcal{E}) \to \mathcal{O}_{\mathbf{P}(\mathcal{E})}(1)$. ⌟

Proof: For any surjective map $\mathcal{E}_T \to \mathcal{L}$ where $\mathcal{L}$ is a line bundle, locally $H^0(\mathcal{L}) \cong H^0(\mathcal{E}_T)$ is of dimension n and thus $\mathcal{L}$ is basepoint-free. Now the associated map $\varphi_{\mathcal{L}} : T \to \mathcal{O}_{\mathbf{P}(\mathcal{E})}$ **?** pulls $\mathcal{O}_{\mathbf{P}(\mathcal{E})}(1)$ to $\mathcal{L}$. □

Def. (9.7.1.14) [Relative Grassmannians]. Let $\mathcal{E} \in \mathfrak{Coh}(S)$, define the **relative Grassmannian of** $\mathcal{E}$ to be $\mathrm{Gra}_S(\mathcal{E}, k) = \underline{\mathrm{Quot}}^{k,\mathcal{O}_S}_{\mathcal{E}/S/S}$.

Then if $\mathcal{E}$ is finite locally free, it is a quotient of the group scheme $\mathrm{GL}(n)_S$, and when $\mathcal{E} \cong \mathcal{O}_S^n$ and $S = \mathbb{Z}$, this is just the Grassmannian variety $\mathrm{Gra}(n, k)$ defined in(9.2.1.20).

In particular, $\mathrm{Gra}(n + 1, 1) \cong \mathbb{P}^n_{\mathbb{Z}}$ by(9.7.1.13). ⌟

Proof: First we prove for $\mathcal{E}$ finite locally free: There is a natural action of $\mathrm{GL}(n)$ on $\underline{\mathrm{Quot}}^{k,\mathcal{O}_S}_{\mathcal{E}/S/S}$, it is clearly a quotient map, and the kernel is a closed subgroup of $\mathrm{GL}(n)_S$ by(18.5.1.4). Thus $\mathrm{Gra}(\mathcal{E}, k)$ is a quotient of $\mathrm{GL}(n)$ by definition(9.1.1.21).

In general, $\mathcal{E}$ is a locally a quotient of a finite locally free sheaf, thus $\mathrm{Gra}(\mathcal{E}, k)$ is locally projective by(9.7.1.7). □

Prop. (9.7.1.15) [Quotient by Flat Projective Equivalence Relations]. ⌟

Proof: Cf.[Nit05]P31. □

Prop. (9.7.1.16) [Grassmannian Varieties are projective]. The Grassmannian variety $\mathrm{Gra}(\mathcal{E}, k)$ is locally projective, and when $\mathcal{E}$ is locally free, it is projective, and if $\mathcal{E}$ is trivial, it is H-projective. ⌟

Proof: It injects into $\mathbb{P}(\wedge^k\mathcal{E})$ by the natural transformation

$$T_S : (\mathcal{O}_T^n \to \mathcal{Q}) \mapsto (\wedge^k(\mathcal{O}_T^n) \to \wedge^k\mathcal{Q}).$$

In particular, the corresponding very ample line bundle is just $\wedge^k\mathcal{F}$, where $f^*\mathcal{E} \to \mathcal{F}$ is the universal element and $f : \mathrm{Gra}(\mathcal{E}, k) \to S$, by(9.7.1.13). □

Cor. (9.7.1.17) [Grassmannian Varieties and Projective Space]. There is a canonical isomorphism $G(n, n - 1) \cong \mathbb{P}^{n-1}$ identifying sections with surjections from $\mathcal{O}_X^n$. ⌟

Prop. (9.7.1.18) [Flag Varieties]. The flag variety(9.2.1.22) represents the functor $T \mapsto \{$ the isomorphism classes of flags in $\mathcal{O}_T^n$ of the given dimensions$\}$. ⌟

Cor. (9.7.1.19) [Flag Varieties are Projective]. The flag varieties are projective as they are closed subsets of a product of Grassmannian varieties. ⌟

2 Picard Schemes

Main references are [Kle05]. For simplicity, we assume S is locally Noetherian and restrict to the category of locally Noetherian schemes over S, and X/S is separated.

Notice a morphism $X \to S$ is said to have integral geometric fibers if for any alg.closed field k and a morphism $\mathrm{Spec}\, k \to S$, X_k is integral.

Picard Functors

Def. (9.7.2.1) [Picard Functors]. Let $X \in \mathcal{S}\mathrm{ch}_S$, the **Picard functor** is the functor

$$\underline{\mathrm{Pic}}_X : \mathcal{S}\mathrm{ch}_S \to \mathcal{G}\mathrm{rp} : T \mapsto \mathrm{Pic}(X_T) = H^1(X_T, \mathcal{O}^*_{X_T}).$$

The problem of this functor is that it is not a Zariski sheaf.

Define the **relative Picard functor** $\widetilde{\underline{\mathrm{Pic}}}_{X/S} : \mathcal{S}\mathrm{ch}_S \to \mathcal{G}\mathrm{rp} : T \mapsto \mathrm{Pic}(X_T)/\operatorname{pr}_T^*(\mathrm{Pic}(T))$. Let the shifification of this ring in the Zariski/étale/fppf topology denoted by $\underline{\mathrm{Pic}}_{X/S,\mathrm{Zar}}, \underline{\mathrm{Pic}}_{X/S,\text{ét}}, \underline{\mathrm{Pic}}_{X/S}$. Then there are maps of presheaves:

$$\underline{\mathrm{Pic}}_X \to \widetilde{\underline{\mathrm{Pic}}}_{X/S} \to \underline{\mathrm{Pic}}_{X/S,\mathrm{Zar}} \to \underline{\mathrm{Pic}}_{X/S,\text{ét}} \to \underline{\mathrm{Pic}}_{X/S}.$$

⌟

Remark (9.7.2.2). In the following we will frequently use a technical condition s.t. $\mathcal{O}_S \to f_*(\mathcal{O}_X)$ is an isomorphism. This is true when X is a proper variety over S, by(6.11.5.2). ⌟

Prop. (9.7.2.3). Assume $\mathcal{O}_S \cong f_*\mathcal{O}_X$, then the functor $\mathcal{N} \to f^*\mathcal{N}$ is fully faithful from the category of finite locally free sheaves on S to the category of finite locally free sheaves on S s.t. f_* is a left partial inverse. ⌟

Proof: For any finite locally free sheaf $\mathcal{N}$, there is an isomorphism $\mathcal{N} \cong f_*f^*\mathcal{N}$ by checking locally, and for any other finite locally free sheaf $\mathcal{N}'$, $\mathcal{H}om(\mathcal{N}, \mathcal{N}')$ is also finite locally free, thus the natural map $f^*\mathcal{H}om(\mathcal{N}, \mathcal{N}') \to \mathcal{H}om(f^*\mathcal{N}, f^*\mathcal{N}')$ is an isomorphism by checking locally. Thus $\mathrm{Hom}(\mathcal{N}, \mathcal{N}') \cong \mathrm{Hom}(f^*\mathcal{N}, f^*\mathcal{N}')$. □

Def. (9.7.2.4) [Rigidification]. Assume $f : X \to S$ has a section $g : S \to X$, then for any $T \in \mathcal{S}\mathrm{ch}/S$ and $\mathcal{L} \in \mathrm{Pic}(X_T)$, a g**-rigidification of** $\mathcal{L}$ is an isomorphism $u : \mathcal{O}_T \cong g_T^*\mathcal{L}$. ⌟

Prop. (9.7.2.5). Let $f : X \to S$ be a morphism of schemes with a section g, then for any $T \in \mathcal{S}\mathrm{ch}/S$, the group of isomorphism classes of pairs $(\mathcal{L}, u)$ where $\mathcal{L} \in \mathrm{Pic}(X_T)$ and u is a g-rigidification of $\mathcal{L}$, is isomorphism to $\widetilde{\underline{\mathrm{Pic}}}_{X/S}(T)$. ⌟

Proof: For any $\mathcal{M} \in \mathrm{Pic}(X_T)$, let $\mathcal{L} = \mathcal{M} \otimes (f_T^* g_T^* \mathcal{M})^{-1}$, then $\mathcal{L} = \mathcal{M} \in \mathrm{Pic}(X_T)/\operatorname{pr}_T^* \mathrm{Pic}(T)$, and there is a canonial isomorphism $g_T^*\mathcal{L} \cong \mathcal{O}_T$.

Conversely, if $u : \mathcal{O}_T \cong g_T^*\mathcal{L}$ and there exists some $\mathcal{N} \in \mathrm{Pic}(T)$ s.t. $v : \mathcal{L} \cong f_T^*\mathcal{N}$, let $w = g_T^* \circ u : \mathcal{O}_T \cong g_T^*\mathcal{L} \cong \mathcal{N}$, then there are isomorphism of pairs: $v : (\mathcal{L}, u) \cong (f_T^*\mathcal{N}, w)$, $f_T^* w : (\mathcal{O}_{X_T}, \mathrm{can}) \cong (f_T^*\mathcal{N}, w \circ \mathrm{can})$, thus $(\mathcal{L}, u) = e$. □

Prop. (9.7.2.6) [No Automorphisms after Rigidification]. Let $f : X \to S$ be a morphism of schemes. If for any $T \in \mathcal{S}\mathrm{ch}_S$, $f_T : X_T \to T$ satisfies $\mathcal{O}_T \cong (f_T)_*\mathcal{O}_{X_T}$, and f has a section g, then for any $(\mathcal{L}, u)$ where u is a g-rigidification of $\mathcal{L}$, $\mathrm{Aut}(\mathcal{L}, u)$ is trivial. ⌟

Proof: For such an automorphism $v : \mathcal{L} \to \mathcal{L}$, $g_T^*(v) = \mathrm{id}$, Also notice $\mathrm{Hom}(\mathcal{L}, \mathcal{L}) = H^0(\mathcal{H}om(\mathcal{L}, \mathcal{L})) = H^0(\mathcal{O}_{X_T}) \cong H^0(\mathcal{O}_T)$, thus v is tensoring a line bundle $\mathcal{L}$ from $\mathcal{O}_T$. Thus g^*v is multiplying $\mathcal{L}$. So $\mathcal{L} \cong \mathcal{O}_T$ and v is trivial. □

Prop. (9.7.2.7) [Comparison Theorems]. Let $f : X \to S$ be a morphism of schemes. If for any $T \in \mathcal{S}\mathrm{ch}_S$, $f_T : X_T \to T$ satisfies $\mathcal{O}_T \cong (f_T)_*\mathcal{O}_{X_T}$, then

- The morphisms $\widetilde{\underline{\mathrm{Pic}}}_{X/S} \hookrightarrow \underline{\mathrm{Pic}}_{X/S,\mathrm{Zar}} \hookrightarrow \underline{\mathrm{Pic}}_{X/S,\text{ét}} \hookrightarrow \underline{\mathrm{Pic}}_{X/S}$ are injections. In particular, $\widetilde{\underline{\mathrm{Pic}}}_{X/S}$ is separated in the fppf topology.

- If f has a section, then $\widetilde{\underline{\mathrm{Pic}}}_{X/S} \cong \underline{\mathrm{Pic}}_{X/S,\mathrm{Zar}} \cong \underline{\mathrm{Pic}}_{X/S,\text{ét}} \cong \underline{\mathrm{Pic}}_{X/S}$.
- If f has a section Zariski locally, then $\underline{\mathrm{Pic}}_{X/S,\mathrm{Zar}} \cong \underline{\mathrm{Pic}}_{X/S,\text{ét}} \cong \underline{\mathrm{Pic}}_{X/S}$.
- if f has a section étale locally, then $\underline{\mathrm{Pic}}_{X/S,\text{ét}} \cong \underline{\mathrm{Pic}}_{X/S}$.

⌟

Proof: 1: It suffices to show that $\widetilde{\underline{\mathrm{Pic}}}_{X/S} \to \underline{\mathrm{Pic}}_{X/S}$ are injective. For this, notice first $\underline{\mathrm{Pic}}_{X/S}$ is also the fppf-sheaf associated to $\underline{\mathrm{Pic}}_X$, as any line bundle on T is Zariski-locally trivial. Then if $\mathcal{L} \in \mathrm{Pic}(X_T)$ is fppf-locally trivial, then for some fppf covering $\pi : T' \to T$, $(f_{T'})_*\pi_X^*\mathcal{L} \cong \mathcal{O}_{T'}$ by hypothesis. And this equals $\pi^*(f_T)_*\mathcal{L}$ by flat base change. So $(f_T)_*\mathcal{L}$ is an invertible sheaf(by hypothesis used on f_T) and $(f_T)_*(f_T)^*\mathcal{L} \cong \mathcal{L}$ because it is true after f.f. base change to T'(flat base change used).

2: By item1, it suffices to show $\widetilde{\mathrm{Pic}}_{X/S}$ satisfies the fppf-descent, but this follows from the facts that $\mathrm{Pic}_{X/S}$ is a rigid fibered category(6.1.3.5), $\mathfrak{QCoh} / \mathfrak{Sch}$ is a stack(6.1.5.12) and Pic satisfy the fpqc descent(6.5.3.1).

3, 4 follow from 2 by base change. □

Prop. (9.7.2.8) [Comparison of Points]. Let $\mathrm{Spec}\, A \in \mathfrak{Sch}_S$ where A is a local ring, then

- the natural maps $\mathrm{Pic}_X(A) \cong \widetilde{\underline{\mathrm{Pic}}}_{X/S}(A) \cong \underline{\mathrm{Pic}}_{X/S,\mathrm{Zar}}(A)$ are isomorphisms.
- If A is Artin local with alg.closed residue field, then $\mathrm{Pic}_X(A) \cong \underline{\mathrm{Pic}}_{X/S,\text{ét}}(A)$.
- If A is an alg.closed field k, then $\mathrm{Pic}_X(k) \cong \underline{\mathrm{Pic}}_{X/S}(k)$

⌟

Proof: 1: Since A is local, $\mathrm{Pic}(\mathrm{Spec}\, A) = 0$, and it has a unique minimal point, thus 1 is clear.

2: Every étale A-algebra of f.t. is a direct product of copies of A**?**, thus it is clear any fppf local scheme is a scheme.

3: In this case, any fppf covering of $\mathrm{Spec}\, k$ has a section, thus this follows from(9.7.2.7). □

Prop. (9.7.2.9). If X/S is proper of f.p., then an element in $\underline{\mathrm{Pic}}_{X/S}(S)$ is trivial iff it is trivial Zariski-locally on S. ⌟

Proof: Cf.[Neron Model, P202]. □

Relative Effective Divisors

Prop. (9.7.2.10) [Divisor Functor]. The **divisor functor** $\underline{\mathrm{Div}}_{X/S} : \mathfrak{Sch}_S \to \mathfrak{Grp}$ is given by $T \mapsto \{\text{relative effective divisors on } X_T/T\}$. This is truly a functor by(6.8.1.12). ⌟

Thm. (9.7.2.11) [$\underline{\mathrm{Div}}_{X/S}$ is Representable]. If S is a locally Noetherian scheme and $X \to S$ is projective and flat, then $\underline{\mathrm{Div}}_{X/S}$(9.7.2.10) is representable by an open subscheme of the Hilbert scheme $\underline{\mathrm{Hilb}}_{X/S}$. ⌟

Proof: Let $H = \underline{\mathrm{Hilb}}_{X/S}$ and $W \subset X \times H$ the universal closed subscheme. Then pr_H is projective and flat. Let V be the open loci of points of W s.t. W is an effective divisor, $U = H \backslash q(W \backslash V)$, then U is open in H and $q^{-1}U$ is an effective divisor on $X \times U/U$. By definition of Hilbert scheme, for any effective divisor D on some X_T/T is the pullback of W via g. Now we show for any $t \in D$, $g(t) \in U$. This follows from(6.8.1.10) and f.f. descent of regularness(6.1.5.28). Thus g factors through U, as U is open. □

Def. (9.7.2.12) [Relative Abel Map]. The **relative Abel map** is the functor

$$A_{X/S}(T) :\mapsto \underline{\mathrm{Div}}_{X/S}(T) \to \widetilde{\underline{\mathrm{Pic}}}_{X/S}(T) : D \mapsto \mathcal{L}_{X_T}(D).$$

⌟

Def. (9.7.2.13) [Linear System Functor]. Let $X \in \mathcal{S}\mathrm{ch}_S$ and $\mathcal{L} \in \mathrm{Pic}(X)$, the **linear system functor** $\underline{\mathrm{LinSys}}_{\mathcal{L}/X/S} : \mathcal{S}\mathrm{ch}_S \to \mathcal{S}\mathrm{et}$ is defined to be the inverse image of $\mathcal{L} \in \widetilde{\underline{\mathrm{Pic}}}_{X/S}$ in $\underline{\mathrm{Div}}_{X/S}$ via the Abel map(9.7.2.12). ⌟

Thm. (9.7.2.14) [$\underline{\mathrm{LinSys}}_{\mathcal{L}/X/S}$ is Representable]. Let X be a proper variety over S and $\mathcal{L} \in \mathrm{Pic}(X)$, then $\underline{\mathrm{LinSys}}_{\mathcal{L}/X/S}$ is represented by some projective space $\mathbb{P}(\mathcal{Q})$ over S. ⌟

Proof: Cf.[Kle05]P25.**?** □

Prop. (9.7.2.15). Assume X/S is proper and $\mathcal{F} \in \mathcal{C}\mathrm{oh}(X)$, then there exists a unique $\mathcal{Q} \in \mathcal{C}\mathrm{oh}(S)$ with functorial isomorphism

$$q : \mathcal{H}om(\mathcal{Q}, \mathcal{N}) \cong f_*(\mathcal{F} \otimes f^*\mathcal{N})$$

for any $\mathcal{N} \in \mathcal{QC}\mathrm{oh}(S)$.

And the formation of $\mathcal{Q}$ commutes with base change. ⌟

Proof: Cf.[Kle05]P24.**?** □

Prop. (9.7.2.16). Situation as in(9.7.2.15), if S is a local ring with closed point s, the following are equivalent:

- The $\mathcal{O}_S$-module $\mathcal{Q}$ is locally free.
- For all $\mathcal{N} \in \mathcal{QC}\mathrm{oh}(\mathcal{O}_S)$, the functor $\mathcal{N} \mapsto f_*(\mathcal{F} \otimes f^*\mathcal{N})$ is right exact.
- For all $\mathcal{N} \in \mathcal{QC}\mathrm{oh}(\mathcal{O}_S)$, the natural map $f_*(\mathcal{F}) \otimes \mathcal{N} \to f_*(\mathcal{F} \otimes f^*\mathcal{N})$ is an isomorphism.
- The natural map $H^0(X, \mathcal{F}) \otimes k(s) \to H^0(X_s, \mathcal{F}_s)$ is a surjection.

⌟

Proof: Cf.[Kle05]P24.**?** □

Prop. (9.7.2.17) [$\underline{\mathrm{Div}}_{X/S}$ and $\underline{\mathrm{LinSys}}_{\mathcal{P}/X_{\underline{\mathrm{Pic}}_{X/S}}/\underline{\mathrm{Pic}}_{X/S}}$]. If X is a proper variety over S and $\widetilde{\underline{\mathrm{Pic}}}_{X/S}$ is representable with the universal sheaf $\mathcal{P}$, then $\underline{\mathrm{Div}}_{X/S}$ with the relative Abel map(9.7.2.12) is isomorphic to $\underline{\mathrm{LinSys}}_{\mathcal{P}/X_{\underline{\mathrm{Pic}}_{X/S}}/\underline{\mathrm{Pic}}_{X/S}}$ and also $\mathbb{P}(\mathcal{Q})$ over $\underline{\mathrm{Pic}}_{X/S}$, where $\mathcal{Q}$ is the coherent sheaf associated to $\mathcal{P}$(9.7.2.15). ⌟

Proof: It follows from definitions(9.7.2.13)(9.7.2.10) and(9.7.2.12) and the definition of a universal sheaf. The last assertion follows from(9.7.2.14). □

Prop. (9.7.2.18) [$\underline{\mathrm{Div}}_{X/S}$ is Proper over $\underline{\mathrm{Pic}}_{X/S}$]. Let X/S be locally projective flat with integral geometric fibers, then

- $A_{X/S} : \underline{\mathrm{Div}}_{X/S} \to \underline{\mathrm{Pic}}_{X/S}(T)$ is proper.
- If $\widetilde{\underline{\mathrm{Pic}}}_{X/T} \cong \mathrm{Pic}_{X/T}$, then $A_{X/S} : \underline{\mathrm{Div}}_{X/S} \to \underline{\mathrm{Pic}}_{X/S}(T)$ is projective.

⌟

Proof: If $\widetilde{\underline{\mathrm{Pic}}}_{X/T} \cong \mathrm{Pic}_{X/T}$, then by(9.7.2.17), it is projective. For general case, notice proper satisfies fpqc descent, so we can base change to $X \times_S X \to X$, then it has a section, i.e. the diagonal section. Thus by(9.7.2.7), $\widetilde{\underline{\mathrm{Pic}}}_{X/T} \cong \mathrm{Pic}_{X/T}$ and $A_{X \times_S X/X}$ is projective, thus $A_{X/S}$ is proper. □

Picard Schemes

Def. (9.7.2.19) [Picard Scheme]. For the 5 different presheaves on $\mathcal{S}ch_S$ in(9.7.2.1), if one of them is representable, then all the sheaves after it are all isomorphic to it and representable, because fpqc sites are subcanonical. So it will make no confusion to call the representing scheme the **Picard scheme**. ⌟

Prop. (9.7.2.20). If $\underline{\mathrm{Pic}}_{X/S}$ is representable, then it is locally of f.t. over S. ⌟

Proof: Because S is locally Noetherian, by(6.8.4.2), it suffices to show that for any directed inverse system $(T_i, f_{ii'}) \in \mathcal{A}\mathrm{ff}_S$,

$$\varinjlim_I \underline{\mathrm{Pic}}_{X/S}(T_i) \cong \underline{\mathrm{Pic}}_{X/S}(\varinjlim_I T_i).$$

For the rest, Cf.[Kle05]P33.**?** □

Prop. (9.7.2.21) [Points of $\underline{\mathrm{Pic}}_{X/S}$]. If $\underline{\mathrm{Pic}}_{X/S}$ exists, then schematic points of $\underline{\mathrm{Pic}}_{X/S}$ corresponds to line bundles on the geometric fibers of X/S. ⌟

Proof: This follows from the definition of schematic points and(9.7.2.8)item3. □

Thm. (9.7.2.22) [Grothendieck]. Let $f : X \to S$ be locally projective, flat with integral geometric fibers, then

- $\underline{\mathrm{Pic}}_{X/S,\text{ét}}$ is representable by a scheme separated and locally of f.p. over S.
- If moreover S is Noetherian and X/S is projective, then $\underline{\mathrm{Pic}}_{X/S,\text{ét}}$ is a disjoint union of open subschemes, each an increasing union of open quasi-projective S-schemes.

Moreover, by(9.7.2.7), if f has a section e, then there is a **Poincaré class** $p_{X/S} \in \mathrm{Pic}(X \times \mathrm{Pic}_{X/S,\text{ét}})$ with a rigidification along e. ⌟

Proof: Cf.[Kle05]P27.**?** □

Cor. (9.7.2.23). If S is Noetherian and X/S is projective flat with integral geometric fibers, then any qc locally closed subscheme of $\underline{\mathrm{Pic}}_{X/S}$ is quasi-projective. ⌟

Prop. (9.7.2.24) [Tangent Space of $\underline{\mathrm{Pic}}_{X/k}$]. Let X be a scheme over a field. Assume $\underline{\mathrm{Pic}}_{X/k}$ is representable by a scheme and equals $\underline{\mathrm{Pic}}_{X/k,\text{ét}}$, then $T_e(\underline{\mathrm{Pic}}_{X/k}) \cong H^1(X, \mathcal{O}_X)$. ⌟

Proof: By(9.2.2.1), the tangent space equals $\ker(\underline{\mathrm{Pic}}_{X/k}(k[\varepsilon]) \to \underline{\mathrm{Pic}}_{X/k}(k))$.

Take the first order thickening $X_k \subset X_{k[\varepsilon]} = X_\varepsilon$, there is an exact sequence $0 \to \mathcal{O}_X \to \mathcal{O}_{X_\varepsilon}^* \to \mathcal{O}_X^* \to 1$, where $\mathcal{O}_X \to \mathcal{O}_{X_\varepsilon}^* : a \mapsto 1 + a\varepsilon$. And it is split. Thus we have a split exact sequence

$$0 \to H^1(\mathcal{O}_X) \to H^1(\mathcal{O}_{X_\varepsilon}^*) \to H^1(\mathcal{O}_X^*) \to 0.$$

Now $\underline{\mathrm{Pic}}_{X/S,\text{ét}}$ is also the shifification of $\widetilde{\underline{\mathrm{Pic}}}_{X/k} : T \mapsto H^1(X_T, \mathcal{O}_{X_T}^*)$, thus there is a natural map

$$H^1(\mathcal{O}_X) \to \ker(\underline{\mathrm{Pic}}_{X/k}(k[\varepsilon]) \to \underline{\mathrm{Pic}}_{X/k}(k)) = T_e(\underline{\mathrm{Pic}}_{X/k}).$$

And it can be shown that this is a k-homomorphism.

To show this map is an isomorphism, by flat base change we can assume k is alg.closed. Then by(9.7.2.8), the maps $H^1(\mathcal{O}_X^*) \to \underline{\mathrm{Pic}}_{X/k}(k)$ and $H^1(\mathcal{O}_{X_\varepsilon}^*) \to \underline{\mathrm{Pic}}_{X/k}(k[\varepsilon])$ are isomorphisms, thus $H^1(\mathcal{O}_X) \to T_e(\underline{\mathrm{Pic}}_{X/k})$ is also an isomorphism by five lemma. □

Thm. (9.7.2.25) [Grothendieck]. Assume X is proper over S integral, then there exists a non-empty open subscheme $V \subset S$ s.t. $\underline{\mathrm{Pic}}_{X_V/V}$ is representable, and is a disjoint union of quasi-projective subschemes. ⌟

Proof: Cf.[Kle05]P34. □

Cor. (9.7.2.26) [Murre-Oort/Artin]. Let X be a proper scheme over a field k, then $\underline{\mathrm{Pic}}_{X/k}$ is representable by a disjoint union of quasi-projective subschemes. ⌟

Prop. (9.7.2.27). Let $X \to Y$ be a surjective morphism of proper schemes over a field k, then the dual map $\underline{\mathrm{Pic}}_{Y/k} \to \underline{\mathrm{Pic}}_{X/k}$ is affine. ⌟

Proof: □

Prop. (9.7.2.28). If X/S is projective and flat with integral geometric fibers, then any connected component of $\underline{\mathrm{Pic}}_{X/S}$ is clopen of f.t.. ⌟

Proof: By(9.7.2.22), $\underline{\mathrm{Pic}}_{X/S}$ is locally Noetherian, so each connected components are clopen(6.4.1.23), and they are of f.t. as $\underline{\mathrm{Pic}}^{\Phi}_{X/S}$ are(9.7.2.40). □

Prop. (9.7.2.29) [Projectiveness of Subschemes]. Let S be Noetherian and $X \to S$ be smooth projective with irreducible geometric fibers, then every quasi-compact closed subscheme of $\underline{\mathrm{Pic}}_{X/S}$ over S is projective. ⌟

Proof: By(9.7.2.23), it suffices to show it is universally closed. As $X \to S$ is both proper and flat, it suffices to show for $X \to S$ f.f.. Then we can base change via the f.f. covering $X \to S$, thus we can assume it has a section, so $\widetilde{\underline{\mathrm{Pic}}}_{X/S} \cong \mathrm{Pic}_{X/S}$. Then we use valuation criterion: for any valuation ring A with fraction field K, it suffices to extend a line bundle on X_K to a line bundle on X_A, because Z is closed and A is reduced. By replacing $\mathcal{L}$ with $\mathcal{L}(n)$, we can assume $\mathcal{L}$ has a global section, which implies $\mathcal{L}$ is an effective Cartier divisor D, as X_K is integral. Notice A is regular and X_T/T is smooth, so X_T is regular**??** and thus locally factorial. Then the closure of D in X_T is also a divisor**?**. □

Cor. (9.7.2.30). If $k \in \texttt{Field}$ and $X \in \mathcal{S}m\mathcal{P}roj\,/k$, then all connected components of $\underline{\mathrm{Pic}}_{X/k}$ are proper. ⌟

Proof: This follows from(9.7.2.29) and(9.1.4.16). □

Prop. (9.7.2.31) [Product Varieties]. If $k \in \texttt{Field}$ and X, Y are two complete varieties over a field k with rational points, then $\underline{\mathrm{Pic}}_{X\times Y/k} \cong \underline{\mathrm{Pic}}_{X/k} \times \underline{\mathrm{Pic}}_{Y/k}$, with $p_{X\times Y} = \mathrm{pr}_1^* p_X \otimes \mathrm{pr}_2^* p_Y$. ⌟

Proof: This follows from see-saw principal(6.11.1.22), the theorem of the cube(6.11.1.23) and(9.7.2.5). □

$\underline{\underline{\mathrm{Pic}^0_{X/S}}}$

Def. (9.7.2.32) [$\underline{\mathrm{Pic}}^0_{X/S}$]. If $\underline{\mathrm{Pic}}_{X/S}$ exists, then its identity component is a subgroup scheme(9.1.4.11), denoted by $\underline{\mathrm{Pic}}^0_{X/S}$. ⌟

Prop. (9.7.2.33) [Projectiveness of $\underline{\mathrm{Pic}}^0_{X/k}$]. Let X be a projective variety over a field k, then $\underline{\mathrm{Pic}}^0_{X/S}$ is representable(9.7.2.22) and is quasi-projective. And it is projective if X/k is geo.normal. ⌟

Proof: Cf.[Kle05]P37.**?** □

Cor. (9.7.2.34)[Subfamily and Morphisms Relations]. The Poincaré class p_X in $\mathrm{Pic}(X\times\underline{\mathrm{Pic}}^0(X))$ is the unique line bundle that satisfies $p_b=b$ for a point $b\in\underline{\mathrm{Pic}}^0(X)$, and p_0 is trivial.

For a subfamily c of $\mathrm{Pic}^0(X)$ parametrized by an scheme T over k, there is a morphism

$$T\to\underline{\mathrm{Pic}}^0(X):t\mapsto c_t\in\underline{\mathrm{Pic}}^0(X)(\kappa(t))$$

over k. ⌟

Proof: A point $b\in\underline{\mathrm{Pic}}^0(X)$ is a morphism $k(b)\to\underline{\mathrm{Pic}}^0(X)$, and the restriction of p to b is just b, by(9.7.2.22).

The second assertion follows from the first, because this subfamily corresponds to a morphism $T\to\underline{\mathrm{Pic}}^0(X)$, and the restriction of p at the. image of t in $\underline{\mathrm{Pic}}^0(X)$ is just the subfamily restricted at t, which is c_t. □

Prop. (9.7.2.35) [$\underline{\mathrm{Pic}}^0_{X/k,\mathrm{red}}$ is an Abelian Variety]. If X is a smooth projective variety over a field k, then $\underline{\mathrm{Pic}}^0_{X/k,\mathrm{red}}$ is an Abelian variety. ⌟

Proof: $\underline{\mathrm{Pic}}^0_{X/S,\mathrm{red}}$ is also a smooth proper connected algebraic group by(9.7.2.30)(9.7.2.28), thus it is an Abelian variety. □

Prop. (9.7.2.36) [Dual Picard Maps]. By functoriality, if $X/S,X'/S$ are connected schemes with sections s.t. $\underline{\mathrm{Pic}}_{X/S}$ and $\underline{\mathrm{Pic}}_{X'/S}$ are representable, then the pullback along φ induces a dual homomorphism of group schemes:

$$\varphi^\vee:\underline{\mathrm{Pic}}^0_{X'/S,\mathrm{red}}\to\underline{\mathrm{Pic}}^0_{X/S,\mathrm{red}}.$$

In other words, it is the unique morphism $\underline{\mathrm{Pic}}^0_{X'/S,\mathrm{red}}\to\underline{\mathrm{Pic}}^0_{X/S,\mathrm{red}}$ s.t.

$$(\varphi\times\mathrm{id}_{\underline{\mathrm{Pic}}^0_{X'/S,\mathrm{red}}})^*p_{X'/S}=(\mathrm{id}_X\times\varphi^\vee)^*p_{X/S}.$$

⌟

Prop. (9.7.2.37) [Double Picard Map]. Let X/S be a connected scheme s.t. $\widetilde{\underline{\mathrm{Pic}}}_{X/S,\mathrm{red}}$ is representable with a Poincaré class $p_X\in\mathrm{Pic}(X\times\underline{\mathrm{Pic}}^0_{X/S,\mathrm{red}})$, and $(\underline{\mathrm{Pic}}^0_{X/S,\mathrm{red}})^\vee$ is representable, then p_X satisfies $(p_X)_0=0$, thus inducing a map $X\to(\underline{\mathrm{Pic}}^0_{X/S,\mathrm{red}})^\vee$. ⌟

Def. (9.7.2.38) [Néron-Severi Group Scheme]. Let X be a complete k-variety, the **Néron-Severi group** $\mathrm{NS}(X_{\overline{k}})$ of $X_{\overline{k}}$ is defined to be

$$\mathrm{NS}(X_{\overline{k}})=\mathrm{Pic}(X_{\overline{k}})/\,\underline{\mathrm{Pic}}^0(X_{\overline{k}})=\pi_0(\underline{\mathrm{Pic}}_{\overline{X}/\overline{k}})(\overline{k})\text{(8.1.12.4)(8.3.1.2)},$$

which in fact equals $\pi_0(\underline{\mathrm{Pic}}_{X_{k^s}/k^s})(k^s)=\mathrm{Pic}(X_{k^s})/\,\underline{\mathrm{Pic}}^0(X_{k^s})=\mathrm{NS}(X_{k^s})$.

Also denote

$$N^1(X_{\overline{k}})=\mathrm{Pic}(X_{\overline{k}})/\,\mathrm{Pic}^\tau(X_{\overline{k}})=\mathrm{NS}(X_{\overline{k}})/\,\mathrm{NS}(X_{\overline{k}})_{\mathrm{tor}}\text{(8.1.12.25)}=N^1(X_{k^s}).$$

⌟

Prop. (9.7.2.39) [Theorem of the Base]. $\mathrm{NS}(X_{\overline{k}})$ is f.g. In particular, $N^1(X_{\overline{k}})$ is a finite free $\mathbb{Z}$-module, and its rank $\rho(X)$ is called the **Picard number** of X. ⌟

Proof: Cf. [Kleiman, Toward a numerical theory of ampleness, P334]. □

Prop. (9.7.2.40) [$\underline{\mathrm{Pic}}^{\Phi}_{X/S}$]. If X/S is locally projective, flat with integral geometric fibers, $\Phi \in \mathbb{Q}[\lambda]$, let $\underline{\mathrm{Pic}}^{\Phi}_{X/S}$ denote the subfunctor of $\underline{\mathrm{Pic}}_{X/S}$ representing invertible sheaves $\mathcal{L}$ with $\chi(\mathcal{L}(n)) = \Phi(n)$, then $\underline{\mathrm{Pic}}^{\Phi}_{X/S}$ are clopen subschemes of $\underline{\mathrm{Pic}}_{X/S}$ of f.t. and form a disjoint cover of it, and forming it commutes with base change. Moreover, if X/S is projective and S is Noetherian, then each $\underline{\mathrm{Pic}}^{\Phi}_{X/S}$ is quasi-projective over S. ⌟

Proof: Cf.[Kle05]P60.**?**

The first assertion follows from the fact Euler character is locally constant so $\underline{\mathrm{Pic}}^{\Phi}_{X/S}$ form a clopen disjoint covering of $\underline{\mathrm{Pic}}_{X/S}$ and use(9.6.1.5) and(9.6.1.7). □

Prop. (9.7.2.41) [Quasi-Coherence and Boundedness]. If $\underline{\mathrm{Pic}}_{X/S}$ is representable and $\Lambda \subset \underline{\mathrm{Pic}}_{X/S}$ be a subset with corresponding set of line bundles L, then Λ is qc iff L is bounded(8.1.12.24). ⌟

Proof: If L is bounded by $T \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}}/S$, then there is a map $\theta : T \to \underline{\mathrm{Pic}}_{X/S}$ that $\Lambda \subset \theta(T)$. Notice T is a Noetherian space, thus so is $\theta(T)$, and Λ is qc.

Conversely, if Λ is qc, then it is contained in an open subscheme $U \subset \underline{\mathrm{Pic}}_{X/S}$ of f.t. over S, then U gives out a line bundle on X_T for some fppf covering T of U. Such T can be chosen to be f.t. over S as U is f.t., so L is bounded by T. □

Cor. (9.7.2.42) [Quasi-Coherence and Hilbert Polynomials]. If S is Noetherian and X/S is projective and flat, and $\underline{\mathrm{Pic}}_{X/S}$ is representable, let $\Lambda \subset \underline{\mathrm{Pic}}_{X/S}$ be any subset and Π the corresponding set of Hilbert polynomials, then $\#\Pi < \infty$ if Λ is qc, and $\#\Pi = 1$ if Λ is connected. ⌟

Proof: If Λ is qc, then L is bounded by some $T \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}}/S$, and then by locally constancy of Hilbert polynomials, $\#\Pi < \infty$.

If Λ is connected, then so is the induced reduced structure on its closure $\overline{\Lambda}$. $\overline{\Lambda}$ gives out a line bundle on X_T for some fppf covering T of $\overline{\Lambda}$. Notice $T \to \overline{\Lambda}$ is open and Hilbert polynomial is locally constant on T, so there is only one Hilbert polynomial type. □

Torsion Components

Prop. (9.7.2.43). If X/S is projective, flat with integral geometric fibers, then for $n \in \mathbb{Z}_+$, $[n] : \underline{\mathrm{Pic}}_{X/S} \to \underline{\mathrm{Pic}}_{X/S}$ is of f.t. ⌟

Proof: Cf.[**?**]. □

Prop. (9.7.2.44). If X/S is proper and $\underline{\mathrm{Pic}}_{X/S}$ exists, then $\underline{\mathrm{Pic}}^{\tau}_{X/S}$ is an open subgroup of f.t.. ⌟

Proof: Cf.[**?**]P59. □

Prop. (9.7.2.45). If X is a k-scheme s.t. $\underline{\mathrm{Pic}}_{X/k}$ is representable, then $\underline{\mathrm{Pic}}^{\tau}_{X/S}$ is an open subgroup, and forming it commutes with change of fields. Moreover, if X/S is projective, then $\underline{\mathrm{Pic}}^{\tau}_{X/S}$ is clopen of f.t.. ⌟

Proof: Using(9.1.4.17) and(9.7.2.20), it suffices to prove $\underline{\mathrm{Pic}}^{\tau}_{X/S}$ is of f.t. when X is projective over S. For this, it suffices to prove for $k = \overline{k}$. In this case, by(8.1.12.25) and(8.1.12.26), there is an algebraic k-scheme T and $\mathcal{M} \in \mathcal{T}$ s.t. the corresponding map $\theta : T \to \underline{\mathrm{Pic}}_{X/k}$ satisfies $\underline{\mathrm{Pic}}^{\tau}_{X/S} \subset \theta(T)$. Notice T is a Noetherian space, thus so is $\theta(T)$, and Λ is qc. □

Cor. (9.7.2.46). Let X is a projective variety over a field k, then $\underline{\mathrm{Pic}}^{\tau}_{X/k}$ is quasi-projective. And if X is geo.normal, then it is projective. ⌟

Proof: By(9.7.2.45)(9.7.2.23), $\underline{\mathrm{Pic}}_{X/S}$ is quasi-projective. To show it is proper, it suffices to show for $k = \overline{k}$. In this case, $\underline{\mathrm{Pic}}^{\tau}_{X/k}$ is covered by f.m. translates of $\mathrm{Pic}^0_{X/k}$ as it is qc, and $\underline{\mathrm{Pic}}^0_{X/k}$ is projective by(9.7.2.33), so $\underline{\mathrm{Pic}}_{X/k}$ is also proper, as it is closed so is the scheme-theoretic image of these copies $\underline{\mathrm{Pic}}^0_{X/k}$. □

Prop. (9.7.2.47). Let X/S be locally projective flat with integral geometric fibers, then $\underline{\mathrm{Pic}}^{\tau}_{X/S}$ is a clopen subgroup of $\underline{\mathrm{Pic}}_{X/S}$ of f.t., and forming it is compatible with base change. Moreover, if X/S is projective with S Noetherian, then $\underline{\mathrm{Pic}}^{\tau}_{X/S}$ is quasi-projective. ⌟

Proof: Cf.[Kle05]P58. □

Cor. (9.7.2.48) [Torsion Components are Projective]. If X/S is smooth projective with integral geometric fibers and S is Noetherian, then $\underline{\mathrm{Pic}}^{\tau}_{X/S}$ is projective. ⌟

Proof: This follows from(9.7.2.47) and(9.7.2.29). □

Prop. (9.7.2.49). If S is Noetherian and X/S is locally projective flat with integral geometric fibers, then for any $s \in S$ with residue field $k(s)$ and an alg.closure $\overline{k}(s)$, the group

$$\underline{\mathrm{Pic}}^{\tau}_{X_{\overline{k}(s)}/\overline{k}(s)}(\overline{k}(s))/\,\underline{\mathrm{Pic}}_{X_{\overline{k}(s)}/\overline{k}(s)}(\overline{k}(s))$$

is a finite group, and its order is uniformly bounded. ⌟

Proof: It is finite by(9.7.2.47), and the number of connected components of $\underline{\mathrm{Pic}}^{\tau}_{X_{\overline{k}(s)}/\overline{k}(s)}$ is constant for a non-empty open subset of S by [EGA 4.3, 9.7.9], so it is bounded by Noetherian induction. □

3 Picard Spaces

Thm. (9.7.3.1) [Artin]. If $X \to S$ is proper flat and f.p. morphism of algebraic spaces s.t. forming $f_*\mathcal{O}_X$ commutes with base change, then $\underline{\mathrm{Pic}}_{X/S}$ is representable by an algebraic space, and is locally of f.p. over S. ⌟

Proof: □

4 Moduli of Curves

Def. (9.7.4.1) [Smooth Curves of Genus g]. Given a scheme S, there is a category $\mathcal{M}_g$ fibered in sets over $\mathcal{S}\mathrm{ch}/S$ where $\mathcal{M}_g(T)$ is the set of smooth and proper morphisms of schemes $C \to T$ that the fibered are all geometrically connected curves of genus g.

Similarly there is a category Z_g fibered in sets over $\mathcal{S}\mathrm{ch}/S$ of smooth pointed curves of genus g ⌟

9.8 Group Algebraic Spaces

Main references are [Sta]Chap76.

Notation (9.8.0.1).

- Use notations defined in Algebraic Stacks9.6.
- Fix $S \in \mathcal{S}\mathrm{ch}$ and $B \in \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}\,/S$. $\mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}\,/B = (\mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}\,/S)/B$.

⌟

Def. (9.8.0.2) [Group Algebraic Spaces]. The category $\mathcal{G}\mathrm{rp}\mathcal{S}\mathrm{p}\,/B$ of **group algebraic space** over B is defined to be

$$\mathcal{G}\mathrm{rp}\mathcal{S}\mathrm{p}\,/B = \mathcal{S}\mathrm{h}_{\mathrm{fppf}}^{\mathcal{G}\mathrm{rp}}\,/B \cap \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}\,/B \subset \mathcal{S}\mathrm{h}_{\mathrm{fppf}}\,/B.$$

⌟

1 Quotient of Groupoids

Main references are [Quotient Spaces Modulo Algebraic Groups, Kollar, 1997].

Def. (9.8.1.1) [Quotients of Groupoids]. Let $U \in \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}\,/B$, $j : R \to U \times_B U$ be a pre-relation on U over B, $\varphi : U \to X \in \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}\,/B$, then

- For $u \in |U|$, the **R-orbit** of u is the equivalent class of $u \in |U|$ generated by $|R| \subset |U| \times |U|$.
- For $T \subset |U|$, T is called **R-invariant** if $s^{-1}(T) = t^{-1}(T) \subset |R|$.
- φ is said to be **R-invariant** if for it equalizes the two maps $s, t : R \to U$.
- φ is said to be **set-theoretically R-invariant** if for any $\mathrm{Spec}\, k \in \mathcal{S}\mathrm{ch}\,/B, k = \overline{k}$, $\varphi(k)$ equalizes the two maps $s, t : R(k) \to U(k)$.
- φ is said to **separate R-orbits** if it is set-theoretically R-invariant and for any $\mathrm{Spec}\, k \in \mathcal{S}\mathrm{ch}\,/B, k = \overline{k}$ and $u, u' \in U(k)$, $\varphi(u) = \varphi(u') \in X(k)$ implies u, u' are in the same R-orbits.
- φ is said to be an **orbit space for** R if it is R-invariant and surjective, and separates R-orbits.
- φ is said to be a **course quotient for** R if it is a categorical quotient and it is an orbit space for R.
- If $S = B, U, R, X \in \mathcal{S}\mathrm{ch}$, then φ is said to be a **course quotient in schemes for** R if it is a categorical quotient in schemes and it is an orbit space for R.
- If φ is R-invariant, The **sheaf of R-invariant functions** $(\varphi_*\mathcal{O}_U)^R$ as the étale $\mathcal{O}_X$-subalgebra of $\varphi_*\mathcal{O}_U$ which is the equalizer of two maps induced from $s, t : R \to X$.

⌟

Prop. (9.8.1.2). Situation as in(9.8.1.1), if R, U are locally of f.t. over B, φ is an orbit space for R iff it is R-invariant and for any $\mathrm{Spec}\, k \in \mathcal{S}\mathrm{ch}\,/B, k = \overline{k}$,

$$U(k)/(\text{equivalent relations generated by } j(R(k))) \to X(k)$$

is bijective. ⌟

Proof: Cf.[Sta]04A0. □

Def. (9.8.1.3) [Good Quotients]. Situation as in(9.8.1.1), φ is said to be a **good quotient** if

- φ is affine, surjective, R-invariant.
- For any base change φ' of φ, $|\varphi'|$ is a closed map, and $|\varphi|(Z_1 \cap Z_2) = |\varphi|(Z_1) \cap |\varphi|(Z_2) \subset |X|$ for any closed subsets $Z_1, Z_2 \subset |U|$.
- $\mathcal{O}_X \to (\varphi_* \mathcal{O}_U)^R$ is an isomorphism.

⌟

Def. (9.8.1.4)[Geometric Quotients]. Situation as in(9.8.1.1), φ is said to be a **geometric quotient** if

- φ is an orbit space for R,
- φ is universally submersive,
- $\mathcal{O}_X \to (\varphi_* \mathcal{O}_U)^R$ is an isomorphism.

⌟

Thm. (9.8.1.5) [Kollar]. Let $S \in \mathcal{S}\mathrm{ch}$ be excellent, $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}_{\mathcal{A}\mathrm{ff}}/S, X \in \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}^{\mathrm{sep,ft}}/S$. Let $m : G \times X \to X$ be a proper G-action on X, and one of the following holds:

- G is a reductive group scheme over S,
- $S = \operatorname{Spec} k$ where $k \in \mathtt{Field}, \operatorname{char} k > 0$.

⌟

Proof: then a geometric quotient $\varphi : X \to X/G$ exist(9.8.1.4), and $X/G \in \mathcal{A}\mathrm{lg}\mathcal{S}\mathrm{p}^{\mathrm{sep,ft}}/S$. Cf.[Quotient Schemes modulo Algebraic Groups, Kollar]P35. □

2 Quotients of Schemes

Prop. (9.8.2.1). Let $u_0, u_1 : X_1 \to X_0$ be an equivalence relation on the algebraic scheme X_0 over R_0. Assume that

- $u_0 : X_1 \to X_0$ is locally free of rank r.
- For all $x_0 \in X$, $u_0(u_1^{-1}(x))$ is contained in an open affine subscheme of X_0.

Then a quotient $u : X_0 \to X$ exists. Moreover, u is locally free of rank r. ⌟

Proof: Cf[Mil17b]P597. □

9.9 Higher Dimensional Geometry

1 Bend and Break

2 Cone Theorem

3 Homological Methods

Prop. (9.9.3.1) [Birkar-Cascini-Hacon-Mkernan]. ⌟

4 Minimal Model Program

9.10 Toric Varieties

10 Algebraic K-Theory of Schemes

10.1 Algebraic K-Theory

1 Introduction

Algebraic K-theory is about natural constructions of cohomology theories/spectra from algebraic data such as commutative rings, symmetric monoidal categories and various homotopy theoretic refinements of these.

When applied to the stack of vector bundles then algebraic K-theory subsumes topological K-theory and also differential K-theory.

2 K-Theory of Categories

K-Groups of Triangulated Categories

Def. (10.1.2.1) [K-Groups of Triangulated Categories]. Let $\mathcal{D}$ be a triangulated categories, then the **K-group of** $\mathcal{D}$ is defined to be the quotient

$$\bigoplus_{X\to Y\to Z \text{ distinguished}} 1 \to \bigoplus_{X\in\mathcal{D}} \to K_0(\mathcal{D}) \to 0$$

where $e_{X\to Y\to Z}$ is mapped to $e_Y - e_X - e_Z$. ⌟

Prop. (10.1.2.2) [Naturality].

- An exact functor between triangulated categories induce a map of their corresponding K-groups,
- A bi-exact bifunctor $F : \mathcal{D}\times\mathcal{D}' \to \mathcal{E}$(4.8.4.8) induces a bilinear map $K_0(\mathcal{D})\times K_0(\mathcal{D}') \to K_0(\mathcal{E})$ sending $([X],[X'])$ to $F(X,X')$.
- A δ-functor from an Abelian category to a triangulated category induces a map of their corresponding K-groups(Notice these two K-groups are defined differently).
- A functor from an exact category to a triangulated category that sends exact sequences to distinguished triangles induces a map of their corresponding K-groups.

⌟

K-Theory of quasi-exact categories

Def. (10.1.2.3) [Quasi-Exact Categories]. A **quasi-exact category** is a pair $(\mathcal{C},\mathcal{E})$ where $\mathcal{C}$ is a pointed balanced small additive category and $\mathcal{E}$ is a set of short sequences

$$0 \to X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \to 0$$

(where we call φ an **admissible monomorphism** and ψ an **admissible epimorphism**) satisfying the following:

- **Ex1**: For any complex $0 \to X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \to 0$ in $\mathcal{E}$, φ is the kernel of ψ and ψ is the cokernel of φ.
- For any $X, Y \in \mathcal{C}$, $0 \to X \to X \oplus Y \to Y \to 0$ is in $\mathcal{E}$.
- $\mathcal{E}$ is closed under isomorphisms.
- Admissible monomorphisms are stable under compositions and base change by admissible epimorphisms.
- Admissible epimorphisms are stable under compositions and base change by admissible monomorphisms.

⌟

Def. (10.1.2.4). For any quasi-exact category $(\mathcal{C}, \mathcal{E})$, we can define the category $Q(\mathcal{C})$ as the category s.t.

- $\mathrm{Ob}(Q(\mathcal{C})) = \mathrm{Ob}(\mathcal{C})$,
- For $X, Y \in \mathrm{Ob}(Q(\mathcal{C}))$, $\mathrm{Map}_{Q(\mathcal{C})}(X, Y)$ consists of isomorphism classes of roofs $(X \xleftarrow{\varphi} S, S \xrightarrow{f} Y)$ s.t. φ is an admissible epimorphism and f is an admissible monomorphism.
- The compositions are given by base change.

The conditions in(10.1.2.3) ensures that $Q(\mathcal{C})$ is truly a category. ⌟

Def. (10.1.2.5)[K-Groups of Quasi-Exact Categories]. For any quasi-exact category $(\mathcal{C}, \mathcal{E})$, $Q(\mathcal{C})$ is path-connected as $\mathcal{C}$ is pointed, so we can define the **K-group of quasi-separated categories** as

$$K_i(\mathcal{C}, \mathcal{E}) = \pi_{i+1}(\mathbb{B}(Q(\mathcal{C})).$$

⌟

Prop. (10.1.2.6)[K_0-Groups]. For any quasi-exact category $(\mathcal{C}, \mathcal{E})$, $K_0(\mathcal{C}, \mathcal{E})$ can be described as the kernel:

$$\bigoplus_{[0\to A\to B\to C\to 0]\in\mathcal{E}} \mathbb{Z} \to \bigoplus_{A\in\mathcal{C}} \mathbb{Z} \to K_0(\mathcal{A}) \to 0,$$

where $e_{0\to A\to B\to C\to 0}$ is mapped to $e_B - e_A - e_C$. ⌟

Proof: □

3 K-Theory of Rings

Def. (10.1.3.1)[K-Theories of Rings]. For $R \in \mathcal{CR}\mathrm{ing}$, Let $\mathcal{P}\mathrm{roj}_R^{\mathrm{fg}}$ be the 1-category of f.g. projective R-modules, and let $\iota\,\mathcal{P}\mathrm{roj}_R^{\mathrm{fg}}$ be the maximal subgroupoid, then it is a E_∞-space. Let

$$K(R) = (\iota\,\mathcal{P}\mathrm{roj}_R^{\mathrm{fg}})^{\infty-\mathrm{ab}}(4.9.2.7).$$

And let

$$K_0(R) = \pi_0(K(R)), \quad K_j(R) = \pi_j(K(R), 0).$$

⌟

Prop. (10.1.3.2) [Ring Structure]. There is an $\mathbb{E}_\infty$-Ring structure on $K_{\geq 0}(R)$, so

$$K_*(R) = \oplus_{j\geq 0} K_j(R)$$

has a graded ring structure. ⌟

Prop. (10.1.3.3) [Matsumoto]. For $k \in$ `Field`, there are natural isomorphisms

$$K_i^{\mathrm{Mil}}(k) \cong K_i(k)$$

for $i = 0, 1, 2$, thus inducing a map

$$K_*^{\mathrm{Mil}}(k) \to K_*(k)$$

that is not necessarily an isomorphism. ⌟

Proof: ? □

4 K-Theory of Schemes

Thm. (10.1.4.1) [Thomason, Quillen]. Let X be an affine regular and separated scheme, and $X = U \cup V$ is an affine open cover, then there is a Cartesian square of spectra

$$\begin{array}{ccc} K(X) & \longrightarrow & K(U) \\ \downarrow & & \downarrow \\ K(V) & \longrightarrow & K(U\cap V) \end{array}$$

⌟

Proof: □

Cor. (10.1.4.2) [Descent Spectral Sequence]. There is a spectral sequence

$$H^p(X; \pi_q(K)) \Rightarrow K_{p-q}(X).$$

⌟

Proof: ? □

Def. (10.1.4.3) [Graded Determinant Map]. For $X \in \mathcal{S}\mathrm{ch}$ affine or regular, let $\mathbf{Pic}^{\mathbb{Z}}(X) = \mathbf{Pic}(X) \rtimes H^0(X;\mathbb{Z})$, where $H^0(X;\mathbb{Z})$ acts on $\mathbf{Pic}(X)$ locally by $n.\mathcal{L} = \mathcal{L}^{(-1)^n}$. Then there is a graded determinant map

$$(\det, \mathrm{rank}) : \iota\,\mathcal{P}\mathrm{roj}^{\mathrm{fg}}(X) \to \mathbf{Pic}^{\mathbb{Z}}$$

that is a morphism of $\mathbb{E}_\infty$-rings:

$$\begin{array}{ccc} \det(M\oplus N) & \xrightarrow{\cong} & \det(M)\otimes\det(N) \\ \downarrow{\scriptstyle \cong, (-1)^{\mathrm{rank}(M)\,\mathrm{rank}(N)}} & & \downarrow{\scriptstyle\cong} \\ \det(N\oplus M) & \xrightarrow{\cong} & \det(N)\otimes\det(M) \end{array}$$

is commutative. Thus by universal property of group completion, we get a map

$$K(X) \to \mathbf{Pic}^{\mathbb{Z}}(X).$$

Thus we have maps

$$K_j(X) \xrightarrow{(\det,\mathrm{rank})} \pi_j(\mathbf{Pic}^{\mathbb{Z}}(X)),$$

and the kernel is denoted by $SK_j(X)$. ⌟

Prop. (10.1.4.4). The graded determinant map(10.1.4.3) induces a surjective ring homomorphism

$$K_0(X) \to \mathbf{Pic}^{\mathbb{Z}}(X).$$

⌟

Proof: $\mathcal{L} \otimes \mathcal{O}_X^{n-1}$ is mapped to $(\mathcal{L}, n)$, and these generate $\mathrm{Pic}^{\mathbb{Z}}(X)$. □

Prop. (10.1.4.5). If R is a local ring, then there is an isomorphism

$$K_1(R) \xrightarrow{(\det,\mathrm{rank})} \pi_1(\mathbf{Pic}^{\mathbb{Z}}(R)) \cong R^*.$$

⌟

Prop. (10.1.4.6). Let X be a an irreducible regular Noetherian scheme of dimension 1, then there is an isomorphism

$$K_0(X) \xrightarrow[\cong]{(\det,\mathrm{rank})} \mathrm{Pic}^{\mathbb{Z}}(X).$$

⌟

Proof: [Motives at p]L7P4.? □

Prop. (10.1.4.7) [Properties of K-Groups]. For $j \in \mathbb{Z}$, $K_j : \mathcal{S}\mathrm{ch}^{\mathrm{op}} \to \mathcal{A}\mathrm{b}$ are functors satisfying the following properties:

- there is a rank map $\mathrm{rank} : K_0(X) \to H^0(X, \mathbb{Z})$, which is an isomorphism if X is a local scheme.
- If X is qcqs and $X = U \cup V$ is an open cover, there is a long exact sequence
$$\cdots \to K_j(X) \to K_j(U) \oplus K_j(V) \to K_j(U \cap V) \to K_{j-1}(X) \to \cdots .$$
- If X is qcqs and $Y \to X$ is a closed immersion s.t. Y is regular, then there are natural maps
$$i_* : K_j(Y) \to K_j(X)$$
that fits into a long exact sequence
$$\cdots \to K_j(Y) \xrightarrow{i_*} K_j(X) \to K_j(X \setminus Y) \to K_{j-1}(Y) \to \cdots .$$
- If X is regular, then the projection $X \times \mathbb{A}^1 \to X$ induces isomorphisms
$$K_j(X) \cong K_j(X \times \mathbb{A}^1).$$
- If X is qcqs, there is a natural isomorphism
$$K_j(X)\{0\} \oplus K_j(X)\{0(1) - 0\} \cong K_j(\mathbb{P}^1_X).?$$

⌟

Proof: ? □

Def. (10.1.4.8) [K-Groups of Schemes]. For $X \in \mathcal{S}\mathrm{ch}_{\mathrm{qcqs}}$, its algebraic K-theory is defined to be the spectrum

$$K(X) = \varprojlim_{\mathrm{Spec}\, R \to X} K(R).$$

It follows from(10.1.4.1) that this defines a ⌟

Prop. (10.1.4.9) [Cup Products, Push and Pull]. For any regular separated Noetherian scheme X, there is a cup product map

$$\cup : K_i(X) \times K_j(X) \to K_{i+j}(X).$$

And if $f : X' \to X$ is a morphism of regular separated Noetherian schemes, there is a graded ring homomorphism $f^* : K_*X \to K_*X'$. And if f is proper, there are pushforward maps $f_* : K_i(X') \to K_i(X)$. And in this case, they satisfy the projection formula

$$f_*(f^*a \cup b) = a \cup f_*b.$$

There is a canonical inclusion $\mathcal{O}^*(X) \subset K_1(X)$, and the restriction of $f^*(\mathcal{O}^*(X)) \subset \mathcal{O}^*(X')$, which is just the pullback map. And if f is finite flat, then the image of $f_*(\mathcal{O}^*(X')) \subset \mathcal{O}^*(X)$, which is just the norm map.

The cup product map restricted to $\mathcal{O}^*(X) \times \mathcal{O}^*(X) \to K_2(X)$ is called the **universal norm map**, denoted by $\{u, v\}$. ⌟

Proof: ? □

Conj. (10.1.4.10) [Beilinson-Parshin]. For $k \in \texttt{Field}$, $\#k < \infty$, $X \in \mathcal{S}m\mathcal{P}\mathrm{roj}/k$, $i > 0$, $K_i(X) \otimes \mathbb{Q} = 0$. ⌟

Proof: □

Remark (10.1.4.11). In fact, when $\dim X = 0$ this is done by Quillen's computation of K-groups of fields, Cf.[On the Cohomology and K-theory of the General Linear Groups over a Finite Field, Quillen, 1972].

when $\dim X = 1$, $K_i(X)$ are in fact finite, by [Finite Generation of K-Groups of a Curve over a Finite Field, Don 1982]. ⌟

<u>**Comparison Maps**</u>

Prop. (10.1.4.12) [Logarithm Differential Maps]. For $S \in \mathcal{CR}\mathrm{ing}$, $R \in \mathcal{CR}\mathrm{ing}/S$, $X = \operatorname{Spec} R$ and $q \in \mathbb{N}$, there are homomorphisms

$$\mathrm{dlog} : K_q(R) \to \Omega^q_{R/\mathbb{S}},$$

satisfying

- $\mathrm{dlog}(a \cup b) = \mathrm{dlog}\, a \cup \mathrm{dlog}\, b$.
- If $a \in R^* \subset K_1(R)$, then $\mathrm{dlog}\, a = a^{-1}\mathrm{d}a \in \Omega^1_{R/S}$.
- On $K_0(R)$, dlog is the degree map.
- If R'/R is a finite flat extension of regular rings, then

$$\mathrm{tr}^{\Omega}_{R'/R} \circ \mathrm{dlog}_{R'} = \mathrm{dlog}_R \, \mathrm{tr}^K_{R'/R}.$$

⌟

Proof: □

Prop. (10.1.4.13). If $S \in \mathcal{CR}\mathrm{ing}$, and $Y = \operatorname{Spec} R$ is an smooth affine precurve over S, with a smooth completion X over S, and $Z = X \setminus Y$, then in fact the image of dlog is contained in

$$H^0(X, \Omega^q_{X/S}(\log Z)).$$

⌟

Proof: Cf.[Scholl, P411]?. □

K_2 of Curves

Prop. (10.1.4.14)[Faddeev's Exact Sequence]. Let X be a non-singular complete curve over a field k. Then for any point $P \in X$, consider the tame symbol $\{-,-\}_P$ at P(3.10.1.5), then there is an exact sequence

$$0 \to K_2(X) \to K_2(R(X)) \xrightarrow{\prod_{P\in X}\{-,-\}_P} \kappa(P)^\times.$$

⌟

Proof: ? □

Prop. (10.1.4.15) [Étale Abel-Jacobi Maps]. If Y is a smooth variety over a number field F, $p \in \mathbf{P}, n, j \in \mathbb{Z}_+$, and $H^{j+1}(Y_{\mathbb{Q}}, \mathbb{Q}_p(n))^{\mathrm{Gal}_F} = 0$, then there is an **Abel-Jacobi map**

$$\mathrm{AJ}_{n,j} : K_{2n-j-1}(Y) \to H^1(\mathrm{Gal}_F, H^j(Y_{\mathbb{Q}}, \mathbb{Q}_p)(n)).?$$

In case Y is a curve, $j = 1$ and $n = 2$, then the Abel-Jacobi map is defined integrally:

$$\mathrm{AJ}_2 : K_2(Y) \to H^1(\mathrm{Gal}_F, H^1(Y_{\mathbb{Q}}, \mathbb{Z}_p)(2)).$$

It is defined as follows: There is a Chern class map $c_2 : K_2(Y) \to H^2(Y, \mathbb{Z}_p(2))$, and by torsion-freeness(8.4.7.43) and weight reason?, the first column in the Hochschild-Serre spectral sequence

$$E_2^{i,j} = H^i(\mathrm{Gal}_F, H^j(Y_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(n))) \Rightarrow H^{i+j}(Y, \mathbb{Z}_p(n))$$

vanishes. So there is a low degree exact sequence

$$0 \to H^2(\mathrm{Gal}_F, H^0(Y_{\mathbb{Q}}, \mathbb{Z}_p(2))) \to H^2(Y, \mathbb{Z}_p(2)) \xrightarrow{\text{H-S}_2} H^1(\mathrm{Gal}_F, H^1(Y_{\mathbb{Q}}, \mathbb{Z}_p(2))) \to H^3(\mathrm{Gal}_F, H^0(Y_{\mathbb{Q}}, \mathbb{Z}_p(2))).$$

Then define $\mathrm{AJ}_2 = -\,\text{H-S}_2 \circ c_2$. ⌟

Proof: □

10.2 Brauer-Grothendieck Groups

References are [Central Simple Algebras and Galois Cohomology, Gille and Szamuely] and [The Brauer-Grothendieck Group].

1 Brauer Groups

Def. (10.2.1.1) [Brauer Groups]. For $X \in \mathcal{S}\text{ch}$, the **Brauer group** $\mathrm{Br}(X)$ is defined to be $\mathrm{Br}(X) = \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m) = H^2_{\text{fppf}}(X, \mathbb{G}_m)$(8.4.7.37). And for $R \in \mathcal{CR}\text{ing}$, $\mathrm{Br}(R)$ is defined to be $\mathrm{Br}(R) = \mathrm{Br}(\operatorname{Spec} R)$. ⌟

Prop. (10.2.1.2). If X is a regular Noetherian scheme that is qc or integral, $\mathrm{Br}(X) \to \mathrm{Br}(R(X))$ is injective, and $\mathrm{Br}(X)$ is a torsion Abelian group. ⌟

Proof: The qc case reduces to the integral case, and this follows from [Brauer-Grothendieck Groups]Chap3.5.

The second assertion follows from the first and the fact $\mathrm{Br}(R(X))$ is torsion(10.2.2.5). □

Cor. (10.2.1.3). If $X \to Y$ is a birational morphism of integral regular schemes, then $\mathrm{Br}(Y) \to \mathrm{Br}(X)$ is injective. ⌟

Proof: This follows from the fact $\mathrm{Br}(Y) \to \mathrm{Br}(X) \to \mathrm{Br}(R(X)) = \mathrm{Br}(R(Y))$ is injective. □

Azumaya Brauer Groups

Prop. (10.2.1.4) [Azumaya Algebras of Schemes]. For $X \in \mathcal{S}\text{ch}$, an **Azumaya algebra** over X is a coherent $\mathcal{O}_X$-algebra $\mathcal{A}$ s.t. $\mathcal{A}_x \neq 0$ for any $x \in X$, and satisfies the following equivalent definitions:

- There exists an étale covering $\{U_i \to X\}$ s.t. for each i, there exists $r_i \in \mathbb{Z}_+$ s.t. $\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{O}_{U_i} \cong \mathbf{End}(\mathcal{O}_{U_i}^{\otimes r_i})$.
- There exists an fppf covering $\{U_i \to X\}$ s.t. for each i, there exists $r_i \in \mathbb{Z}_+$ s.t. $\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{O}_{U_i} \cong \mathbf{End}(\mathcal{O}_{U_i}^{\otimes r_i})$.
- $\mathcal{A} \in \mathcal{V}\text{ect}_X$, and for any arithmetic point $x \in X$, $\mathcal{A}_x$ is isomorphic to $\mathrm{Mat}(r_x, \kappa(x))$ for some $r_x \in \mathbb{Z}_+$. And this r_x is called the **degree of** $\mathcal{A}$ at x.
- $\mathcal{A} \in \mathcal{V}\text{ect}_X$, and the canonical homomorphism $\mathcal{A} \otimes \mathcal{A}^{\text{op}} \to \mathbf{End}_{\mathcal{O}_X}(\mathcal{A})$ is an isomorphism.

In particular, this definition is compatible with the definition of Azumaya algebras over fields in(3.6.3.2), by(3.6.3.25).

The category of Azumaya algebras over X is denoted by Az_X. For $n \in \mathbb{Z}_+$, the subset of Azumaya algebras over X of constant degree n is denoted by $\mathrm{Az}^b(X)$. ⌟

Proof: $1 \to 2 \to 3 \to 4$ is trivial by(3.6.3.25). $4 \to 1$: Cf.[Milne80 Etale Cohomologies]P141.? □

Def. (10.2.1.5)[Azumaya Brauer Groups]. Let $X \in \mathcal{S}\text{ch}$, the **Azumaya Brauer group** $\mathrm{Br}_{\mathrm{Az}}(X)$ is defined to be the set of equivalence class of Azumaya algebras over X under the equivalence relation that $\mathcal{A} \sim \mathcal{A}'$ iff there exists $\mathcal{E}, \mathcal{E}' \in \mathcal{V}\text{ect}(X)$ with positive ranks at each point s.t.

$$\mathcal{A} \otimes_{\mathcal{O}_X} \mathbf{End}(\mathcal{E}) \cong \mathcal{A}' \otimes_{\mathcal{O}_X} \mathbf{End}(\mathcal{E}').$$

Moreover, $\mathrm{Br}_{\mathrm{Az}}(X)$ is a group under tensor product and the inverse is given by $\mathcal{A} \to \mathcal{A}^{\text{op}}$. ⌟

Proof: To show this is an equivalence and the group operation is well-defined, use the fact that for $\mathcal{E}, \mathcal{E}' \in \mathcal{V}\mathrm{ect}(X)$,

$$\mathbf{End}(\mathcal{E}) \otimes_{\mathcal{O}_X} \mathbf{End}(\mathcal{E}) \cong \mathbf{End}(\mathcal{E} \otimes \mathcal{E}').$$

And the inverse is of the form given, by(10.2.1.4). □

Lemma (10.2.1.6). Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{F}, \mathcal{G} \in \mathcal{V}\mathrm{ect}(\mathcal{O})$ s.t. $\mathbf{End}(\mathcal{F}) \cong \mathbf{End}(\mathcal{G})$, then there exists an invertible sheaf $\mathcal{L}$ s.t. $\mathcal{F} \otimes \mathcal{L} \cong \mathcal{G}$. ⌟

Proof: Let $\mathcal{L} \subset \mathcal{H}om(\mathcal{F}, \mathcal{G})$ be generated as an $\mathcal{O}_X$-module by local isomorphisms $\varphi : \mathcal{F} \cong \mathcal{G}$ s.t. the conjugation by φ coincides with the given isomorphism, then local computation and the fact all automorphisms of $\mathrm{Mat}(n)$ is inner shows that $\mathcal{L}$ is invertible, and the evaluation map

$$\mathcal{F} \otimes \mathcal{L} \to \mathcal{G}$$

is an isomorphism. □

Prop. (10.2.1.7). If $\mathcal{A} \in \mathrm{Az}_X$ has constant degree d, then $[\mathcal{A}] \in \mathrm{Br}_{\mathrm{Az}}(X)$ is annihilated by d. ⌟

Proof: Choose an étale covering $\{U_i \to X\}$ and isomorphisms $\mathcal{A}|_{U_i} \cong \mathrm{Hom}(\mathcal{F}_i, \mathcal{F}_i)$, where $\mathcal{F}_i \in \mathcal{V}\mathrm{ect}^d(X)$, then

$$\mathcal{A}^{\otimes d}|_{U_i} \cong \mathbf{End}(\mathcal{F}_i^{\oplus d}).$$

Consider the maps

$$p_i : \mathcal{F}_i^{\oplus d} \to \wedge^d \mathcal{F}_i \subset \mathcal{F}_i^{\oplus d},$$

then $p_i^2 = d! p_i$ and $\mathrm{rank}(p_i) = 1$. We show now that these p_i glue together to get a global section p of $\mathcal{A}^{\otimes d}$: by(10.2.1.6), there exist compatible invertible sheaves $\mathcal{L}_{ij}$ on $U_i \cap U_j$ s.t.

$$\mathcal{F}_i|_{U_{ij}} \otimes \mathcal{L}_{ij} \cong \mathcal{F}_j|_{U_{ij}}.$$

These isomorphisms can clearly generate isomorphisms to glue $\{p_i\}$ together.

Then consider $\mathcal{H} = \mathcal{A}^{\otimes d} \circ p \subset \mathcal{A}^{\otimes d}$, we claim that

- $\dim \mathcal{H} = d^d$,
- left multiplication by $\mathcal{A}^{\otimes d}$ induces an isomorphism $\mathcal{A}^{\otimes d} \cong \mathbf{End}(\mathcal{H})$.

Which will imply that $d[\mathcal{A}] = 0 \in \mathrm{Br}_{\mathrm{Az}}(X)$. To show these claims, it suffices to do local calculations: If $\mathcal{F} \cong \mathcal{O}_X e_1 \oplus \ldots \oplus \mathcal{O}_X e_d$, then $\mathcal{A} \cong \mathbf{End}(\mathcal{O}_X^d)$, and

$$p : e_{\sigma(1)} \otimes \ldots \otimes e_{\sigma(d)} \mapsto \mathrm{sgn}(\sigma) e_1 \otimes \ldots \otimes e_d, \sigma \in \mathcal{S}_d, \quad 0 \text{ on other basis vectors}$$

So

$$\mathcal{H} = \{f : \mathcal{F}^{\otimes d} \to \mathcal{F}^{\otimes d} : e_{\sigma(1)} \otimes \ldots \otimes e_{\sigma(d)} \mapsto \mathrm{sgn}(\sigma) v_1 \otimes \ldots \otimes v_d, \quad 0 \text{ on other basis vectors}\}$$

Then $\mathcal{A} \cong \mathbf{End}(\mathcal{O}_X^d)$ is clear. □

Cor. (10.2.1.8) [Azumaya Brauer Groups are Torsion]. If $X \in \mathcal{S}\mathrm{ch}$ is qc or connected, then $\mathrm{Br}_{\mathrm{Az}}(X)$ is a torsion Abelian group. ⌟

Comparison of Two Brauer Groups

Prop. (10.2.1.9) [Azumaya Brauer Groups via Cohomology]. Let $X \in \mathcal{S}\mathrm{ch}$, there exists an isomorphism of pointed sets

$$\mathrm{Az}_X^n \cong \check{H}^1_{\text{ét}}(X, \mathrm{PGL}(n)).$$

⌟

Proof: As $\mathrm{PGL}(n) = \mathrm{Aut}(\mathrm{Mat}(n))$ and any Azumaya algebra is a twist-form for $\mathrm{Mat}(n)_X$, any $\mathcal{A} \in \mathrm{Az}_X^n$ defines a 1-cocycle for $\mathrm{PGL}(n)$. It is clear that if this cocycle is a coboundary, then $\mathcal{A} \cong \mathrm{Mat}(n)_X$. Its left to show that any 1-cocycle comes from these: As $\mathrm{PGL}(n) \subset \mathrm{GL}(n^2)$, and 1-cocycle is a 1-cocycle for $\mathrm{GL}(n^2)$, thus by(6.1.6.1) corresponds to a vector bundle $\mathcal{E}$ of rank n^2. By taking a refinement, this means there is a covering $\{U_i \to X\}$ and isomorphisms $\varphi_i : \mathrm{Mat}(n, \mathcal{O}_{U_i}) \cong \mathcal{E}|_{U_i}$ as modules such that the transformation maps $\varphi_i^{-1} \circ \varphi_j \in \mathrm{PGL}(n, \mathcal{O}_{U_{ij}}) \subset \mathrm{GL}(n^2, \mathcal{O}_{U_{ij}})$, which means exactly $\mathcal{E} \in \mathrm{Az}_X^n$. □

Prop. (10.2.1.10) [$\mathrm{Br}(X)$ and $\mathrm{Br}_{\mathrm{Az}}(X)$]. Assume $X \in \mathcal{S}\mathrm{ch}$ is qc and every finite subset of X is contained in an affine scheme, by(6.3.2.19), the exact sequence

$$1 \to \mathbb{G}_m \to \mathrm{GL}(n) \to \mathrm{PGL}(n) \to 1$$

of algebraic groups gives a map

$$\check{H}^1_{\text{ét}}(X, \mathrm{GL}(n)) \to \mathrm{Az}^n(X) = \check{H}^1_{\text{ét}}(X, \mathrm{PGL}(n)) \xrightarrow{\delta_n} \check{H}^2_{\text{ét}}(X, \mathbb{G}_m) \hookrightarrow \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m) = \mathrm{Br}(X).$$

by(10.2.1.9) and(6.3.2.14). So the kernel of $\delta : \mathrm{Az}_X^n \to \mathrm{Br}(X)$ is given by Azumaya algebras of the form $\mathbf{End}(\mathcal{E})$ for $\mathcal{E} \in \mathcal{V}\mathrm{ect}^n(X)$. These maps for various n give a map

$$\mathrm{Az}(X) \to \mathrm{Br}(X).$$

Then

- This map is an injective homomorphism, so $\mathrm{Br}_{\mathrm{Az}}(X) \subset \mathrm{Br}(X)$.
- If X has an ample invertible sheaf, then the map induces an isomorphism

$$\mathrm{Br}_{\mathrm{Az}}(X) \cong \mathrm{Br}(X)_{\mathrm{tor}}.$$

In particular, if X is a regular quasi-projective scheme over some $A \in \mathcal{CR}\mathrm{ing}$, then by(10.2.1.2),

$$\mathrm{Br}_{\mathrm{Az}}(X) \cong \mathrm{Br}(X)_{\mathrm{tor}} = \mathrm{Br}(X).$$

For general X, this is also doable, by Gabber and de Jong**?**. ⌟

Proof: 1: By taking disjoint union, it suffices to show that for $\mathcal{A} \in \mathrm{Az}_X^n, \mathcal{B} \in \mathrm{Az}_X^m$,

$$\delta_{mn}(\mathcal{A} \otimes \mathcal{B}) = \delta_n(\mathcal{A}) \cdot \delta_m(\mathcal{B}).$$

But this is clear from the description of δ_n: by the hypothesis and [Milne80 Etale Cohomology, Prop4.2.19]**?** and(6.3.2.19), we may take an étale refinement $\{U_i\}$ and assume the cocycle corresponding to $\mathcal{A}$ is given by a cocycle c_{ij} s.t. $c_{ij} \in \Gamma(U_{ij}, \mathrm{GL}(n))$. Then $\delta(\mathcal{A})$ is represented by the 2-cocycle with $a_{ijk} = c_{jk} c_{ik}^{-1} c_{ij} \in \Gamma(U_{ijk}, \mathbb{G}_m)$.

The injectivity follows from the presentation

$$\mathrm{Br}_{\mathrm{Az}}(X) \cong \varinjlim \mathrm{Az}_X^n / \sim = \varinjlim \check{H}^1_{\text{ét}}(X, \mathrm{PGL}(n))/\check{H}^1_{\text{ét}}(X, \mathrm{GL}(n)).$$

and the fact the image of $\check{H}^1_{\text{ét}}(X, \mathrm{GL}(n))$ in $\check{H}^1_{\text{ét}}(X, \mathrm{PGL}(n))$ is the class of $\mathbf{End}(n, E)$: a $\mathtt{a} \in \check{H}^1_{\text{ét}}(X, \mathrm{GL}(n))$ corresponds to a vector bundle $\mathcal{E}$ of rank n with trivializations $\varphi_i : \mathcal{O}_{U_i}^n \cong E|_{U_i}$ s.t. $\mathtt{a}$ is represented by $(\varphi_i^{-1}\varphi_j)$. Then $\mathcal{A} = \mathbf{End}(n, \mathcal{E}) \in \mathrm{Az}_X^n$ has trivializations $\psi_i : \mathrm{Mat}(n, \mathcal{O}_{U_i}) \cong \mathbf{End}(n, \mathcal{E})|_{U_i}$, and $\mathcal{A}$ corresponds to the 1-cocycle

$$(\psi_i^{-1}\psi_j) = (\alpha_{ij}), \quad \alpha_{ij}(a) = \varphi_j^{-1}\varphi_i a \varphi_i^{-1}\varphi_j, a \in \mathrm{Mat}(n, \mathcal{O}_{U_{ij}})$$

which is exactly the image of the class $\mathtt{a}$ under the map $\mathrm{GL}(n) \to \mathrm{PGL}(n) : u \mapsto \mathrm{conj}(u)$.

2: Cf.[Brauer-Grothendieck Group]Chap4.? □

Prop. (10.2.1.11) [Kummer Exact Sequences]. For $X \in \mathcal{S}\mathrm{ch}, n \in \mathbb{Z}_+$, the Kummer exact sequence of algebraic groups

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \to 1$$

gives exact sequences

$$0 \to \mathrm{Pic}(X)/n\,\mathrm{Pic}(X) \to H^2_{\mathrm{fppf}}(X, \mu_n) \to \mathrm{Br}(X)[n] \to 0,$$

$$0 \to \mathrm{Br}(X)/n\,\mathrm{Br}(X) \to H^3_{\mathrm{fppf}}(X, \mu_n) \to \mathrm{H}^3_{\text{ét}}(X, \mathbb{G}_m)[n] \to 0.$$

by(8.4.7.37). ⌟

Prop. (10.2.1.12) [Mayer-Vietoris Exact Sequence]. Let $X \in \mathcal{S}\mathrm{ch}$ and $X = U \cup V$ be a Zariski covering with $U \cap V = W$, then by(10.2.1.2) there is an exact sequence

$$\begin{aligned} 0 &\to \Gamma(X, \mathcal{O}_X^\times) \to \Gamma(V, \mathcal{O}_X^\times) \oplus \Gamma(V, \mathcal{O}_X^\times) \to \Gamma(W, \mathcal{O}_X^\times) \\ &\to \mathrm{Pic}(X) \to \mathrm{Pic}(U) \oplus \mathrm{Pic}(V) \to \mathrm{Pic}(W) \\ &\to \mathrm{Br}(X) \to \mathrm{Br}(U) \oplus \mathrm{Br}(V) \to \mathrm{Br}(W) \to \mathrm{H}^3_{\text{ét}}(X, \mathbb{G}_m) \to \ldots \end{aligned}$$

And when U is locally factorial, then $\mathrm{Pic}(U) \to \mathrm{Pic}(W)$ is surjective?, so there is an exact sequence

$$0 \to \mathrm{Br}(X) \to \mathrm{Br}(U) \oplus \mathrm{Br}(V) \to \mathrm{Br}(W) \to \mathrm{H}^3_{\text{ét}}(X, \mathbb{G}_m).$$

⌟

Prop. (10.2.1.13) [Hochschild Spectral Sequence]. ⌟

Residue Homomorphism

Prop. (10.2.1.14) [Faddeev]. For $k \in \mathtt{Field}$, there is an exact sequence

$$0 \to \mathrm{Br}(k) \to \mathrm{Br}(\mathbb{P}^1_k) \xrightarrow{\mathrm{res}} \bigoplus_{x \in \mathrm{closed}(\mathbb{P}^1_k)} H^2(\kappa(x), \mathbb{Q}/\mathbb{Z}) \to H^1(k, \mathbb{Q}/\mathbb{Z}) \to 0$$

⌟

Proof: Cf. [GS06, 6.4.5]?. □

Artin Conjecture

Conj. (10.2.1.15) [Artin]. For $X \in \mathcal{S}\mathrm{ch}/\mathbb{Z}$ proper, $\#\operatorname{Br}(X) < \infty$. ⌟

Proof: Cf.[Central Simple Algebras and Galois Cohomology, 6.4.5.]. □

Prop. (10.2.1.16) [Artin & Tate Conjecture]. For a proper surface $X/\mathbb{Z}$, the Artin conjecture for X(10.2.1.15) is equivalent to Tate conjecture for divisors of X. ⌟

Proof:

□

Prop. (10.2.1.17) [Artin vs. Tate-Šafarevič Conjecture]. For $F \in \mathtt{NField}$, for a regular integral scheme X of dimension 2 that is flat proper over $\mathcal{O}_F$ that has a section, the Artin conjecture for X is equivalent to the finiteness of $\text{Ш}(\operatorname{Jac}(X_F))$. ⌟

Proof: □

2 Field cases

Prop. (10.2.2.1) [Indexes of Brauer Classes]. For $k \in \mathtt{Field}$, any Brauer class in $\operatorname{Br}_{\mathrm{Az}}(k)$ is represented by a unique central division ring.

So we can define the **index of the Brauer class** D as the $\operatorname{ind}([D]) = \sqrt{[D:k]} \in \mathbb{Z}_+$(3.6.3.16). And the **period of the Brauer class** D to be the exponent of $[D] \in \operatorname{Br}_{\mathrm{Az}}(k)$. ⌟

Proof: The existence of this division ring follows from Wedderburn theorem(3.6.1.22), and to show uniqueness, notice if

$$\operatorname{Mat}(n; D) \cong \operatorname{Mat}(m; D') = A$$

when we can recover D as $D = D' = \operatorname{End}_A(V)$, where V is the unique simple module, by(3.6.1.21). □

Prop. (10.2.2.2). For $k \in \mathtt{Field}$ and $\alpha \in \operatorname{Br}(k)$, $\operatorname{per}(\alpha) | \operatorname{ind}(\alpha)$. ⌟

Proof: ? □

Prop. (10.2.2.3) [Period-Index Conjecture]. For $k \in \mathtt{Field}, k = \overline{k}$ and $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$, if $\alpha \in \operatorname{Br}(R(X))$, then $\operatorname{ind}(\alpha) | \operatorname{per}(\alpha)^{\dim X - 1}$. ⌟

Prop. (10.2.2.4) [Brauer Groups and Galois Cohomology]. For any $k \in \mathtt{Field}$, the **Brauer group** $\operatorname{Br}(k)$ is defined as the profinite cohomology $H^2(\operatorname{Gal}(k^{\mathrm{sep}}/K), (k^{\mathrm{sep}})^\times)$. For a Galois extension L/k, $\operatorname{Br}(L/k)$ is defined as $H^2(\operatorname{Gal}(L/k), L^\times)$. Then by(8.7.2.2) we have

$$\varinjlim \operatorname{Br}(L/k) = \operatorname{Br}(k).$$

And by Hochschild-Serre spectral sequence and by Hilbert's multiplicative theorem90: $H^1(H, k_s^*) = 0$, we have the low term:

$$0 \to \operatorname{Br}(L/k) \xrightarrow{\inf} \operatorname{Br}(k) \xrightarrow{\mathrm{res}} \operatorname{Br}(L)^{\operatorname{Gal}(L/k)} \to H^3(\operatorname{Gal}(L/k), L^\times) \to H^3(k, (k^{\mathrm{sep}})^\times).$$

So $\operatorname{Br}(L/k)$ is the kernel of $\operatorname{Br}(k) \to \operatorname{Br}(L)$. ⌟

Proof: Cf.[Neukirch Cohomology of Number Fields Chap6.3].? □

Cor. (10.2.2.5) [Brauer Groups are Torsion]. For any $k \in \mathtt{Field}$, $\mathrm{Br}(k) \in \mathcal{A}b^{\mathrm{tor}}$, by(8.7.2.3). In particular, $\mathrm{Br}_{\mathrm{Az}}(k) \cong \mathrm{Br}(k)$ by(10.2.1.10). ⌟

Cor. (10.2.2.6). For any $k \in \mathtt{Field}, \#k < \infty$, $\mathrm{Br}(\mathbb{F}_q) = 0$, because the finite Galois extension are cyclic and unramified. ⌟

Prop. (10.2.2.7) [Finite Fields]. If $k \in \mathtt{Field}^{\mathrm{fin}}$, then for any $n \in \mathbb{N}$, $\check{H}^1(k, \mathrm{PGL}(n)) = 0$, and $\mathrm{Br}(k) = 0$. ⌟

Proof: This follows from(10.2.2.1) and the fact any finite division ring is commutative(3.2.1.8). □

Prop. (10.2.2.8) [Valued Fields]. Let (R, K, k) be a complete DVR, then there exists a split exact sequence

$$0 \to \mathrm{Br}(k) \to \mathrm{Br}_{\mathrm{tame}}(K) \to H^1(k, \mathbb{Q}/\mathbb{Z}) \to 0.$$

⌟

Proof: Cf.[Brauer-Grothendieck Group, P32]. □

Prop. (10.2.2.9). ⌟

3 Local Field cases

Thm. (10.2.3.1) [Brauer Groups of Local Fields]. For $K \in \mathtt{LField}$,

- the invariant map(14.6.2.7) is a canonical injection

$$\mathrm{inv} : \mathrm{Br}(K) \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

  whose image is

$$\begin{cases} \mathbb{Q}/\mathbb{Z} & , K \in p\text{-}\mathtt{LField} \\ \frac{1}{2}\mathbb{Z}/\mathbb{Z} & , K = \mathbb{R} \\ 0 & , K = \mathbb{C} \end{cases}$$

- Every Azumaya algebra over K is cyclic**?**.
- Every element of $\mathrm{Br}(K)$ has period equal to index(10.2.2.1).

⌟

Proof: 1: This follows from the definition of a class formation(14.6.1.1).
The rest follows from [Poonen, P25].**?** □

Cor. (10.2.3.2). For $K \neq \mathbb{C} \in \mathtt{LField}$, there exists a unique nontrivial quaternion algebra over K, and its the only division ring with exponent 2. ⌟

4 Global Field cases

Thm. (10.2.4.1) [Brauer-Hasse-Noether]. For $F \in \mathtt{NField}$,

- there is a canonical exact sequence

$$1 \to \mathrm{Br}(F) \to \bigoplus_{\mathfrak{p} \in \Sigma_F} \mathrm{Br}(F_{\mathfrak{p}}) \xrightarrow{\mathrm{inv}_F} \mathbb{Q}/\mathbb{Z} \to 0,$$

  and in the characterization via Azumaya algebras(10.2.1.5)(10.2.1.10), the first map sends $[D]$ to the family $([D \otimes_F F_v])_v$.

- Every Azumaya algebra over F is cyclic**?**.
- Every element of $\mathrm{Br}(F)$ has exponent equal to index.

⌟

Proof: 1, 2: Cf.[Neukirch P146] and [Poonen, P26].**?**

3: It follows from item1 that for any division ring D/F, $[D]\in\mathrm{Br}(F)$has exponent $n=\mathrm{lcm}(\mathrm{ord}(\mathrm{inv}_v([D])))$. So it follows from(10.2.3.1) that there $n_v|\,\mathrm{ind}([D])$ for any v, so $n|\,\mathrm{ind}([D])$.

And it follows from Grünwald-Wang(14.6.4.32) and the local-global compatibility of inv_v that there exists a cyclic extension L/K of degree n that splits D. Then it follows from(3.6.3.17)(10.2.2.1) that there exists $B=\mathrm{Mat}(r;D)$ s.t. $L\subset B$ and $[B:F]=[L:K]^2$. Thus $[D:F]|[L:K]^2$, so $\mathrm{ind}(D)=n$. □

Prop. (10.2.4.2)[Norm Groups of Division Rings, Eichler]. If $F\in\mathtt{NField}$ and D/F is a division ring of index n, then $\mathrm{Nm}_{D/K}(D^\times)\subset F^\times$ is the set of elements that is positive under all $v\in\Sigma_F^{\mathbb{R}}$ s.t. $D_v\ncong\mathrm{Mat}(n;F_v)$. ⌟

Proof: Cf.[P-R94]P38. □

Prop. (10.2.4.3) [Wang]. If $F\in\mathtt{NField}$ and D/F is a division ring of index n, then $SL(1;D)=[D^\times,D^\times]$. ⌟

Prop. (10.2.4.4). ⌟

5 Severi-Brauer Varieties

References are [Severi − Brauer varieties: a geometric treatment, Kollar] and [Central Simple Algebras and Galois Cohomology].

Def. (10.2.5.1) [Severi-Brauer Varieties]. For $k\in\mathtt{Field}$, a **Severi-Brauer variety** over k is a k-variety X that is a k-form for $\mathbb{P}^n_k$ for some $n\in\mathbb{N}$.

If K/k is a field extension and $X_k\cong\mathbb{P}^n_K$, then K is called a **splitting field** for X. ⌟

Prop. (10.2.5.2). Let $k\in\mathtt{Field}$ and X a Severi-Brauer variety over k, then a **twisted-linear subvariety** of X is a closed subvariety of X s.t. the inclusion $Y_{\overline{k}}\subset X_{\overline{k}}\cong\mathbb{P}^n_{\overline{k}}$ embeds $Y_{\overline{k}}$ as a linear subvariety of $\mathbb{P}^n_{\overline{k}}$. ⌟

Prop. (10.2.5.3)[Châtelet]. For $k\in\mathtt{Field}$ and an n-dimensional Severi-Brauer variety X over k, the following are equivalent:

- $X\cong\mathbb{P}^n_k$.
- $X\sim\mathbb{P}^n_k$.
- $X(k)\neq\varnothing$.
- X contains a twisted-linear subvariety of codimension 1.

⌟

Proof: $1\to 2$ is trivial. If 2 holds, then to show item3, if $\#k=\infty$, then any Zariski open subset of $\mathbb{P}^n_k$ contains a k-point, and if $\#k<\infty$, clearly any Severi-Brauer variety over k splits over a finite Galois field extension of k, so by the proof of(10.2.5.6)**?** shows that $SB_n(K)\cong H^1(k,\mathrm{PGL}(n))=1$(10.2.2.7). Thus $X\cong\mathbb{P}^n_k$ has a rational point.

4 → 1: The twisted-linear subvariety is a divisor of X**?**, so it defines a rational map φ_D into some projective variety, and when base changed to $\overline{k}$, it is the isomorphism of X with $\mathbb{P}^n_{\overline{k}}$. Thus it must be an isomorphism.

3 → 4: Cf.[Central Simple Algebras]P341.**?** □

Cor. (10.2.5.4) [Galois Splitting Fields]. Let $k \in$ `Field` and X a Severi-Brauer variety over k, then X has a finite Galois splitting field. ⌟

Proof: It suffices to show that k^s is a splitting field for X. But for this, by the theorem, it suffices to notice X_{k_s} always has a rational point(6.11.1.10). □

Cor. (10.2.5.5). Severi-Brauer groups satisfy the local-global property. ⌟

Proof: Cf.[Poonen]P108. □

Prop. (10.2.5.6) [Severi-Brauer Varieties and Galois Cohomologies]. For $k \in$ `Field`, there is an isomorphism of pointed sets $H^1(k, \mathrm{PGL}(n)) \cong SB_n(L/K)$, where $SB_n(L/K)$ is the isomorphism classes of Severi-Brauer varieties of dimension $n-1$ that splits in L. ⌟

Proof: Cf.[Neukirch Cohomology of Number Fields P348]. □

6 Brauer-Manin Obstruction

Prop. (10.2.6.1). For $F \in$ `GField` and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{sm}}/F$, there is a natural continuous right-linear pairing

$$\gamma : X(\mathbf{A}_F) \times \mathrm{Br}(X) \to \mathbb{Q}/\mathbb{Z}$$

s.t. the restriction to $X(F) \times \mathrm{Br}(X)$ is trivial.

Let $X(\mathbf{A}_F)^{\mathrm{Br}}$ denote the left kernel of γ, then we say the **Brauer-Manin obstruction** is sufficient for X if $X(F) \subset X(\mathbf{A}_F)^{\mathrm{Br}}$ is dense. ⌟

Proof: **?** □

Prop. (10.2.6.2). If $F \in$ `GField` and $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/F$, then if X satisfies the weak approximation, then Brauer-Manin obstruction is sufficient. ⌟

Proof: □

7 Norm Residue Isomorphism Theorem

See Voevodsky's work.

11 Condensed Mathematics and Analysis

11.1 Condensed Mathematics(Scholze)

Main references are [Condensed Mathematics, Scholze]. [Lectures on Condensed Mathematics, Clausen-Scholze], [Lectures on Analytic Geometry, Clausen-Scholze].

Notation (11.1.0.1).
- Use notations defined in Profinite Cohomology.

⌟

1 Introduction

Remark (11.1.1.1). Delete this subsection.? ⌟

Condensed mathematics is invented to overcome the subtleties when dealing with algebra together with topology. For example, the category of topological Abelian groups doesn't form an Abelian category.

2 Condensed Objects

Def. (11.1.2.1) [κ-Condensed Objects]. The pro-étale site $*_{pro\,\text{ét}}$ of a point is isomorphic to $\mathcal{P}\mathrm{rof}$ in the standard topology. For any uncountable strong limit cardinal κ, the site $\mathcal{P}\mathrm{rof}_\kappa$ is the category of κ-small profinite sets S in the standard topology.

Then for any $\mathcal{C}\in\mathcal{C}\mathrm{at}$, we can define the category $\mathrm{Cond}_\kappa(\mathcal{C})$ of **κ-condensed objects** in $\mathcal{C}$ to be the category $\mathrm{Func}(\mathcal{P}\mathrm{rof}_\kappa,\mathcal{C})$. ⌟

Prop. (11.1.2.2) [Adjointness]. Given an uncountable strong limit cardinal κ, the functors

$$X\mapsto \underline{X}:\mathcal{T}\mathrm{op}\,/\,\mathcal{G}\mathrm{rp}\,/\,\mathcal{CA}\mathrm{lg}\to \mathrm{Cond}(\mathcal{S}\mathrm{et})/\,\mathrm{Cond}(\mathcal{G}\mathrm{rp})/\,\mathrm{Cond}(\mathcal{CA}\mathrm{lg})$$

are faithful, and fully faithful when restricted to the category of κ-small objects.

And there is an adjunction

$$X\mapsto \underline{X}:\mathcal{T}\mathrm{op}\rightleftharpoons \mathrm{Cond}(\mathcal{S}\mathrm{et}):T\mapsto T(*)_{\mathrm{top}}=\varinjlim_{S\in\mathcal{P}\mathrm{rof}_\kappa/T} S.$$

In particular, $\underline{X}(*)_{\mathrm{top}}\cong X_{\kappa\text{-}\mathcal{CG}}$. ⌟

Proof: Firstly, $\underline{X}$ is truly a condensed set: for the sheaf condition, let $S'\to S$ be surjective morphism of profinite spaces, then the sheaf condition is true set-theoretically, and for any map $S\to T$, if $S'\to S\to T$ is continuous, then $S\to T$ is continuous, because $S'\to S$ is a closed map.

It suffices to check the set case, and the faithfulness and fully faithfulness follows from the adjointness

$$\mathrm{Hom}_{\kappa\text{-Cond}(\mathcal{S}\mathrm{et})}(T, \underline{X}) = \mathrm{Hom}(T(*)_{\mathrm{top}}, X).$$

Notice that any $s \in T(S)$ induces a map of sets $\overline{s} : S \to T(*) : x \mapsto T(* \xrightarrow{x} S)(s)$, inducing the topology of $T(*)$. And by definition, a morphism $T \to \underline{X}$ is just a morphism $T(*) \to X$ that for any $S \to T$, the composition $S \to T(*) \to X$ is continuous. And by definition, this is just a morphism from $T(*)_{\mathrm{top}} \to X$.

The last assertion follows from the fact any compact Hausdorff space S is a quotient space of its Stone-Čech compactification. □

Prop. (11.1.2.3)[Free Condensed Abelian Groups]. By the adjoint functor theorem(4.1.1.34), the forgetful functor from $\mathrm{Cond}(\mathcal{A}\mathrm{b})$ to $\mathrm{Cond}(\mathcal{S}\mathrm{et})$ has a left adjoint $T \mapsto \mathbb{Z}[T]$. Concretely, $\mathbb{Z}[T]$ is the sheafification of the functor that sends a compact Hausdorff space S to the free Abelian group $\mathbb{Z}[T(S)]$. In particular, by Yoneda lemma, for any compact Hausdorff space S, there is a condensed Abelian group $\mathbb{Z}[S]$ that for any condensed Abelian group M, $\mathrm{Hom}(\mathbb{Z}[S], M) = M(S)$. ⌟

Lemma (11.1.2.4). Consider the site of all κ-small compact Hausdorff topological spaces, then the category of sheaves on this site is equivalent to that of $\mathcal{P}\mathrm{rof}_\kappa$(via restriction). ⌟

Proof: Use(6.1.2.25), because any κ-small compact Hausdorff space is a quotient space of a κ-small profinite space(βS_0(4.4.2.15), noticing that $|\beta S| \leq 2^{2^{|S|}} < \kappa$). □

Lemma (11.1.2.5). Consider the site of all κ-small extremally disconnected spaces, then the category of sheave son this site is equivalent to that of κ-small condensed sets, via restriction. ⌟

Proof: Because any κ-small compactly generated space is a quotient space of a κ-small extremally disconnected space(βS(4.4.2.17), noticing that $|\beta S| \leq 2^{2^{|S|}} < \kappa$). □

Cor. (11.1.2.6) [$\mathrm{Cond}(\mathcal{A}\mathrm{b})$ **and Extremally Disconnected Spaces].** The category of κ-condensed Abelian groups is equivalent to the category of presheaves $\mathcal{F}$ on the category of κ-extremally disconnected spaces that $\mathcal{F}(\varnothing) = 0$ and $\mathcal{F}(S_1 \coprod S_2) = \mathcal{F}(S_1) \times \mathcal{F}(S_2)$. ⌟

Proof: It suffices to show that the second sheaf condition is automatic: For a surjective map of extremally disconnected spaces $f : \widetilde{S} \to S$, there is an isomorphism

$$\mathcal{F}(S) \xrightarrow{\mathcal{F}(f)} \{g \in \mathcal{F}(\widetilde{S}) | \mathcal{F}(p_1)(g) = \mathcal{F}(p_2)(g)\}.$$

By(4.4.1.32), there is a section $\sigma : S \to \widetilde{S}$ that $f \circ \sigma = \mathrm{id}_S$, thus $\mathcal{F}(\sigma) \circ \mathcal{F}(f) = \mathrm{id}$, thus $\mathcal{F}(f)$ is injective. For the surjectivity, suppose $\mathcal{F}(p_1)(g) = \mathcal{F}(p_2)(g)$, then

$$\mathcal{F}(p_2)(\mathcal{F}(f)\mathcal{F}(\sigma)(g)) = \mathcal{F}((\sigma \circ f) \times_S \mathrm{id}_{\widetilde{S}})\mathcal{F}(p_1)(g) = \mathcal{F}((\sigma \circ f) \times_S \mathrm{id}_{\widetilde{S}})\mathcal{F}(p_2)(g) = \mathcal{F}(p_2)(g)$$

And similarly $\mathcal{F}(p_2)$ is injective, thus $g = \mathcal{F}(f)\mathcal{F}(\sigma)(g)$ is in the image. □

Prop. (11.1.2.7)[Category of Condensed Abelian Groups]. The category of κ-condensed Abelian groups satisfies Grothendieck's Axiom $AB3, AB4, AB5, AB6, AB3^*, AB4^*$. And also it is generated by compact projective objects. ⌟

Proof: We use(11.1.2.6). Because all limits and colimits of Abelian groups commutes with finite products, the limits and colimits in the category of condensed Abelian groups are just the pointwise limits and colimits, thus the axioms follow form that of the category $\mathcal{A}$b.

By(11.1.2.3), the condensed Abelian group $\mathbb{Z}[S]$ for S κ-extremally disconnected satisfies $\mathrm{Hom}(\mathbb{Z}[S], M) = M(S)$, and by arguments above, $M \to M(S)$ commutes with all limits and colimits, thus $\mathbb{Z}[S]$ is compact and projective. And we show every M admits a surjection from some direct sum of $\mathbb{Z}[S]$: use Zorn's lemma, choose the maximal object M' that admits a surjection, if $M/M' \neq 0$, then find a nonzero map $\mathbb{Z}[S] \to M/M'$(because $M(S) = 0$ for any S implies $M = 0$), then it lifts to a nonzero map $\mathbb{Z}[S] \to M$ by projectivity, contradiction. □

Cor. (11.1.2.8).
- We can define the tensor of two condensed Abelian groups M, N as the shifification of the presheaf $S \mapsto M(S) \otimes N(S)$.
- We can define an internal Hom, which is right adjoint to tensor operator. In particular, for any compact Hausdorff space S, $\underline{\mathrm{Hom}}(M, N)(S) = \mathrm{Hom}(\mathbb{Z}[S] \otimes M, N)$.
- The derived category $D(\mathrm{Cond}(\mathcal{A}\mathrm{b}))$ is also compactly generated, and we can define Rtensor and RHom as in2.

Proof: Cf.[Condensed Mathematics, P13].? □

⌟

Prop. (11.1.2.9). Let $\kappa' > \kappa$ be uncountable strongly limit cardinals, then there is a natural functor from the set of κ-condensed sets to the category of κ'-condensed sets by pulling back along the morphism of sites $\mathcal{P}\mathrm{rof}_{\kappa'} \to \mathcal{P}\mathrm{rof}_{\kappa}$. Then this functor is fully faithful and commutes with all colimits and λ-small limits, where λ is the cofinality of κ. ⌟

Proof: This should have something to do with(6.1.2.25), thus it is left adjoint to the restriction functor and $i^s i_s \cong \mathrm{id}$, thus it is fully faithful and commutes with all colimits. For the limits, cf.[Condensed Mathematics, P14].? □

Def. (11.1.2.10) [Condensed Objects]. For any $\mathcal{C} \in \mathcal{C}\mathrm{at}$, define the category $\mathrm{Cond}(\mathcal{C})$ of **condensed objects** in $\mathcal{C}$ is defined to be the filtered colimits of the category of κ-condensed sets along the filtered poset of all uncountable limit cardinals κ. ⌟

Prop. (11.1.2.11). If X is a T1 topological space, then $\underline{X}$ is a condensed set that all maps from points are quasicompact. Conversely, if T is a condensed set that all maps from points are quasicompact, then $T(*)_{\mathrm{top}}$ is a compactly generated $T1$ space. ⌟

Proof: Cf.[Condensed Mathematics, P16].? □

Prop. (11.1.2.12) [$\mathcal{T}$op and $\mathrm{Cond}(\mathcal{S}\mathrm{et})$].
- The functor $X \mapsto \underline{X}$ induces an equivalence between compact Hausdorff space and qcqs condensed sets.
- A compactly generated space X is weak Hausdorff iff $\underline{X}$ is quasi-separated. For any quasi-separated condensed set T, the space $T(*)_{\mathrm{top}}$ is compactly generated weak Hausdorff.

⌟

Proof: Cf.[Condensed Mathematics, P16].? □

Prop. (11.1.2.13). The example $(R, \mathrm{disc}) \to (\mathbb{R}, \mathrm{Nat})$.?

In particular, enlarging topological abelian groups into an abelian category precisely forces us to include non-quasi-separated objects. ⌟

3 Cohomologies

Prop. (11.1.3.1). For any set I, there is an isomorphism

$$\check{H}^i(\prod_I S^1, \mathbb{Z}) \cong \bigwedge^i(\oplus_I \mathbb{Z}).$$

preserving the natural cup product. ⌟

Proof: If I is finite, this follows from the classical calculation of the cohomology of the tori. If I is infinite, then we should use lemma(11.1.3.2) below. □

Lemma (11.1.3.2). If $S_j, j \in J$ is a filtered system of compact Hausdorff spaces and $S = \varprojlim_{j\in J} S_j$, then there are natural maps

$$\varinjlim_j \check{H}^i(S_j, \mathbb{Z}) \to \check{H}^i(S, \mathbb{Z})$$

are isomorphisms. ⌟

Proof:

□

Prop. (11.1.3.3) [$\mathbb{Z}$-Cohomology]. Let S be a compact Hausdorff space, then there are natural functorial isomorphisms

$$H^i(S, \underline{\mathbb{Z}}) \cong H^i_{\text{Cond}}(S, \mathbb{Z}).$$

⌟

Proof: Because the Čech and sheaf cohomology of S are equal by(6.3.5.13), it suffices to calculate for Čech cohomology.

Firstly, if S is a profinite set, let $S = \varprojlim_j S_j$ where S_j are finite, then □

Prop. (11.1.3.4) [$\mathbb{R}$-Cohomologies Vanish]. For any compact Hausdorff space S,

$$H^i_{\text{Cond}}(S, \mathbb{R}) = 0$$

for $i > 0$, and $H^0(S, \mathbb{R}) = C(S, \mathbb{R})$. ⌟

Proof: Cf.[Condensed Mathematics, P21]. □

4 LCAs

5 Solid Abelian Groups

Def. (11.1.5.1) [Solid Abelian Group]. For a profinite set $S = \varprojlim S_i$, define the condensed Abelian group

$$\mathbb{Z}[S]^{\blacksquare} = \varprojlim \mathbb{Z}[S_i].$$

There is a natural map $S \to \mathbb{Z}[S]^{\blacksquare}$, inducing a map $\mathbb{Z}[S] \to \mathbb{Z}[S]^{\blacksquare}$.

Then a **solid Abelian group** is a condensed Abelian group A that for any profinite set S and a morphism of Abelian groups $\mathbb{Z}[S] \to A$ extends to a morphism $\mathbb{Z}[S]^{\blacksquare} \to A$.

A complex $C \subset D(\text{Cond}(\mathcal{A}\text{b}))$ is called a **solid complex** if for all profinite set S, the natural map

$$R\operatorname{Hom}(\mathbb{Z}[S]^{\blacksquare}, C) \to R\operatorname{Hom}(\mathbb{Z}[S], C)$$

is an isomorphism. ⌟

Prop. (11.1.5.2) [Free Solid Abelian Group]. For a profinite set S,

- Consider**?**

$$\mathbb{Z}[S]^{\blacksquare} = \varprojlim \mathbb{Z}[S_i] = \varprojlim \underline{\mathrm{Hom}}(C(S_i, \mathbb{Z}), \mathbb{Z}) = \underline{\mathrm{Hom}}(C(S, \mathbb{Z}), \mathbb{Z}).$$

  This means that the underlying Abelian group of $\mathbb{Z}[S]^{\blacksquare}$ is the $\mathbb{Z}$-valued measures on S.

- There is some set $|I| \leq 2^{|S|}$, that there is an isomorphism $\mathbb{Z}[S]^{\blacksquare} \cong \prod_I \mathbb{Z}$.
- $\mathbb{Z}[S]^{\blacksquare}$ is solid both as a module and a complex.

⌟

Proof: 2: Take an isomorphism $C(S, \mathbb{Z}) \cong \oplus_I \mathbb{Z}$**?**, then

$$\mathbb{Z}[S]^{\blacksquare} = \underline{\mathrm{Hom}}(C(S, \mathbb{Z}), Z) \cong \underline{\mathrm{Hom}}(\bigoplus_I \mathbb{Z}, \mathbb{Z}) \cong \prod_I \mathbb{Z}.$$

3: We need to show the extension property, but by2, it suffices to show for $\mathbb{Z}[S]^{\blacksquare} = \mathbb{Z}$.**?** □

Prop. (11.1.5.3) [Category of Solid Abelian Groups]. The category Solid $\subset$ Cond($\mathcal{A}$b) is an Abelian subcategory that is stable under all limits, colimits and extensions. The objects $\prod_I \mathbb{Z}$, where I is any set, form a family of compact projective generators. The inclusion Solid $\subset$ Cond($\mathcal{A}$b) admits a left adjoint $M \mapsto M^{\blacksquare}$ which is the unique colimit-preserving extension of $\mathbb{Z}[S] \mapsto \mathbb{Z}[S]^{\blacksquare}$.

The functor $D(\mathrm{Solid}) \to D(\mathrm{Cond}(\mathcal{A}b))$ is fully faithful and its essential image is precisely the solid Abelian groups, and the inclusion admits a left adjoint $C \to C^{L\blacksquare}$ which is left derived functor of $M \to M^{\blacksquare}$. ⌟

6 Analytic Geometry

7 Complex Geometry

11.2 Topological Commutative Algebra

Main references are [Hub93], [Bos15], [B-S19], [Mor19] and [Sch12].

1 Topological Abelian Groups and Rings

Def. (11.2.1.1) [Topological Rings]. A **topological Abelian group** is an Abelian group with a topology structure that the addition and inversion are all continuous.

A **topological ring** is a ring endowed with a topology structure that the addition, multiplication and inversion are all continuous.

Similarly we can define a **topological module** over a topological ring. ⌟

Def. (11.2.1.2) [Topologically Nilpotent Element]. Let A be a topological ring, then $x \in A$ is called **topologically nilpotent** iff $x^n \to 0$ when $n \to \infty$. ⌟

Def. (11.2.1.3) [Bounded Sets]. A subset S in a topological ring is called **bounded** iff for all open nbhd U of 0, there exists an open nbhd V of 0 that $VS \subset U$ ⌟

Def. (11.2.1.4)[Strict Morphism]. A **strict morphism** of topological rings is a continuous morphism that the quotient topology and the subspace topology coincides on the image. ⌟

Completion of Topological Abelian Groups

Prop. (11.2.1.5) [Completion]. There exists a completion functor left adjoint to the forgetful functor from the category of complete topological Abelian groups to the category of topological Abelian groups, given by Cauchy filters. ⌟

Proof: □

Prop. (11.2.1.6) [Subgroups and Completion]. Let A be a topological Abelian group, then the completion $i : A \to A^\wedge$ induces a bijection between the set of open subgroups of A and the open subgroups of $A^\wedge$, given by $G \mapsto \overline{i(G)} = G^\wedge$. ⌟

Proof: Cf.[Mor19]P74. □

Def. (11.2.1.7) [Restricted Power Series]. Let R be a topological ring, then we can define the **restricted power series** over R to be

$$R\langle X_1, \ldots, X_n\rangle = \{\sum a_v X^v \in R[[X_1, \ldots, X_n]] | \lim_{v\to\infty} a_v \to 0\}$$

⌟

Adic Rings

Def. (11.2.1.8) [Adic Rings]. An **adic ring** R is a topological ring that the topology coincides with the $\mathfrak{a}$-adic topology for some ideal $\mathfrak{a} \in \mathrm{Ideal}(R)$, and any such $\mathfrak{a}$ is called a **ideal of definition**. ⌟

Prop. (11.2.1.9) [Topologically Nilpotent Elements]. Let A be an adic ring and $x \in A$, then the following are equivalent:

- x is topologically nilpotent.
- There exists an ideal of definition I that the image of x in A/I is nilpotent.

- There exists an ideal of definition I that $x \in I$.

In particular, the set A^{00} of nilpotent elements is an open radical ideal of A, and it is the union of all ideals of definitions in A. ⌟

Proof: $3 \to 1 \to 2$ is trivial. $2 \to 3$: if x is nilpotent in A/I, let $J = I + xA$, then J is an open ideal, and $J^n \in I$, so I-adic and J-adic topologies on A coincide, so J is an ideal of definition.

The rest is easy. □

Prop. (11.2.1.10)[Adic Localization]. If R is an adic ring with an ideal of definition $\mathfrak{a}$, the restricted power series $R\langle\xi\rangle$ is complete w.r.t. the $(\mathfrak{a})$-adic topology, and in fact

$$R\langle\xi\rangle \cong \varprojlim_n R/\mathfrak{a}^n[\xi].$$

For $f \in R$, we can define the **adic completion** of R at f to be the

$$R\langle f^{-1}\rangle = \varprojlim_n (R/\mathfrak{a}^n[\frac{1}{f}]).$$

The the natural map $R\langle\xi\rangle \to R\langle f^{-1}\rangle$ induces an isomorphism

$$R\langle\xi\rangle/(1 - f\xi) \cong R\langle f^{-1}\rangle.$$

⌟

Proof: There is an isomorphism $R[f^{-1}]/(\mathfrak{a}^n) \cong (R/\mathfrak{a}^n)[f^{-1}]$ because localization is flat, so we are done. □

Remark (11.2.1.11). There is another canonical morphism $R[f^{-1}] \to R\langle f^{-1}\rangle$ which exhibits $R\langle f^{-1}\rangle$ as the completion of $R[f^{-1}]$ w.r.t. the ideal $\mathfrak{a}R[f^{-1}]$.

Then $R\langle f^{-1}\rangle$ is endowed with an $\mathfrak{a}$-adic topology, and if $\mathfrak{a}$ is f.g., then $R\langle f^{-1}\rangle$ is complete w.r.t. to the $\mathfrak{a}R\langle f^{-1}\rangle$-adic topology. Also we see $R\langle f^{-1}\rangle$ doesn't depend on the choice of ideal of definition of $\mathfrak{a}$. ⌟

Proof: Consider the projective system of exact sequences:

$$0 \to (1 - f\xi)R/\mathfrak{a}^n[\xi] \to R/\mathfrak{a}^n[\xi] \to R/\mathfrak{a}^n[f^{-1}] \to 0.$$

which is a surjective system so by Mittag-Leffler(4.1.1.44), $\varprojlim$ is exact(5.9.3.2), and there is an exact sequence

$$0 \to \varprojlim_n (1 - f\xi)R[\xi] \to \varprojlim_n R[\xi] \to \varprojlim_n R[f^{-1}] \to 0.$$

Now $\varprojlim_n (1 - f\xi)R[\xi] \cong (1 - f\xi) \cong (1 - f\xi)R\langle\xi\rangle$, because $(1 - f\xi)$ is not a zero-divisor in $R/\mathfrak{a}^n$, and we get the desired isomorphism. □

Def. (11.2.1.12) [Completed Tensor Product]. Let $(A, \mathfrak{a}), (B, \mathfrak{b})$ be two complete adic rings, then we can define a **complete tensor product** ring $A\widehat{\otimes}B$ as

$$A\widehat{\otimes}B = \varprojlim_n (A/\mathfrak{a}^n \otimes B/\mathfrak{b}^n)$$

this is just the $(\mathfrak{a} \otimes B + A \otimes b)$-adic completion of the tensor product $A \otimes B$, because $(\mathfrak{a} \otimes B + A \otimes b)^n$ and $(\mathfrak{a}^n \otimes B + A \otimes \mathfrak{b}^n)$ are cofinal. ⌟

Properties of R-Algebras

Def. (11.2.1.13) [Topologically of Finite Presentation]. Let R be an adic ring with an ideal of definition I, then an R-algebra A is called

- **of topologically finite type** if it is isomorphic to an R-algebra $R\langle\zeta_1,\ldots,\zeta_n\rangle/\mathfrak{a}$ that is endowed with the I-adic topology and $\mathfrak{a}$ is an ideal of $R\langle\zeta_1,\ldots,\zeta_n\rangle$.
- **of topologically finite presentation** if moreover the ideal $\mathfrak{a}$ is f.g..
- **admissible** if it is of topologically finite presentation and has no I-torsion.

⌟

Prop. (11.2.1.14) [Raynaud–Gruson]. Let A be an R-algebra of topologically finite type and M a finite A-module that is flat over R. Then M is an A-module of finite presentation. ⌟

Proof: Cf.[Bos15]P165. □

Cor. (11.2.1.15). Let A be an R-algebra of topologically finite type, then if A has no I-torsion, then A is of topologically finite presentation, in particular admissible(11.2.1.13). ⌟

Proof: Cf.[Bos15]P166. □

Prop. (11.2.1.16) [Topologically of Finite Presentation is Local]. Let A be an R-algebra that is I-adically complete and separated, $f_1,\ldots,f_r$ be a set of elements generating the unit ideal, then A is of topologically finite type/topologically finite presentation/admissible iff each $A\langle f_i^{-1}\rangle$ does. ⌟

Proof: Cf.[Bos15]P169. □

2 Valuation Rings

Def. (11.2.2.1) [Valuation Ring]. A **valuation ring** is the maximum elements in the dominating ordering of local rings in a field K, where B **dominates** A iff $A\subset B$ and $\mathfrak{m}_B\cap A=\mathfrak{m}_A$.

A valuation ring in K is called **absolutely algebraically closed** if K is alg.closed. ⌟

Prop. (11.2.2.2) [Valuation is Maximal]. Any local ring A in a field K is dominated by a valuation ring with fractional field K. ⌟

Proof: Note that the dominating relation satisfies the condition of the Zorn's lemma, so it suffices to prove that A is not maximal if its fractional field is not K. Let $t\notin K_0=\mathrm{frac}A$. If t is transcendental over K_0, then $A[t]$ with the maximal ideal $(\mathfrak{m},t)$ dominate A. If t is algebraic over K_0, then there is a a that at is integral over A, hence by(5.2.1.5) there is a maximal ideal of $A[at]$ above A, which proves the lemma. □

Prop. (11.2.2.3) [Valuation Ring Criterion]. A is a valuation ring with field of fraction K iff for any $x\in K$, x or x^{-1} is in A. ⌟

Proof: If A is a valuation ring, then for $x\notin A$, we know that $A[x]$ is a local ring, hence there is no prime over $\mathfrak{m}$ otherwise $A[x]_{\mathfrak{p}}$ is a bigger local ring, so we see $\mathfrak{m}A[x]=A[x]$, i.e. $1=\sum t_ix^i$, so x^{-1} is integral over A. Now $A[x^{-1}]$ has a $\mathfrak{m}'$ over $\mathfrak{m}$, so $A=A[x^{-1}]_{\mathfrak{m}'}$, which shows $x^{-1}\in A$.

Conversely, if for any $x\in K$, x or x^{-1} is in A, we assume A is not K, so A is not field by the condition. Then it has a non-zero maximal ideal, but only one, otherwise we can choose x,y that $x/y,y/x\notin A$. And A is maximal because if there is a $A\subset A'$, and a $x\in A'$, then if $x\notin A$, then $x^{-1}\in A$, hence also in $\mathfrak{m}_A$, so it is in $\mathfrak{m}_{A'}$, but now x^{-1} cannot be in A', contradiction. □

Cor. (11.2.2.4). For $K \subset L$ subfield, if A is a valuation ring of L, then $A \cap K$ is a valuation ring of K. And if L/K is algebraic and A is not a field, then $A \cap K$ is not a field.(This is because the primes of A are all over 0 so cannot contain each other(5.2.1.5) so A is a field). ⌟

Cor. (11.2.2.5). The quotient A/p at a prime is a valuation ring, and any localization of valuation ring is a valuation ring, by this criterion. ⌟

Prop. (11.2.2.6)[Valuation Ring is Normal]. Valuation ring is normal, because for x algebraic over A, either $x \in A$, or x is a combination of x^{-1} thus in A, by(11.2.2.3). ⌟

Cor. (11.2.2.7)[Integral Closure and Valuation Ring]. The integral closure of a subring in a field K is the intersection of valuation rings containing A. ⌟

Proof: Valuation ring is integrally closed, so it suffices to prove if x is not algebraic over A, then there is a valuation ring of A not containing x. This is because $x \notin B = A[x^{-1}]$ otherwise x is integral over A. Now x^{-1} is not a unit in B, hence $x \in p \in B$, hence B_p is dominated by some valuation ring V, and $x \notin V$ because $x^{-1} \in \mathfrak{m}_V$. □

Prop. (11.2.2.8)[Bezout Domain and Valuation Ring]. A valuation ring is equivalent to a Bezout local domain. ⌟

Proof: One way is because the element of minimum valuation generate the ideal. Conversely, for $f, g \in A$, $(f, g) = (h)$, so $f = ah, g = bh$, and $h = cf + dg$, then $ab + cd = 1$, hence a or b is a unit, so $f/g \in A$ or $g/f \in A$. By(11.2.2.3), A is a valuation ring. □

Prop. (11.2.2.9). A valuation ring is Noetherian iff it is discrete valuation iff it is PID. ⌟

Proof: Only need to prove Noetherian then $\Gamma = \mathbb{Z}$. we know ideals of Γ of the form $\{x|x \geq \gamma\}$, where $\gamma > 0$ has a maximal element, so there is a minimal element bigger than 0, so $\Gamma \cong \mathbb{Z}$. □

Prop. (11.2.2.10). In a fixed field, any inclusion relation of two valuation ring is given by localization. ⌟

Proof: Just localize at the image of the maximal ideal $\mathfrak{m}_B \cap A$, then they are valuation rings(11.2.2.5) that dominate each other, thus they are the same by definition(11.2.2.1). □

Def. (11.2.2.11) [Extension of Valuation Rings]. An injective local homomorphism of valuation rings is called an **extension of valuation rings**. By(5.4.1.29), it is equivalent to a f.f. morphism of valuation rings. ⌟

3 Valuations

Def. (11.2.3.1) [Valuations]. For $K \in$ `Field`, a **valuation** on K is a surjective homomorphism of rings $v : K \to \Gamma$ where Γ is an ordered Abelian group(3.2.9.1), called the **value group** of v.

The **rank of a valuation** is defined as the height of its value group(3.2.9.4). ⌟

Prop. (11.2.3.2)[Valuation Ring and Valuation]. Valuation rings(11.2.2.1) A of a field K is equivalent to valuations on K(11.2.3.1).

The equivalence is given by $K = Q(A)$, $\Gamma = K^*/A^*$ and that $A = v^{-1}(\{x \geq 0\})$. ⌟

Proof: These are definitely valuation rings, and if A is a valuation ring by(11.2.2.3), then we set $\Gamma = K^*/A^*$, where A^* is the invertible elements of A and $x \leq y$ iff $y/x \in (A - \{0\})/A^*$. This is totally ordered by(11.2.2.3). □

Cor. (11.2.3.3) [Rank and Dimension]. A valuation ring of rank n has Krull dimension n, because clearly the convex subgroups of Γ is in bijection with ideals of A. ⌟

Prop. (11.2.3.4) [DVRs]. For a Noetherian local domain A of dimension 1 with maximal ideal $\mathfrak{m}$ and residue field k that is not a field, the following are equivalent:

1. A is a valuation ring corresponding to a discrete valuation in(11.2.3.2).
2. A is normal.
3. $\mathfrak{m}$ is a principal ideal.
4. A is regular.
5. Every nonzero ideal is a power of $\mathfrak{m}$.
6. There exists a $x \in A$ that every nonzero ideal is of the form (x^k).

Such a ring is called a **discrete valuation ring** or a DVR. ⌟

Proof: $1 \to 2$: Valuation ring is integrally closed, by(11.2.2.6).

$2 \to 3$: As the radical of any non-trivial ideal (a) is $\mathfrak{m}$, and A is Noetherian, so there is an n that $\mathfrak{m}^n \subset a$ and $\mathfrak{m}^{n-1} \not\subset a$. Then choose $b \in a - \mathfrak{m}^{n-1}$, $x = a/b \in K$, then $x^{-1} \notin A$, then it is not integral over A. So $x^{-1}\mathfrak{m} \not\subset \mathfrak{m}$, but $x^{-1}\mathfrak{m} \subset A$, so it equals A, which means $\mathfrak{m} = (x)$.

$3 \to 4$: Clear.

$4 \to 5$: For any ideal a, its radical is $\mathfrak{m}$ and A is Noetherian, so $\mathfrak{m}^n \subset a$. Now $A/\mathfrak{m}^n$ is Artinian by(5.1.3.4), so by(5.1.3.6) a is a power of $\mathfrak{m}$.

$5 \to 6$: And $x \in \mathfrak{m} - \mathfrak{m}^2$ will do.

$6 \to 1$: Define $v(a) = k$ if $(a) = (x^k)$. □

Cor. (11.2.3.5) [Noetherian Valuation Rings are DVRs]. A Noetherian valuation rings are automatically DVRs. ⌟

Proof: This is implicit in the proof above. □

Prop. (11.2.3.6). Let R be a Noetherian local domain with fraction field K and $R \neq K$, then there exists a Noetherian local ring R' of dimension 1 that dominates R s.t. $R \to R'$ is essentially of f.t.. ⌟

Proof: Cf.[Sta]00P8. □

Cor. (11.2.3.7) [Dominance by DVRs]. Let R be a Noetherian local domain with fraction field K and $R \neq K$, L/K a f.g. filed extension, then there exists a a DVR A with fraction field L which dominants R. ⌟

Proof: First we can reduce to the case L/K is finite: If it is not finite, choose a transcendence basis $x_1, \ldots, x_r$, and replace R by $R[x_1, \ldots, x_r]_{\mathfrak{m}_R, x_1, \ldots, x_r}$.

In the finite case, first we can reduce to the case $\dim R = 1$ by(11.2.3.6), and let A be the integral closure of R in L, then by(5.1.1.51), A is Noetherian, and $R \to A$ is integral so there exists a maximal prime $\mathfrak{n} \subset A$ that $\mathfrak{n} \cap R = \mathfrak{m}_R$. Thus $A_{\mathfrak{n}}$ is a DVR by(11.2.3.5). □

Valuations of Rank 1

In this subsubsection, all valuations are of rank 1.

Remark (11.2.3.8) [Real Valuations]. As an ordered Abelian group of height 1 can be embedded into $\mathbb{R}$(3.2.9.5), a valuation v on a field of rank 1 is equivalent to a real-valued valuation. ⌟

Def. (11.2.3.9) [Multiplicative Valuation]. For a real continuous valuation v, we can define a **multiplicative valuation** $|\cdot|$ where $|a| = \exp(-v(a))$. Then it is multiplicative. ⌟

Def. (11.2.3.10) [non-Archimedean Valuations]. A valuation is called **non-Archimedean** iff $|x + y| \le \max\{|x|, |y|\}$ for any x, y. It is called **Archimedean** iff it is not non-Archimedean . ⌟

Def. (11.2.3.11) [Non-Archimedean field]. A **non-Archimedean field** is a topological field that the valuation is given by a rank1-valuation. ⌟

Prop. (11.2.3.12). A valuation is non-Archimedean iff $\{|n| | n \in \mathbb{N}\}$ is bounded. ⌟

Proof: If it is non-archimedean, then clearly by induction and $n = 1 + (n-1)$ $|n| \le 1$. Conversely, if $|n| \le M$, then consider $|x + y|^n = |(x + y)^n| \le \sum |C_n^k| x^k y^{n-k}| \le M \max\{|x|, |y|\}$, so letting n be large, clearly $|x + y| \le \max\{|x|, |y|\}$. □

Cor. (11.2.3.13). Any valuation on a field of char$\neq 0$ is non-Archimedean. ⌟

Prop. (11.2.3.14) [Equivalent Valuations]. Two valuation on a field is equivalent iff $|x|_1 < 1 \Rightarrow |x|_2 < 1$ and is equivalent to $|x|_1 = |x|_2^s$ for some $s > 0$.

⌟

Proof: if two valuation are equivalent, then $x^n \to 0$ in τ_1 iff $x^n \to 0$ in τ_2, so $|x|_1 < 1 \Rightarrow |x|_2 < 1$.

If $|x|_1 < 1 \Rightarrow |x|_2 < 1$, then let y be an element that $|y|_1 > 1$, then any element $|x| = |y|^\alpha$ for some $\alpha \in \mathbb{R}$. Let $\frac{n_i}{m_i}$ converges to α from above, then $|\frac{x^{n_i}}{y^{m_i}}|_1 < 1$, so $|\frac{x^{n_i}}{y^{m_i}}|_2 < 1$, so $|x|_2 \le |y|_2^\alpha$. Similarly, $|x|_2 \ge |y|_2^\alpha$, so $|x|_2 = |y|_2^\alpha$. So $|x|_1 = |x|_2^s$ for some $s > 0$.

If $|x|_1 = |x|_2^s$ for some $s > 0$, then these two valuations are clearly equivalent. □

Cor. (11.2.3.15) [Weak Approximation]. If $|\cdot|_1, \ldots, |\cdot|_n$ be pairwise inequivalent valuations on K, then for any $a_1, \ldots, a_n \in K$ and $\varepsilon > 0$, there is an $x \in K$ that $|x - a_i|_i < \varepsilon$. ⌟

Proof: As $|\cdots|_1, |\cdots|_n$ are inequivalent, there are α, β that $|\alpha|_1 < 1, |\alpha|_n \ge 1$, $|\beta|_n < 1, |\beta|_1 \ge 1$ by(11.2.3.14), so let $y = \beta/\alpha$, then $|y|_1 > 1$, $|y|_n < 1$.

Now we prove by induction that there is an α that $|\alpha|_1 > 1, |\alpha|_i < 1$ for $i = 2, \ldots, n$. the case $n = 2$ is done, for general n, if the z for $n - 1$ satisfies $|z|_n \le 1$, then $z^m y$ will do, for m large. if $|z| > 1$, then the sequence $|t_m|_i = |\frac{z^m}{1+z^m}|_i$ converges to 1 for $i = 1, n$ and converges to 0 for $i = 2, \ldots, n-1$, so $t^m y$ will do, for m large. □

Prop. (11.2.3.16) [Gelfand]. Any field K with an Archimedean valuation is a subfield of $\mathbb{C}$. ⌟

Proof: We consider its completion. when it contains $\mathbb{C}$, this is a corollary of**??**, otherwise, we consider $K \otimes \mathbb{C}$, then it is a finite dimensional module over K thus also complete. □

Remark (11.2.3.17). Because of this, we usually don't consider only non-Archimedean valuations, and refer to all valuations as **places**, cf.(14.4.1.5). ⌟

Prop. (11.2.3.18) [Ostrowski].

1. $\Sigma_{\mathbb{Q}} = \mathbf{P} \cup \{\infty\}$. Thus any complete Archimedean field is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ by(11.2.3.16).
2. Any non-trivial valuation on $\mathbb{F}_q(t)$ is of the form $|\cdot|_p$ or $|\cdot|_\infty$, where p is an irreducible polynomial in $\mathbb{F}_q[t]$.

⌟

Proof: 1: if it is non-Archimedean, then $|n| \leq 1$, and it is not trivial, so there is a minimal p that $|p| < 1$. Then p is easily seen to be a prime. Then for any $(a, p) = 1$, $a = dp + r$, so $|r| = 1$, so $|a| = 1$.

And if it is Archimedean, then we prove that in $\mathbb{N}$, $|m| = m^\lambda$ for some λ: Let $F(n) = |n|$ and $f = \log_2 F$, then $f(m+n) \leq \max\{f(m), f(n)\}+1$, and if $m = \sum_{i=1}^r d_i n^i$, then $f(m) \leq r(1+f(n))+a_n$, where $a_n = \sup\{f(k)|k < n\}$. And $r \leq \log m/\log n$, so

$$\frac{f(m)}{\log m} \leq \frac{a + f(n)}{\log n} + \frac{b}{\log n}$$

then letting $m \to m^k, k \to \infty$, and then let $n \to n^k, k \to \infty$, we get $\frac{f(m)}{\log m} \leq \frac{f(n)}{\log n}$, for any m, n.

2: Any valuation on $\mathbb{F}_q(t)$ is non-Archimedean(11.2.3.13), and $|n| = 1$ if $(n, p) = 1$, because $n^{p-1} = 1$. Similarly, if there is a minimal hence irreducible P that $|P| < 1$, then use induction and $Q = sP + r$ for some s, r of degree$<\deg Q$, so $|Q| = 1$ for all $(Q, P) = 1$. Otherwise, $|P| \leq 1$ for all P, then $|t| > 1$, otherwise $|\cdot|$ is trivial, so it is easy by induction that $|F(t)| = |t|^{\deg F}$. □

Lemma (11.2.3.19) [Continuity of Roots]. For a separable polynomial f over a valued alg.closed field $\overline{K}$, there is a ε that every polynomial g that are closed enough to f, the roots of g is closed to roots of f respectively. ⌟

Proof: This is easy to see by decomposition as each root of f is close to a root of g. f, g have the same degree so the roots correspond to each other. □

Prop. (11.2.3.20) [Fundamental Inequality]. if (K, v) is a valued field and L/K be a field extension of degree n, if w_i are the valuations of L above v, then

$$\sum_{w_i|v} e(w_i/v)f(w_i/v) \leq [L : K].$$

The equality holds when v is discrete and L/K is separable. ⌟

Proof: Cf.[Clark note Theorem4].**?** □

Def. (11.2.3.21) [Spherically Complete Valued Field]. A valued field K is called **spherically complete** iff each descending chain of metric balls has a nonempty intersection. ⌟

Microbial Valuations

Prop. (11.2.3.22) [Microbial Valuation]. For a valuation ring $R \subset K$, a $f \neq 0 \in R$ is called **topologically nilpotent** iff $f^n \to 0$ in the valuation topology of A. The following are equivalent:

- The topology on K coincides with a rank 1 topology.
- There exists a nonzero topologically nilpotent element in K.
- R has a prime ideal of height 1.

If this is the case, then the valuation defined by A is called **microbial**.

And in this case, for any topological nilpotent element ϖ, $K = R[\varpi^{-1}]$, and $\varpi^r \in R$ for some r, and the topology on R is ϖ^r-adic. And if $\mathfrak{p}$ is a prime ideal of rank 1, then the valuation ring $R_\mathfrak{p}$ is of rank 1, and defines the same topology on R. ⌟

Proof: $1\to 2$: if there is a rank 1 valuation $|-|'$ that defines the same topology as R, then any $|x|'<1$ will be a topological nilpotent element by(11.2.3.23).

$2\to 3$: if ϖ is a topological nilpotent element, then $\mathfrak{p}=\sqrt{(\varpi)}$ is a prime ideal, and it is minimal, because if there is another $\mathfrak{q}\subsetneq\mathfrak{p}$, then $\varpi\notin\mathfrak{q}$, but $\mathfrak{p}\subset(\varpi^n)$ by induction: because $(\varpi)\nsubseteq\mathfrak{q}$, $\mathfrak{q}\subset(\varpi)$, and if $x\in\mathfrak{q}$, then $x=\varpi^n y$, and $\varpi\notin\mathfrak{q}$, so $y\in\mathfrak{q}\subset(\varpi^n)$, so $x\in(\varpi^{n+1})$. Now $\mathfrak{q}=0$ because ϖ is topological nilpotent.

$3\to 1$: It suffices to prove that the valuation defined by $R_{\mathfrak{p}}$ is the same as the topology of R. But this is true in general, just notice that the valuation topology of a nontrivial valuation is also defined by $B(a,\gamma]$.

The final remark is clear as $x\varpi^n\in R\iff|\varpi^n|\leq|x^{-1}|$. □

Lemma (11.2.3.23). Let R be a valuation ring, if $x\in R^*$ is topologically nilpotent, then $|x|<1$, and the converse is also true if R has rank 1. ⌟

Proof: if $|x|\geq 1$, then $x^{\mathbb{N}}\notin B(0,1)$, so it is not topologically nilpotent. And if R has rank 1, $|x|<1$, then for any $\delta\neq 0$, there is some n that $|\delta^{-1}|<|x^{-n}|$(3.2.9.5), so $|x^m|<|\delta|$ for m large, thus x is topologically nilpotent. □

Prop. (11.2.3.24) [Constructing Microbial Valuations]. If A is a valuation ring and $f\in A$ is a non-zero non-unit, then the f-adic Hausdorffization $\overline{A}=A/\cap_n(f^n)$ and the completion $\widehat{A}$ are all microbial. ⌟

Proof: Easy, Cf.[Bhatt Perfectoid Spaces, P63]. □

4 Affinoid Algebras

Tate Algebras

Def. (11.2.4.1) [Tate Algebra]. For a complete non-Archimedean field K with residue field k, we define the **Tate algebra** $T_n=K\langle x_1,\ldots,x_n\rangle$ to be the restricted power series(11.2.1.7) consists of elements $\sum_v a_v x^v$ that $\varinjlim_{|v|\to\infty}|a_v|=0$. It is endowed with the norm $|f|=\max|a_v|$.

The norm satisfies $|fg|=|f||g|$ and $|f+g|\leq|f|+|g|$.

There is a **reduction map** from T_n to $k[x_1,\ldots,x_n]$, it is surjective. ⌟

Proof: T_n is an algebra because the values of coefficients of f is bounded. $|fg|\leq|f||g|$ is easy, to show $|fg|\geq|f||g|$, we assume $|f|=|g|=1$, then their reduction in $K[x_1,\ldots,x_n]$ is non-zero, thus $\overline{fg}$ is non-zero, which shows $|fg|\geq 1$. □

Prop. (11.2.4.2) [Maximum Principle]. A formal power series f converges in $B^n(\overline{K})$ iff it is in T_n. And when it is in T_n, $|f(x)|$ attains a maximum$=|f|$ in $B^n(\overline{K})$. ⌟

Proof: If it converges at $(1,\ldots,1)$, then $\varinjlim_{|v|\to\infty}|a_v|=0$ by(14.2.1.19). Conversely, for any point in $B^n(\overline{K})$, it can be considered in a finite extension field of K, thus complete, hence we can apply(14.2.1.19) again.

For the second assertion, we assume $|f|=1$, then consider its reduction to $k[x_1,\ldots,x_n]$, then there is a $\overline{x}$ in the alg.closure of k that $\overline{f}(\overline{x})\neq 0$. Now $\overline{k}$ can be seen as the residue field of $\overline{K}$. Then the lifting of $\overline{x}$ to a $x\in\overline{K}$ has valuation 1 and $|f(x)|=1$. □

Prop. (11.2.4.3). T_n is a Banach algebra(Easy). ⌟

Cor. (11.2.4.4). An element f of norm 1 of T_n is invertible in T_n iff its reduction in $k[x_1, \ldots, x_n]$ is a unit. Elements of other norms can be reduced to the case of norm 1. ⌟

Proof: One direction is trivial, the other is because $|f - f(0)| < 1$, hence $f = f(0)(1 + g)$, this is invertible by power expansion as T_n is complete. □

Def. (11.2.4.5). A restricted power series $g = \sum g_v X_n^v \in T_n$ with coefficients in T_{n-1} is called **X_n-distinguished of order** s iff g_s is a unit in T_{n-1}, $|g_s| = |g|$ and $|g_s| > |g_v|$ for all $v > s$. ⌟

Lemma (11.2.4.6). For any f.m. elements $f_i \in T_n$, there is a continuous automorphism of T_n that maps $T_n \to T_n, T_i \to T_i + T_n^{\alpha_i}$ that maps f_i to X_n-distinguished elements. ⌟

Proof: Cf.[Rigid and Formal Geometry P16]. □

Prop. (11.2.4.7) [Weierstrass Division]. If $g \in T_n$ is X_n-distinguished of order s, for any $f \in T_n$, there is a unique form $f = qg + r$, where $q \in T_n$ and $r \in T_{n-1}[X_n]$ of degree $r < s$. Moreover, $|f| = \max\{|q||g|, |r|\}$. ⌟

Proof: Cf.[Rigid and Formal Geometry P17]. □

Cor. (11.2.4.8)[Weierstrass Preparation]. If $g \in T_n$ is X_n-distinguished of order s, then there exists uniquely a $r \in T_{n-1}[X_n]$ of degree s and $g = re$, where e is a unit in T_n. ⌟

Proof: By(11.2.4.7) applied to $X_n^s = qg + r$ with $|r| \leq 1$. Then $\omega = X_n^s - r$ is X_n is the desired polynomial, it suffice to show q is a unit. Let g be normalized that $|g| = 1$, then $|q| = 1$, by reduction to polynomials, we see $\widetilde{\omega} = \widetilde{q}\widetilde{g}$, and $\widetilde{\omega}, \widetilde{g}$ are both polynomials of degree s, so $\widetilde{q} \in k^*$, so q is a unit by(11.2.4.4).

Uniqueness: if $g = e\omega$, then $X_n^s = e^{-1}g + (X_n^s - \omega)$, so uniqueness follows from that of Weierstrass division. □

Prop. (11.2.4.9) [Noether Normalization]. For any proper ideal $\mathfrak{a}$ of T_n, There is a d and a finite injection $T_d \to T_n/\mathfrak{a}$. ⌟

Proof: We may assume $\alpha \neq 0$, thus choose a $g \in \alpha \neq 0$, then using(11.2.4.6), we may assume g is X_n-distinguished. Now the Weierstrass division theorem(11.2.4.7) says that $T_{n-1} \to T_n/(g)$ is finite. Hense $T_{n-1} \to T_n/(g) \to T_n/\mathfrak{a}$ is finite. Now we can use induction to find a $T_d \to T_{n-1}/T_{n-1} \cap \mathfrak{a}$ finite, thus also $T_d \to T_n/\mathfrak{a}$ is finite. □

Cor. (11.2.4.10) [Residue Field of Tate Algebra]. The residue field of a maximal ideal of T_n is a finite extension field of K, because $T_n/\mathfrak{m}$ has dimension 0, thus $K \to T_n/\mathfrak{m}$ finite injective. ⌟

Proof: Because finite injection $T_d \to T_n/\mathfrak{m}$ shows T_n is a field(5.2.1.3), thus we must have $d = 0$. □

Cor. (11.2.4.11). The map from $B^n(\overline{K})$ to the set of maximal ideals of T_n are surjective. ⌟

Proof: Evaluation map defines a map $T_n \to K(x_1, \ldots, x_n)$ that is surjective, thus the kernel is a maximal ideal. Conversely, for any maximal ideal $\mathfrak{m} \subset T_n$, $K' = T_n/\mathfrak{m}$ is finite over K, so we may assume $K' \subset \overline{K}$.

We show that this map $\varphi : T_n \to \overline{K}$ is contractive, otherwise there is a $|a| = 1, |\alpha = \varphi(a)| > 1$. Consider the minimal polynomial p of $|\alpha|$, all the conjugates of α has the same valuation as K, as K is Henselian, thus p has ascending Newton polygon, thus by(11.2.4.4) it is invertible in T_n. But $\varphi(p(a)) = 0$, contradiction.

So $|\varphi(x)| \leq |x|$, then it is continuous, and $(\varphi(T_1), \ldots, \varphi(T_n)) \subset B^n(K^n)$, so we are done. □

Cor. (11.2.4.12) [Main Theorem]. T_n is Noetherian, UFD, Jacobson of Krull dimension n. ⌟

Proof: Noetherian: Use induction, as in the proof of(11.2.4.9), $T_{n-1} \to T_n/(g)$ is finite for some $g \subset \mathfrak{a}$, then also $T_n/\mathfrak{a}$ is finite over T_{n-1}, thus Noetherian as a T_{n-1} module, thus Noetherian as a ring.

UFD: Cf.[Rigid and Formal Geometry P20].

Jacobson: We need to show that any prime ideal $\mathfrak{p}$ is an intersection of maximal ideals. The case of $\mathfrak{p}$ is by(11.2.4.2). For $\mathfrak{p} \neq 0$, by Noetherian normalization(11.2.4.9), there is a $T_d \subset T_n/\mathfrak{p}$ finite. Then use induction and generalized Nullstellensatz(5.2.6.10), $T_n/\mathfrak{p}$ is Jacobson, thus $\mathfrak{p} = \mathrm{rad}(T_n/\mathfrak{p})$.

Dimension n: Cf.[Formal and Rigid Geometry P22]. □

Prop. (11.2.4.13). For an ideal $\mathfrak{a} \in T_n$, there are $a_1, \ldots, a_r$ which generate $\mathfrak{a}$ that $|a_i| = 1$, and any elements in f has a representation of the form $\sum f_i a_i$ with $|f_i| \leq |f|$.

The same assertion holds for submodules of T_n^k. ⌟

Proof: Cf.[Formal and Rigid Geometry P27,29].? □

Cor. (11.2.4.14). Each ideal of T_n is closed hence complete in T_n. This follows immediately from(11.2.4.12) and(14.2.4.13). ⌟

Cor. (11.2.4.15). For any ideal $\mathfrak{a}$ of T_n, the distance from an element to $\mathfrak{a}$ attains minimum. ⌟

Proof: Cf.[Bos15] P28. □

Affinoid Algebras

Def. (11.2.4.16) [Affinoid Tate Algebra]. A normed algebras of the form $A = T_n/\mathfrak{a}$ are called **affinoid (Tate) algebras**, so it is Noetherian and Jacobson by(11.2.4.12). An affinoid algebra has a natural semi-norm by $|f|_{\sup} = \sup |f|_{\mathfrak{m}}$ in $A/\mathfrak{m}$ for a maximal ideal $\mathfrak{m}$ of A by(11.2.4.10). ⌟

Proof: We need to show the sup is finite, for this, notice $|f| = |g|$ for some g in the residue norm(11.2.4.17), so for any maximal ideal $\mathfrak{m}$ of A, the inverse is a maximal ideal $\mathfrak{n}$ in T_n by finiteness, thus $|f|_{\mathfrak{m}} = |g|_{\mathfrak{n}} \leq |g|_{\sup} = |g| = |f|$, so $|f|_{\sup} \leq |f|$.

For the second-last equality, notice on T_n, $|\cdot|_{\sup}$ and $|\cdot|$ equal, by(11.2.4.2) and(11.2.4.11). □

Def. (11.2.4.17) [Residue Norm]. For a Tate algebra $A = T_n/\mathfrak{a}$, there is a natural residue norm on it. This is a complete K-algebra norm on A, and $T_n \to A$ is continuous and open. For any $f \in A$, the residue norm is attained at an element of T_n.

Any residue norm is bigger than the sup-norm, by the proof of(11.2.4.16). ⌟

Proof: It is a K-algebra norm is easily verified, should notice $|f| = 0$ iff $f = 0$, because $\mathfrak{a}$ is closed(11.2.4.14). The last assertion follows from(11.2.4.15). □

Remark (11.2.4.18). The sup norm may not even be a norm, if $\mathfrak{a}$ is not radical, but the fact that sup norm is smaller than any residue norm, together with(11.2.4.22), is enough for use. ⌟

Prop. (11.2.4.19). For $T_d \to A$ a finite injection, assume A is a torsion-free T_d-module, then for any $f \in A$, there is a unique minimal monic polynomial P of f over T_d.

In this case, $|f|_{\sup} = \sup |a_i|_{\sup}^{1/i}$ where a_i are coefficients of P. ⌟

Proof: Because A is torsion-free, we reduce to the quotient field of T_n, then f has a minimal monic polynomial, and T_n is UFD, hence Gauss lemma shows that this polynomial has coefficients in T_d. Hence $T_n[f] = T_n[X]/(p)$.

For the second, notice first for finite extension the Spec map is surjective, thus we may assume $A = T_n[f] = T_n[X]/(p)$, and for a maximal ideal $\mathfrak{m}$ of T_n, let $T_n/\mathfrak{m} = k$, then $A/(\mathfrak{m}) = k[X]/(\overline{p})$, then maximal ideals of $A/(\mathfrak{m})$ corresponds to roots α_i of $\overline{p}$ in $\overline{k}$, so

$$\sup_{\varphi^{-1}(\mathfrak{n})=\mathfrak{m}} |f|_{\mathfrak{n}} = \sup |\alpha_i| = \max |a_i|_{\mathfrak{m}}^{1/i},$$

so the result follows. □

Cor. (11.2.4.20). $|f|_{\sup} \in \sqrt[N]{|K|}$ for some N and all $f \in A$, because the minimal polynomial has coefficients in T_n, and sup norm and Gauss norm coincide on T_n by the proof of(11.2.4.16). ⌟

Cor. (11.2.4.21) [Maximum Principle]. $|f|_{\sup} = |f|_{\mathfrak{m}}$ for some maximal ideal $\mathfrak{m}$. ⌟

Proof: Since A is Noetherian(11.2.4.12), it has f.m. minimal primes, hence $|f|_{\sup} = |f|_{\sup}$ in A/p_i for some minimal prime of A. Hence we reduce to the case of(11.2.4.19), hence the conclusion follows from(11.2.4.2) and the proof of(11.2.4.19). □

Prop. (11.2.4.22) [Residue Norms Equivalent]. Any morphism from a Noetherian k-algebra to an affinoid algebras A is continuous w.r.t any residue norms. In particular, any k-Banach algebra topology on A coincides with the k-affinoid topology on A, and all residue norms on an affinoid algebra are equivalent.

Moreover, for any morphism of k-affinoid algebras $B \to A$, the norm on A can be replaced by an equivalent one that makes A into a normed B-algebra. ⌟

Proof: Use(14.2.4.10), it suffices to show the condition holds, for $\mathfrak{B} = \{\mathfrak{m}^v\}$ where $\mathfrak{m}$ are maximal ideals of A: The residue field is finite by(11.2.4.10), their intersections is (0) because if $f \in \cap_{\mathfrak{m}} \cap_n \mathfrak{m}^n$, Krull's theorem(5.2.2.15)(use localization) says for each maximal ideal $\mathfrak{m}$ there is a $m \in \mathfrak{m}$ that $(1-m)f = 0$, so $Ann(f) = (1)$, so $f = 0$.

For the second assertion, see [non-Archimedean Analysis P229]. □

Cor. (11.2.4.23). The notion of power-boundedness and topological nilpotence is independent of residue norm chosen. ⌟

Cor. (11.2.4.24) [Restricted Power Series]. For an affinoid algebra A, the restricted power series in A:

$$A\langle X_i\rangle = \{\sum a_v X^v | \varinjlim_{|v|\to\infty} a_v = 0\}$$

is an affinoid algebra, this is independent of the residue norm chosen. ⌟

Def. (11.2.4.25) [Strongly Noetherian]. A is called **strongly Noetherian** if $A\langle T_1, \ldots, T_n\rangle$ are Noetherian for any $n \geq 0$. ⌟

Lemma (11.2.4.26). The image A is dense in $A\langle X\rangle/(X-f)$(in the residue norm, and thus in all other norms, by(11.2.4.22)(11.2.4.17)), this is because a restricted power series can be truncated by a finite part and a part with small norm, and the finite part is in the image of A. ⌟

Def. (11.2.4.27) [Affinoid Generator]. For a morphism of affinoid algebras $A \to A'$, a set of elements h_i in A' is called a set of **affinoid generator** iff there is a surjection

$$A\langle X_1, \ldots, X_n\rangle \to A', \quad X_i \mapsto h_i$$

Of course h_i is power-bounded, by the residue norm given. ⌟

Lemma (11.2.4.28). If $\pi' : A\langle X_1, \ldots, X_n\rangle \to A' : X_i \to h'_i$ is a surjective morphism of affinoid algebras that $A\langle X_1, \ldots, X_n\rangle$ is endowed with the Gauss norm and A' is endowed with the residue norm, then any set of elements $h = (h_1, \ldots, h_n)$ that $|h_i - h'_i| < 1$ is a set of affinoid generators. ⌟

Proof: By non-Archimedean property, $|h_i| \leq 1$ thus also $|h'_i| \leq 1$, and Let $\varepsilon = \max\{|h_i - h|\} < 1$. The strategy is simple, if for each g in A', we can find a f that $|f| = |g|, |\pi(f) - g| \leq \varepsilon|g|$, then by iteration, there is a f that $\pi(f) = g$. But by(11.2.4.17) and(11.2.4.15), if we choose a f that $\pi'(f) = g$ and $|f| = |g|$, then

$$|\pi(f) - g| = |\sum a_v h^v - \sum a_v h'^v| = |\sum a_v (h^v - h'^v)| \leq \varepsilon|f| = \varepsilon|g|.$$

□

Def. (11.2.4.29) [Distinguished Element]. For an affinoid algebra A and an element $x \in \operatorname{Sp} A$(17.5.1.1), a element $f \in A\langle X_1, \ldots, X_n\rangle$ is called X_n**-distinguished of order** s **at** x iff it is distinguished in $A/\mathfrak{m}_x\langle X_1, \ldots, X_n\rangle$ is distinguished of order s in the sense of(11.2.4.5)(notice $A/\mathfrak{m}_x$ is a complete valued field by(11.2.4.10)). ⌟

Prop. (11.2.4.30) [Fibererd-Pushouts]. When R, A_1, A_2 are all affinoid algebras, the amalgamated sum is also an affinoid algebra. In other words, the category of affinoid algebras admits amalgamated sums(fibered pushouts by(14.2.1.15)). ⌟

Proof: Cf.[Formal and Rigid Geometry P245]. □

Prop. (11.2.4.31). $T_n \widehat{\otimes} T_m \cong T_{m+n}$. $K' \widehat{\otimes} T_{n,K} = T_{n,K'}$. ⌟

Prop. (11.2.4.32). For affinoid algebras R, A_1, A_2 and ideals $\mathfrak{a}_1 \subset A_1, \mathfrak{a}_2 \subset A_2$, there is an isomorphism:

$$(A_1 \widehat{\otimes}_R A_2)/(\mathfrak{a}_1, \mathfrak{a}_2) \cong (A_1/\mathfrak{a}_1) \widehat{\otimes}_R (A_2/\mathfrak{a}_2)$$

⌟

Proof: Cf.[Rigid and Formal Geometry P248]. □

Prop. (11.2.4.33) [Finite Extension of Affinoid Algebras]. If B is an affinoid K-algebra and $\varphi : B \to A$ is a finite ring map, then A can be provided a topology to make it an affinoid K-algebra, and φ is continuous. ⌟

Proof: We can associate to A a Banach algebra topology induced from $B^n \to A \to 0$ that is continuous. Now it is an affinoid K-algebra: we may assume $B = T_n$, then $A = \sum T_n a_i$, and we may assume $|a_i| < 1$ then clearly there is a continuous extension $T_n\langle X_i\rangle \to A$ extending this map, so A is affinoid. □

Construction of Affinoid Tate Algebras

Def. (11.2.4.34) [Affinoid Localizations]. Let A be an affinoid Tate algebra, then for a finite set of elements $\{f_i, g_j\} \subset A$, we can define the localization

$$A\langle f_i, g_j^{-1}\rangle = A\langle \zeta_1, \ldots, \zeta_i, \xi_1^{-1}, \ldots, \xi_j\rangle/(\zeta_i - f_i, 1 - \xi_j g_j).$$

⌟

5 Huber Rings

Def. (11.2.5.1) [Huber Ring]. A **Huber ring** is a topological ring A s.t. there is an open subring $A_0 \subset A \in \mathcal{R}\mathrm{ing}$ that the induced topology on A_0 is I-adic for some f.g. ideal $I \in \mathrm{Ideal}(A)$. Such an A_0 is called a **ring of definition** of A, and I is called the **ideal of definition** of A. The category $\mathcal{H}\mathrm{ub}\,\mathcal{R}\mathrm{ing}$ is defined to be the subcategory of topological rings consisting of Huber rings. ⌟

Prop. (11.2.5.2) [Boundedness and Rings of Definition]. A subring $A_0 \subset A$ of a Huber ring is a ring of definition iff it is open and bounded. ⌟

Proof: Clearly a ring of definition is open and bounded, for the converse, let (A_0', I) be a couple of definition, and A_0 is an open and bounded subset of A, then $I^k \subset A_0$ for some n, and set $J = I^k A_0$. As A_0 is bounded, for any open nbhd U of 0, there exists $m > 0$ that $I^{km} A_0 \subset U$, thus $J^m \subset U$. This shows J is a fundamental system of nbhd of 0, thus A_0 is J-adic and is a ring of definition. □

Cor. (11.2.5.3). For $A \in \mathcal{H}\mathrm{ub}\,\mathcal{R}\mathrm{ing}$.

- If A_0, A_1 are two rings of definition of A, then so does $A_0 \cap A_1$ and $A_0 A_1$.
- Every open subring B of A is a Huber ring.
- If $B \subset C$ are subrings of A and B is bounded, C is open, then there is a ring of definition A_0 that $B \subset A_0 \subset C$.

⌟

Proof: 1: By(11.2.5.2).

2: Let $I^n \subset B$, then $(B \cap A_0, I^n)$ is a couple of definition of B.

3: By2, C is Huber, take a ring of definition A_0 of C, then $A_0 B$ is open and bounded in C, thus a ring of definition. □

Lemma (11.2.5.4). If A is a Huber ring and $T \subset A$ is a subset that generates an open ideal of A, then for any open nbhd U of A, the subgroup $T^n U$ is open. ⌟

Proof: Let (A_0, I) be a couple of definition. By assmption the ideal J generated by T is open, thus J^n is also open, and contains some I^m. Now we can change I^m to I. Now I is f.g., so there is a finite subset $M \subset A$ that $I \subset T^n M$. Notice M is bounded because it is finite, so there is an integer r that $I^r M \subset U$, thus $I^{r+1} \subset T^n U$, and $T^n U$ is open. □

Def. (11.2.5.5) [Tate Huber Ring]. A **Tate Huber ring** is a Huber ring s.t. there exists an open subring A_0 that the induced topology on A_0 is t-adic for some $t \in A_0$ which becomes a unit in A. Such a t is called a **pseudo-uniformizer** of A. ⌟

Prop. (11.2.5.6) [Examples of Tate Huber Rings].

- If K is a complete non-Archimedean field and R is a K-Banach algebra, then R is Tate with a ring of definition by $(R_{\leq 1}, t)$, where t is a pseudo-uniformizer of K.

- If A_0 is any ring and $g \in A_0$ is a nonzero-divisor, and let $A = A_0[g^{-1}]$ equipped with the g-adic topology, then it is an Tate Huber ring.

⌟

Prop. (11.2.5.7) [Properties of Tate Huber Rings]. If a Huber ring A is Tate with a topological nilpotent unit g and $A_0 \subset A$ is any ring of definition, then there exists n large that $g^n \subset A_0$. And in this case, A_0 is g^n-adic and $A = A_0[(g^n)^{-1}]$.

In this case, a subset $S \subset A$ is bounded iff $S \subset g^{-n}A_0$ for some n. ⌟

Proof: Because A_0 is open in g, there is some n that $g^n \subset A_0$, and then with n even larger we can assume $g \in I$, because g is topologically nilpotent, and gA_0 is also open in A_0, thus it contains I^m for some m. So now $g^{mn}A_0 \subset I^m \subset g^n A_0$, which means A_0 is g^n-adic.

To show $A = A_0[(g^n)^{-1}]$, it suffices to notice $g^{kn}x \to 0$ as $k \to \infty$ for any $x \in A$, so for k large, $g^{kn}x \in A_0$.

The last assertion is easy, as open subsets of A and $g^{kn}A_0$ are cofinal. □

Prop. (11.2.5.8) [Power-Bounded Elements and Topologically Nilpotent Elements]. The subset A^0 of power-bounded elements in A is a subring, and it is the filtered colimit of all the ring of definition in A, thus open. It is also integrally closed in A.

The subset A^{00} fo topologically nilpotent elements of A is a radical ideal of A^0. But it is in general not an ideal of A.

Recall A is called uniform if A^0 is bounded(14.2.1.6), or equivalently A^0 is a ring of definition, by(11.2.5.2). ⌟

Proof: By(11.2.5.3), every power-bounded element is contained in a ring of definition, and any ring of definition is bounded, so A^0 is the union of all rings of definitions of A, and this is filtered by(11.2.5.3).

To show A^0 is integrally closed, notice by what we already proved, if a is integral over A^0, then it is integral over a ring of definition A_0, but then $\{a^n\} \subset A_0[a]$ is bounded, so $a \in A^0$.

Showing A^{00} is a radical ideal of A^0 is easy and omitted. □

Cor. (11.2.5.9). If $A \in \mathcal{H}\mathrm{ub}\,\mathcal{R}\mathrm{ing}$ is separated, Tate and uniform, then A is reduced. ⌟

Proof: Assume that A_0 the set of power-bounded elements is a ring of ideal and $g \in A_0$ is a pseudo-uniformizer. If x is nilpotent, then g^{-n} is nilpotent for any x, so power-bounded and $g^{-n}x \in A_0$, which means $x \in g^n A_0$ for any n. But A_0 is separated, so $x = 0$. □

Cor. (11.2.5.10). For $A \in \mathcal{H}\mathrm{ub}\,\mathcal{R}\mathrm{ing}$, an ideal $J \in \mathrm{Ideal}(A)$ is open iff $A^{00} \in \sqrt{J}$. ⌟

Proof: If J is open, then clearly $A^{00} \subset \sqrt{J}$. Conversely, if $A^{00} \subset \sqrt{J}$ and (A_0, I) is a couple of definition, then $I \subset A^{00}$ by(11.2.1.9), so $I \subset \sqrt{J}$. And I is f.g., so $I^N \subset J$ for some J, thus J is open. □

Prop. (11.2.5.11). If K is a complete non-Archimedean field, then any Banach K-algebra R is a complete Tate ring, and if K, R are perfectoids, then $R^{00} = K^{00}R^0$. ⌟

Proof: In the perfectoid case, first $K^{00}R^0 \subset R^{00}$, and for any topological nilpotent α, $\alpha^n \subset tR^{00}$ for a pseudo-uniformizer t. Thus R^{00} and $K^{00}R^0$ has the same radical, it suffices to show $K^{00}R^0$ is radical, but the quotient $R^0/K^{00}R^{00}$ is a perfect K^0/K^{00}-algebra by perfectoidness, thus it must be radical. □

Prop. (11.2.5.12) [Complete Perfect Tate ring is Uniform, André]. If A is a complete Tate ring of char$p$ that is perfect, then A is uniform. ⌟

Proof: Let (A_0, t) be a ring of definition, let $A_n = A_0^{\frac{1}{p^n}}$, then $A_\infty = \operatorname{colim} A_n = (A_0)_{\mathrm{perf}}$. We check $t^{\frac{1}{p^n}} A^0 \subset A_\infty \subset t^{-1} A_0$, which shows A^0 is bounded.

If $f \in A^0$, then $t^a f^{\mathbb{N}} \subset A \subset A_\infty$, and A_∞ is perfect, so $t^{\frac{a}{p^n}} f \in A_\infty$ for all n. Notice the Frobenius is a continuous bijection of Banach spaces, so it is open by Banach theorem(11.7.2.5), so $A_0^p \supset t^{mp} A_0$, thus $t^m A_1 \subset A_0$, and then $t^{\frac{m}{p^n}} A_{n+1} \subset A_n$. So $t^{\sum_n m/p^n} A_n \subset A_1$. So $t^c A_\infty \subset A_0$, for c large. □

Huber Pairs

Def. (11.2.5.13) [Huber Pairs]. For $A \in \mathcal{H}\mathrm{ub}\mathcal{R}\mathrm{ing}$, a **ring of integral elements** is an open and integrally closed subring of A contained in A^0(11.2.5.8)(e.g. A^0 itself, by(11.2.5.8)). A **Huber pair** is a pair (A, A^+) that A is a Huber ring and A^+ is a ring of integral elements. A morphism of Huber pairs should preserve the ring of integers.

A Huber ring is called an **Affinoid Tate ring** if A is Tate. ⌟

Prop. (11.2.5.14). $A^{00} \subset A^+$ as an ideal for any ring of integral elements A^+. In particular, A^+ contains any pseudo-uniformizer, and the set of rings of integral elements is in bijection with integrally closed subrings of A/A^{00}.

Also, A^+ is a filtered colimits of rings of definitions. ⌟

Proof: $t \in A^{00}$ is topologically nilpotent hence $t^n \subset A^+$ for some n as it is open, and then $t \in A^+$ as it is integrally closed. It is an ideal because it is an ideal of A^0(11.2.5.8).

For the last assertion, notice that A^0 is the filtered colimits of rings of definitions(11.2.5.8), and the intersection of a ring of definition with A^+ is also a ring of definition, because it is open and bounded(11.2.5.2), the result follows. □

Def. (11.2.5.15) [Zariski, Henselian, Complete Huber Pairs]. A Huber ring (A, A^+) is called

- **complete** iff A is complete.
- **Henselian** iff (A^+, A^{00}) is a Henselian pair.
- **Zariski** iff (A^+, A^{00}) is a Zariski pair.

⌟

Prop. (11.2.5.16). An affinoid Tate ring (A, A^+) with a ring of definition (A_0, I) that $A_0 \subset A^+$ is

- Zariski iff I is in the Jacobson radical of A_0.
- Henselian iff the pair (A_0, I) is Henselian.
- Complete then it is Henselian.
- Henselian then it is Zariski.

⌟

Proof: 1: We prove that if $t \in \mathrm{rad}(A_0)$, the for any other $B_0 \supset A_0$, $t \in \mathrm{rad}(B_0)$. If this is true, then as A^+ is a filtered colimits of rings of definitions(because A^0 does), it is clear that t lies in the maximal ideal (check $1 + at$ is unit). For this, if $\mathfrak{m} \subset B_0$ is maximal and $t \notin \mathfrak{m}$, choose n that $t^n B_0 \subset A_0$, and an element $b \in B_0$ that maps to t^{-n-1} modulo $\mathfrak{m}$, then $a = t^n b \in A_0$ is mapped to t^{-1}. Thus the composition $A_0 \to B_0 \to B_0/\mathfrak{m}$ is surjective: $\bar{b}$ is the image of $a^n(t^n b) \in A$. So t is not in a maximal ideal of A_0, contradiction.

Conversely, Cf.[Bhatt Perfectoid Space P57].

2: Cf.[Bhatt Perfectoid Spaces P57].

3: A is complete then A_0 is complete, hence (A_0, I) is Henselian by(5.3.10.6), so it is Henselian by item2. 4: Trivial. □

Adic Morphisms

Def. (11.2.5.17) [Adic Morphisms]. A morphism of Huber rings $f : A \to B$ is called an **adic morphism** if we can choose rings of definitions A_0, B_0 and an ideal of definition I of A that $f(A_0) \subset B_0$, and $f(I)B_0$ is an ideal of definition of B_0.

A morphism $(A, A^+) \to (B, B^+)$ of Huber pairs is called adic if $A \to B$ is. ⌟

Prop. (11.2.5.18). Let $f : A \to B$ be an adic morphism between Huber rings, then:

1. f is continuous and open.
2. If A_0, B_0 are rings of definition s.t. $f(A_0) \subset B_0$, then for any ideal of definition $I \subset A_0$, $f(I)B_0$ is an ideal of definition in B_0.
3. f maps bounded sets to bounded sets.

⌟

Proof: Let $f(A_0) \subset B_0$ and $J = f(I)B_0$. Then $I^n \subset f^{-1}(J^n)$, so f is continuous.

If E is bounded in A, for any n, let m be that $I^m E \subset I^n$, then $f(E)f(I)^m = f(EI^m) \subset f(I^n) \subset J^n$, thus $f(E)J^m \subset J^n$, so $f(E)$ is bounded. □

Construction of Huber Rings

Main references are [Mor19].

Prop. (11.2.5.19) [Quotient]. Let (A, A^+) be a Huber ring and $\mathfrak{a}$ be an ideal of A, then the quotient pair $(A/\mathfrak{a}, (A/\mathfrak{a})^+)$ where $A/\mathfrak{a}$ is the integral closure of $A^+/\mathfrak{a}$ in $A/\mathfrak{a}$. ⌟

Prop. (11.2.5.20) [Completion of Huber Rings]. Let A be a Huber ring and (A_0, I) be a couple of definition. Set $\widehat{A} = \varprojlim_n A/I^n$(as an Abelian group), then:

1. The canonical map $\widehat{A_0} \to \widehat{A}$ is injective and $\widehat{A_0} \cap A = A_0$.
2. If we put the unique topology on $\widehat{A}$ that $\widehat{A_0}$ is an open subgroup, then $\widehat{A}$ is complete.
3. There is a unique topological ring structure on $\widehat{A}$ that $A \to \widehat{A}$ is continuous.
4. $\widehat{A}$ is Huber with a couple of definition $(\widehat{A_0}, I\widehat{A_0})$, and the canonical map $A \to \widehat{A}$ is adic.
5. $\widehat{A_0} \otimes_{A_0} A \to \widehat{A}$ is an isomorphism.

⌟

Proof: Cf.[Mor19]P72. □

Prop. (11.2.5.21). Let A be a Huber ring and $i : A \to \widehat{A}$ be the completion, then under the bijection of(11.2.1.6),

- $\widehat{A}^0 = \widehat{A^0}, \widehat{A}^{00} = \widehat{A^{00}}$.
- $G \subset A$ is a ring of definition iff $\widehat{G} \subset \widehat{A}$ is a ring of definition.
- the map $\mathrm{Cont}(\widehat{A}) \to \mathrm{Cont}(A)$ is a bijection.

⌟

Proof: Cf[Mor19] P75. □

Prop. (11.2.5.22). Let A be a Huber ring, then under the bijection of(11.2.1.6), an open ring A_0 is a ring of integral elements of A iff $A_0^\wedge$ is a ring of integral elements of $A^\wedge$. ⌟

Proof: It is easy to show A_0 is a ring iff $A_0^\wedge$ is a ring, and by(11.2.5.21), $A_0 \subset A^0$ iff $A_0^\wedge \subset (A^\wedge)^0$.

It suffices to prove that if A_0 is open and integrally closed, then $A_0^\wedge$ is integrally closed in $A^\wedge$. Let $x \in A^\wedge$ satisfy $x^d + a_{d-1}x^{d-1} + \ldots + a_0 = 0$, where $a_i \in A_0^\wedge$, because $A_0^\wedge$ is open, we can find $x' \in A$ and $a_i' \in A_0$ that $(x')^d + a_{d-1}'(x')^{d-1} + \ldots + a_0' \in A_0'$, but then $x' \in A_0$ because A_0 is integrally closed, and thus $x = (x - x') + x' \in A_0'$. □

Cor. (11.2.5.23) [Completion of Huber Pairs]. The forgetful functor from the category of complete Huber pairs to the category of Huber pairs has a left adjoint called completion, where $(A, A^+)^\wedge = (A^\wedge, (A^\wedge)^+)$, where $(A^\wedge)^+$ is the closure of the image of $A^\wedge$ in $A^\wedge$. ⌟

Prop. (11.2.5.24) [Completion, Henselization, Zariski Localization]. There are left adjoint to the forgetful functors from the category of complete/Henselian/Zariski pairs to the category of pairs, called the **completion/Henselization/Zariski localization** of pairs. And there are natural maps

$$(A, A^+) \to (A, A^+)_{\mathrm{Zar}} \to (A, A^+)_{Hens} \to (\widehat{A}, \widehat{A}^+)$$

⌟

Proof:

□

Prop. (11.2.5.25) [Tensor Products of Adic Maps of Huber Rings].

- If $(A, A^+) \to (B, B^+)$ is adic, then pullback along the associated map of topological spaces $\mathrm{Spa}(B, B^+) \to \mathrm{Spa}(A, A^+)$ preserves rational subsets.
- Let $(B, B^+) \leftarrow (A, A^+) \to (C, C^+)$ be a diagram of Huber pairs where both morphisms are adic. Let A_0, B_0, C_0 be rings of definition compatible with the morphisms, and $I \subset A_0$ be an ideal of definition. Let $D = B \otimes_A C$ and let D_0 be the image of $B_0 \times_{A_0} C_0$ in D. Make D into a Huber ring by declaring D_0 to be a ring of definition with ID_0 as its ideal of definition and D^+ be the integral closure of the image of $B^+ \otimes_{A^+} C^+$ in D. Then (D, D^+) is a Huber pair, and it is the pushout of the diagram in the category of Huber pairs.

⌟

Proof: For 1, it suffices to show that if T is a finite set of A that TA is open, then TB is open in B: $I \subset TA$ for some ideal of definition $I \subset A_0$, in which case $IB_0 \subset B_0$ is also an ideal of definition by(11.2.5.18), thus open, and so TB is also open as $IB \subset TB$.

2 just follows from the definition. □

Remark (11.2.5.26) [Non-Adic Morphisms]. Pushouts may not exists for non-adic morphisms of Huber rings. For example, $\mathbb{Z}_p \to \mathbb{Z}_p[[T]]$ is not adic(11.2.5.18), and the diagram

$$(\mathbb{Z}_p[[T]], \mathbb{Z}_p[[T]]) \leftarrow (\mathbb{Z}_p, \mathbb{Z}_p) \to (\mathbb{Q}_p, \mathbb{Z}_p)$$

has no pushout in the category of Huber pairs: If there is a pushout (D, D^+), then we will have a morphism

$$(D, D^+) \to (\mathbb{Q}_p\langle T, \frac{T^n}{p}\rangle, \mathbb{Z}_p\langle T, \frac{T^n}{p}\rangle)$$

for each $n \geq 1$. But notice that T is nilpotent in D, and $1/p \in D<$ so $T^n/p \to 0 \in D$ as $n \to \infty$. So $T^n/p \in D^+$ for some n, but then $T^n/p \in \mathbb{Z}_p\langle T, \frac{T^{n+1}}{p}\rangle$, which is impossible. ⌟

Def. (11.2.5.27) [Topological Polynomial Functions]. Let A be a non-Archimedean topological ring, and $\{X_i\}_{i\in I}$ be a family of indeterminates, $\{T_i\}_{i\in I}$ be a family of subsets of A that satisfies $T_i^n U$ is open for any $n > 0, i$ and open nbhd U of A.

Let $\mathbb{N}^{(I)}$ be the set of functions $I \to \mathbb{N}$ with finite support, then for any $\nu \in \mathbb{N}^{(I)}$, let $T^\nu = \prod T_i^{\nu(i)}$. For any nbhd U of A, we set

$$U_{[X,T]} = \{\sum_{\nu\in\mathbb{N}^{(I)}} a_\nu X^\nu | a_\nu \in T^\nu U\},$$

Then there exists a unique topological structure on $A[X]$ that $U_{[X,T]}$ form a fundamental system of nbhds of 0, and denote it by $A[X]_T$. It satisfies:

- the canonical inclusion $\iota : A \to A[X]_T$ is continuous and the set $\{T_i X_i\}_{i\in I}$ is power-bounded.
- ι satisfies the universal property that any continuous map $f : A \to B$ to another non-Archimedean topological ring B that $\{f(T_i)X_i\}_{i\in I}$ is power-bounded factors through $A[X]_T$.

⌟

Proof: Just notice that $(U \cap V)_{[X,T]} \subset U_{[X,T]} \cap V_{[X,T]}$ and $U_{[X,T]} \cdot V_{[X,T]} = (UV)_{[X,T]}$, so they form a topological basis because A is topological.

The first properties are easily verified. For the second, the extension $f' : A[X] \to B$ exists abstractly, and it suffices to show it is continuous. If we let $E \subset B$ be the subring generated by $\{f(T_i)X_i\}_{i\in I}$, then E is bounded, so for any open subgroup $H \subset B$, there is some open subgroup $G \subset B$ that $EG \subset H$, and thus $f^{-1}(G)$ is open and contains some nbhd U, then $U_{[X,T]} \subset (f')^{-1}(G)$, so f' is continuous. □

Def. (11.2.5.28) [Topological Power Series]. Let A, X, T as in(11.2.5.27), then the set

$$A\langle X\rangle_T = \{\sum_{\nu\in\mathbb{N}^{(I)}} a_\nu X^\nu \in A[[X]] | a_\nu \in T^\nu U \ a.e.\},$$

is a subring of $A[[X]]$, and there is a unique topological structure on $A[[X]]$ that

$$U_{\langle X,T\rangle} = \{\sum_{\nu\in\mathbb{N}^{(I)}} a_\nu X^\nu \in A\langle X\rangle_T | a_\nu \in T^\nu U\},$$

form a fundamental system of nbhds of $A\langle X\rangle_T$. ⌟

Proof: The proof is not hard and similar to that of (11.2.5.27) so omitted. □

Prop. (11.2.5.29). Let A, X, T as in(11.2.5.27), then

- $A[X]_T$ is dense in $A\langle X\rangle_T$ and the topology coincide.
- If A is Hausdorff and T_i is bounded for any $i \in I$, then $A[X]_T$ and $A\langle X\rangle_T$ are all Hausdorff.
- If A is complete and T_i is bounded for any $i \in I$, then $A\langle X\rangle_T$ is complete, so it is the completion of $A[X]_T$.

⌟

Proof: Only the completeness needs proof, Cf.[Mor19]P80. □

Prop. (11.2.5.30)[Power Series is Huber]. Let A be a Huber ring with a couple of definition (A_0, I), and $X = \{X_\lambda\}$ be a finite set of indeterminates, T_λ is a family of subsets of A that $T_\lambda A$ is open in A, then

- $A[X]_T$ is a Huber ring with a couple of definition $((A_0)_{[X,T]}, I_{[X,T]})$, and there is a canonical map $A \to A[X]_T$ which is adic.
- $A\langle X\rangle_T$ is Huber with a couple of definition $((A_0)_{\langle X,T\rangle}, I_{\langle X,T\rangle})$, and there is a canonical map $A \to A\langle X\rangle_T$ which is adic.

⌟

Proof: It suffices to prove for any ideal of definition J, $J_{[X,T]} = J \cdot (A_0)_{[X,T]}$ and $J_{\langle X,T\rangle} = J \cdot (A_0)_{\langle X,T\rangle}$. The first is clear. For the second, use the fact J is f.g. and $\{J^n\}$ is a fundamental basis of nbhds of 0. □

Prop. (11.2.5.31) [Example]. Let $A = \mathbb{Z}_p$ and $T = p$, then there is a Huber ring

$$\mathbb{Z}_p\langle X\rangle_T = \{\sum_{n\geq 0} a_n X^n \in \mathbb{Z}_p[[X]] | l^{-n} a_n \to 0\}$$

with a ring of definition

$$(Z_p)_{\langle X,T\rangle} = \{\sum_{n\geq 0} a_n X^n \in \mathbb{Z}_p\langle X\rangle_T | a_n \in p^n \mathbb{Z}_p\}.$$

Notice that $\mathbb{Z}_p\langle X\rangle_T$ is not adic although $\mathbb{Z}_p$ is(because p is nilpotent but pX is not). ⌟

Def. (11.2.5.32) [Localizations]. Let A be a non-Archimedean topological ring and $\{T_i\}$ is a family of subsets of A satisfying $T_i^n U$ is open for any $n > 0, i$ and open nbhd U of A, and $\{s_i\}$ is a family of elements of A, which generates a multiplicative subset $R \subset A$.

Then there is a unique non-Archimedean ring structure on $R^{-1}A$, denoted by $A(\frac{T}{S})$, that the canonical map $\varphi : A \to A(\frac{T}{S})$ is continuous and the set $\{\frac{\varphi(t)}{\varphi(s_i)}\}$ is power-bounded, and it is the initial map for all maps $A \to B$ satisfying this property. ⌟

Proof: Cf.[Mor19]P83. □

Cor. (11.2.5.33). Let J be the ideal of $A[X]_T$ generated by $\{1 - s_i X_i\}$, then $A[X]_T/J$ with the quotient topology satisfies the same universal property as $A(\frac{T}{S})$, so there is a canonical isomorphism

$$A[X]_T/J \cong A(\frac{T}{S}).$$

In particular, $A(\frac{T}{S})$ is a Huber ring, and the canonical map $A \to A(\frac{T}{S})$ is adic. Explicitly, B_0 is the $(A_0)_{[X,T]}$-subalgebra of B generated by the elements $\frac{T_i}{s_i}$. ⌟

Def. (11.2.5.34). If A is Huber ring, then we denote the completion of $A(\frac{T}{S})$ by $A\langle\frac{T}{S}\rangle$, which is also a Huber ring, and the canonical map $A \to A\langle\frac{T}{S}\rangle$ is adic, by(11.2.5.30) and(11.2.5.33). It satisfies the natural universal property. ⌟

Cor. (11.2.5.35). If A is complete, then we can also regard $A\langle\frac{T}{S}\rangle$ as the quotient of $A\langle X\rangle_T$ by the closure of the ideal generated by $\{1 - s_i X_i\}$. ⌟

Prop. (11.2.5.36) [Example]. Let $A = \mathbb{Z}_p[[T]]$ with the (p,T)-adic topology, then

$$A(\frac{p,T}{T}) = \mathbb{Z}_p[[T]][T^{-1}]$$

with a ring of definition $A[\frac{p}{T}]$, and

$$A(\frac{p,T}{p}) = \mathbb{Z}_p[[T]][p^{-1}]$$

with a ring of definition $A[\frac{T}{p}]$.

In $A\langle\frac{p,T}{T}\rangle$, a ring of definition is $A_{\langle X,T\rangle}/(1-pX)$, which is isomorphic to

$$A\langle\frac{T}{p}\rangle = \{\sum_{n\geq 0} a_n(\frac{T}{p})^n | a_n \in A, a_n \to 0\}$$

by(11.2.5.33). ⌟

6 Analytic Points and Analytic Huber Pairs

Def. (11.2.6.1) [Analytic Huber Rings]. A Huber ring is called **analytic** if the ideal generated by the topologically nilpotent elements is the unit ideal. Any Tate ring is analytic. ⌟

Prop. (11.2.6.2) [Equivalent Definitions of Analytic Rings]. For a Huber ring A, the following are equivalent:

1. A is analytic.
2. Any ideal of definition in any ring of definition of A generates the unit ideal of A.
3. Any open ideal of A is trivial.
4. For any non-trivial ideal I of A, the quotient topology on A/I is not discrete.
5. The only discrete A-module is the 0-module.
6. The set $\mathrm{Spa}(A, A^+)$ contains no point with induced topology on the residue field trivial.

⌟

Proof: Cf.[Ked19] P4.? □

Prop. (11.2.6.3) [Analytic Open Mapping Theorem]. If A is an analytic Huber ring, and M, N are complete Banach A-modules, then any continuous surjective map $M \to N$ is open. ⌟

Proof: Hub94, L2.4(i).? □

Analytic Points

Def. (11.2.6.4) [Analytic Points]. Let A be a Huber ring, then a point $x \in \mathrm{Cont}(A)$ is called an **analytic point** if $\mathfrak{p}_x$ is not open in A. The set of analytic points of $\mathrm{Cont}(A)$ is denoted by $\mathrm{Cont}(A)_{\mathrm{an}}$.

If A is Tate, then $\mathrm{Cont}(A)_{an} = \mathrm{Cont}(A)$, because the only open ideal of A is A itself. ⌟

Prop. (11.2.6.5) [Characterizations of Analytic Points]. Let A be a Huber ring, then for a point $x \in \mathrm{Cont}(A)$, the following is equivalent:

1. x is analytic.

2. $|A^{00}|_x \neq 0$.
3. For any ring of definition and ideal of definition (A_0, I) of A, $|I|_x \neq 0$.

⌟

Proof: $1 \to 2$: $\mathfrak{p}_x$ is non-open, so it cannot contain the open subset A^{00} of A**??**.
$2 \to 3$: trivial because any ring of definition contains A^{00}(11.2.5.8). □

Cor. (11.2.6.6). Let A be a Huber ring and I an ideal of definition with a set of generators $(f_1, \ldots, f_n)$, then

$$\mathrm{Cont}(A)_{an} = \cup_{i=1}^n U(\frac{f_1, \ldots, f_n}{f_i}).$$

⌟

Prop. (11.2.6.7) [Analytic Valuation Microbial]. Let A be a Huber ring and $x \in \mathrm{Cont}(A)_{an}$, then x has rank≥ 1, and the valuation $|\cdot|_x$ on $k(x)$ is microbial(11.2.3.22). ⌟

Proof: If x has rank 1, then $\Gamma_x = 1$, and $\mathfrak{p}_x = \{a \in A||a|_x < 1\}$ is open.
If x is analytic, then there are some $a \in A^{00}$ that $|a|_x \neq 0$(11.2.3.22), thus the image of a in $k(x)$ is non-zero and topologically nilpotent, thus $k(x)$ is microbial by(11.2.3.22). □

Prop. (11.2.6.8)[Adic Morphism and Analytic Points]. Let $\varphi : (A, A^+) \to (B, B^+)$ be a morphism of Huber pairs, then:

- If $x \in \mathrm{Spa}(B, B^+)$ is not analytic, then $\mathrm{Spa}(\varphi)(x)$ is not analytic.
- If φ is is adic, then $\mathrm{Spa}(\varphi) : \mathrm{Spa}(B, B^+) \to \mathrm{Spa}(A, A^+)$ carries analytic points to analytic points.
- If B is complete and $\mathrm{Spa}(\varphi) : \mathrm{Spa}(B, B^+) \to \mathrm{Spa}(A, A^+)$ carries analytic points to analytic points, then φ is adic.
- If φ is adic, then the $\mathrm{Spa}(\varphi)$ maps rational subsets to rational subsets. In particular, $\mathrm{Spa}(\varphi)$ is spectral.

⌟

Proof: 1: Trivial.
2: If $f(x)$ is not analytic, then $I \subset \varphi^{-1}(\mathfrak{p}_x)$, so $f(I) \subset \mathfrak{p}_x$, which means $\mathfrak{p}_x$ is not analytic because $f(I)A_0$ is open.
3: Cf.Morel P96**?**.
4: Only notice that $(f(T))$ is open if (T) is open. □

Cor. (11.2.6.9). If A is an analytic Huber ring, then any continuous morphism $f : A \to B$ is adic, by(17.8.4.24). ⌟

7 Huber and Banach Rings

Cf.[Ked19]1.5.

Prop. (11.2.7.1). Let A be a uniform Huber ring, then for $x = \sum_{n=0}^\infty x_n T^n \in A\langle T\rangle$ such that the coefficients x_n generate the unit ideal of A, then multiplication by x defines a strict inclusion $A\langle T\rangle \to A\langle T\rangle$, i.e. $|xg| \geq |g|$. ⌟

Proof: Cf.[Ked19]P25. □

8 Perfectoid Fields

Notation (11.2.8.1). Let $(K, \mathcal{O}_K, \mathfrak{m}_K, k)$ be a non-Archimedean complete valued field. ⌟

Prop. (11.2.8.2). The valuation can in fact be constructed from K^0 as $|x| = \sup\{\frac{n}{k}|x^k \in t^n K^0\}$ by(3.2.9.5), as it is a rank 1 valuation. ⌟

Def. (11.2.8.3) [Perfectoid Field]. If K has residue characteristic p, then it is called a **perfectoid field** iff:

- The value group $|K^\times| \subset \mathbb{R}_+^\times$ is not discrete.
- $\mathcal{O}_K/(p)$ is semi-perfect.

⌟

Prop. (11.2.8.4) [Examples of Perfectoid Fields].

- $K = \mathbb{Q}_p(p^{\frac{1}{p^\infty}})^\wedge$. $\mathcal{O}_K = \mathbb{Z}_p(p^{\frac{1}{p^\infty}})^\wedge$, and $\mathcal{O}_K/(p) \cong [\mathbb{F}_p(t^{\frac{1}{p^\infty}})/(t)]^\wedge$, which is clearly semi-perfect. And its value group is $\mathbb{Z}[p^{-1}]$.
- $K = \mathbb{C}_p$, its value group is $\mathbb{Q}$, and $K = \overline{K}$, so $\mathcal{O}_K/(p)$ is clearly perfect.
- if $\mathrm{char}\, K = p$, then K is a perfectoid field iff K is perfect: if K is perfect, then it is clearly perfectoid, and the semi-perfectness of $\mathcal{O}_K$ implies its perfectness, so also K is perfect(multiply by a p-power of an element in $\mathfrak{m}_K$).
- If K is a perfectoid field and $|p| \leq |\varpi| < 1$ is a pseudo-uniformizer, then $K/(\varpi)$ is perfect hence perfectoid.

⌟

Prop. (11.2.8.5) [Perfectoid Field and Integral Perfectoid Rings]. The ring of integers $\mathcal{O}_K$ for a perfectoid field K is an integral perfectoid ring(8.9.3.1). ⌟

Proof: We assume that K is of char0, then we check conditions in(8.9.3.6). It is clear that $\mathcal{O}_K$ is p-adically complete, p-normal. To find $\varpi^p = pu$, as $|K^*|$ is not discrete, we find x that x^p divides p, and then there exists some y that $y^p \equiv x^p/p \mod p$, thus $(xy)^p \equiv 1 \mod p$, thus $\varpi = xy$ satisfies the condition. □

Prop. (11.2.8.6). If $K \in \mathcal{P}\mathrm{erfd}$, then

- $|K^\times|$ is a p-divisible Abelian group.
- $\mathfrak{m}_K^2 = \mathfrak{m}_K$, and $\mathfrak{m}_K$ is flat**?**.
- $\mathcal{O}_K$ is not Noetherian.

⌟

Proof: 1 : First if $|p| < |x| \leq 1$, we show $|x|$ is p-divisible: there is a $y, z \in K^0$ that $y^p = x + pz$, so $|y|^p = |x|$. Now because $|K^*|$ is not discrete, so there is a $|x| \notin |p|^{\mathbb{Z}}$, by rescaling, we may assume $|p| < |x| \leq 1$, thus $p = xy$ for some y, and $|p| < |y| \leq 1$, too. So $|p|$ is also divisible by p, so it is clear now $|K^*|$ is divisible by p.

2 follows from(8.9.3.5)(11.2.8.5).

$2 \to 3$ by Nakayama's lemma, because otherwise $K^{00} = 0$. □

Cor. (11.2.8.7). The proof of 1 also shows that $|K^\times|$ is generated by $|x|$ that $|p| < |x| < 1$. ⌟

Lemma (11.2.8.8). If $C^\flat$ is a perfectoid space of residue characteristic p, then $1 + \mathfrak{m}_{C^\flat}$ is a $\mathbb{Q}_p$-algebra. ⌟

Proof: Both φ and exponentiation of $\mathbb{Z}_p^*$ is definable, so $p^n t \cdot (1 + x) = (\varphi^n(1 + x))^k$. □

Tilting

Prop. (11.2.8.9) [Pseudo-Uniformizers]. Fix a **pseudo-uniformizer** $|p| \leq |\varpi| < 1$, consider the tilting(5.5.1.9) $\mathcal{O}_K^\flat$, then by(5.5.1.12), this topological group doesn't depends on π chosen. ⌟

Remark (11.2.8.10). There are diagrams:
$$\begin{array}{ccc} \lim_{x\to x^p}\mathcal{O}_K & \longrightarrow & \mathcal{O}_K \\ \downarrow\cong & \nearrow\sharp & \downarrow \\ \mathcal{O}_K^\flat = \lim_\varphi K^0/(\varpi) & \longrightarrow & \mathcal{O}_K/(\varpi) \end{array}.$$ ⌟

Prop. (11.2.8.11) [Tilting of $\mathcal{O}_K$]. There is an element $t \in \mathcal{O}_K^\flat$ that $|t^\sharp| = |\varpi|$, t maps into (π) and gives an isomorphism $\mathcal{O}_K^\flat/(t) \cong \mathcal{O}_K/(\varpi)$.

Moreover, the t-adic topology on $\mathcal{O}_K^\flat$ is complete, and coincides with the topology of $\mathcal{O}_K^\flat$ given as in(5.5.1.9). ⌟

Proof: There are canonical surjective map $K^{0\flat} \to K^0/p \to K^0/\pi$, and by p-divisibility of the value group(11.2.8.6), there is a $f \in K^0$ that $|f|^p = |\pi|$, so in particular $|f| > |\pi|$, thus $f \neq 0 \in K^0/\pi$. and choose a $g \in K^{0\flat}$ lifting $f \mod \pi$, then $g^\sharp \equiv f \mod \pi$, see diagram(11.2.8.10). so $|g^\sharp| = |f|$ as $|f| > |\pi|$. Now let $t = g^p$, then $|t^\sharp| = |f|^p = |\pi|$.

Now clearly t maps into (π), and if g maps to 0 in K^0/π, then by the diagram again, $g^\sharp \in (\pi)$, and $(t^\sharp) = (\pi)$, so $g^\sharp = at^\sharp$ for some $a \in K^0$. so $t|g$ in $K^{0\flat}$, as by(5.5.1.17), $R^{0\flat}$ is a valuation ring in the valuation $|\cdot| \circ \sharp$.

For the last assertion, just use the commutative diagrams:
$$\begin{array}{ccc} K^{0\flat}/(t^{p^n}) & \longrightarrow & K^{0\flat}/(t^{p^{n-1}}) \\ \downarrow & & \downarrow \\ K^0/(\pi) & \xrightarrow{\varphi} & K^0/(\pi) \end{array}$$
, where the vertical are isomorphisms, and compute their inverse limits. □

Cor. (11.2.8.12) [Tilting of Perfectoid Fields].

- $\mathcal{O}_K^\flat$ is a valuation ring of rank 1, with the field of fraction $K^\flat = \mathcal{O}_K^\flat[t^{-1}] \in \mathcal{P}\mathrm{erfd}$.
- Its maximal ideal is $(t^{\frac{1}{p^\infty}})$, with Krull dimension 1.
- The value group and residue field of K and $K^\flat$ is canonical isomorphic.

⌟

Proof: $K^{0\flat}$ has rank no more than K^0 which is 1(11.2.8.3), and it is non-trivial because $|t| = |\pi|$, so the rank is 1, and it is perfect by definition, so K is perfectoid by(11.2.8.4).

For the maximal ideal, the maximal ideal of $K^{0\flat}/t$ is its nilradical, as it is a valuation ring of rank 1(3.2.9.5), which is clearly $(t^{\frac{1}{p^\infty}})$. For the dimension, by(11.2.3.3), the Krull dimension equal the rank, which is 1.

For the residue field, use the isomorphism(11.2.8.11), $K^{0\flat}/t = K^0/\pi$ and the second item just proved, and for the value group, the same lemma(11.2.8.11) gives any $|p| \leq |\pi| < 1$ are in the value group of $K^\flat$, and $|K^\times|$ is generated by these values by(11.2.8.7). □

Prop. (11.2.8.13) [Tilting Continuous Valuations]. If $K \in \mathcal{P}\mathrm{erfd}$, for any continuous valuation on K of any rank, the function $|\cdot|^\flat = |\cdot| \circ \sharp$ is a continuous valuation on $\mathcal{O}_K^\flat$, and every continuous valuation of $\mathcal{O}_K^\flat$ comes from this way. ⌟

Proof: Clearly $|-|^\flat$ is multiplicative and has trivial kernel, and it is non-Archimedean: for $f = (f_n), g = (g_n) \in K^\flat$, $f+g = (\lim_k (f_{n+k}+g_{n+k})^{p^k})$ by(5.5.1.14). So

$$|f+g|^\flat = |(f+g)^\sharp| = |\lim_k (f_k+g_k)^{p^k}| = \lim_k |f_k+g_k|^{p^k} \leq \lim_n \max\{|f_n|,|g_n|\}^{p^n} = \max\{|f_0|,|g_0|\}.$$

so it is non-Archimedean. It is also continuous because $\sharp$ is continuous.

Conversely, we notice a continuous valuation on a rank 1 valuation field corresponds to valuation rings in the residue field k, so by(11.2.8.12), we get a bijection on the continuous valuations. □

Prop. (11.2.8.14) [Almost Purity in Dimension 0**].** If $K \in \mathcal{P}\text{erfd}$ and L/K is a finite field extension, with the natural topology, then:

- $L \in \mathcal{P}\text{erfd}$.
- $[L^\flat : K^\flat] = [L : K]$.
- The map $L \to L^\flat$ defines an isomorphism $K_{fet} \cong K^\flat_{fet}$.

⌟

Proof: This is a special case of almost purity theorem(11.2.10.1). □

Cor. (11.2.8.15). For $K \in \mathcal{P}\text{erfd}$, $\text{Gal}_K \cong \text{Gal}_{K^\flat}$. ⌟

Lemma (11.2.8.16) [Kedlaya]. For $K \in \mathcal{P}\text{erfd}$, then $K^\flat$ is alg.closed iff K is alg.closed. ⌟

Proof: Let $P(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0 \in K^0[X]$ be a irreducible monic polynomial, then its Newton polygon is a line, and we may assume $|a_0| = 1$, as $K^{0\flat}$ is alg.closed, so $|K^{0*}| = |K^{0\flat *}|$(11.2.8.12) is a Q=vector space.

Next we choose a $Q(X) \in K^{0\flat}[X]$ that $Q(X) \equiv P[X] \mod t$, as $K^{0\flat}/t \cong K^0/\pi$(11.2.8.11). Now we consider $P(x+y^\sharp)$, then $P(y^\sharp)$ is divisible by π, so its Newton polygon is now of positive slope, so $c^{-d}P(cx+y^\sharp) \in K^0[X]$ again, where $c^d = |P(y^\sharp)| \leq |\pi|$. Then notice by iteration this argument, we get a sequence of $y_n^\sharp$, and then $y_1^\sharp + c_1 y_2^\sharp + c_1c_2 y_3^\sharp + \ldots + c_1\ldots c_n y_{n+1}^\sharp$ that converges to a root of $P(X)$. □

Prop. (11.2.8.17) [Examples of Tilting].

- If $K = \mathbb{Q}_p(p^{\frac{1}{p^\infty}})^\wedge$, then $\mathcal{O}_K = \mathbb{Z}_p[p^{\frac{1}{p^\infty}}]^\wedge$, thus $K^\flat = \mathbb{F}_p\widehat{((t))_{\text{perf}}}$(5.5.1.11). And if $L = K(\sqrt{p})$, then similarly $L^0 = \widehat{\mathbb{Z}_p[p^{\frac{1}{2p^\infty}}]}$, and $L^\flat = K^\flat(\sqrt{t})$.
- If $K = \mathbb{Q}_p(\mu_{p^\infty})^\wedge$, then $\mathcal{O}_K = \widehat{\mathbb{Z}_p[\mu_{p^\infty}]}$, notice there is a map $\mathbb{Z}_p[\varepsilon^{\frac{1}{p^\infty}}] \to \mathbb{Z}_p[\mu_{p^\infty}]$ with kernel $(1+\varepsilon^{\frac{1}{p}} + \ldots + \varepsilon^{\frac{p-1}{p}})$, so

$$\mathcal{O}_K/(p) = \mathbb{F}_p[\varepsilon^{\frac{1}{p^\infty}}]/(\varepsilon^{\frac{1}{p}}-1)^{p-1} \cong \mathbb{F}_p[t^{\frac{1}{p^\infty}}]/(t^{p-1})$$

with the substitution $t = \varepsilon^{\frac{1}{p}} - 1$. Then by(11.2.8.4), $K^{0\flat} = \mathbb{F}_p\widehat{[t^{\frac{1}{p^\infty}}]}$, and $K^\flat = \mathbb{F}_p\widehat{((t))_{\text{perf}}}$.

⌟

Remark (11.2.8.18). Notice that $K = \mathbb{Q}_p(\mu_{p^\infty})^\wedge$ and $K = \mathbb{Q}_p(p^{\frac{1}{p^\infty}})^\wedge$ have the same tiltings, so the tilting functor is not faithful. this is due to the fact that $\mathbb{Q}_p$ is not perfectoid. This will not happen over a perfectoid base field, see(11.2.9.13). ⌟

9 Perfectoid Algebras

Def. (11.2.9.1) [Perfectoid Algebra]. For K a perfectoid field with tilt $K^\flat$, let $t \in K^\flat$ be a pseudo-uniformizer??ith $\varpi = t^\sharp$, so it has a compatible collection of p^n-th roots $(t^{\frac{1}{p^n}})^\sharp$. Now:

- A **perfectoid algebra** over K is a uniform Banach K-algebra R that R^0/π is semi-perfect.
- A **perfectoid algebra** over K^{0a} is a K^{0a}-algebra A that is t-adically complete and flat over K^{0a}(or A_* over K^0, by(5.7.3.3)), and $K^{0a}/\pi \to A/\pi$ is relative perfect, i.e. the Frobenius induces an isomorphism $A/\pi^{\frac{1}{p}} \cong A/\pi$.
- A **perfectoid algebra** over K^{0a}/π is a K^{0a}/π-algebra A that is flat over K^{0a}/π(or A_* over K^0/π, by(5.7.3.3)), and the map $K^{0a}/\pi \to A$ is relatively perfect, i.e. the Frobenius induces an isomorphism $A/\pi^{\frac{1}{p}} \cong A$.

⌟

Remark (11.2.9.2). notice the definition regarding the relative perfectness doesn't depends on π chosen, by the power lifting theorem(2.6.3.9). ⌟

Prop. (11.2.9.3) [Faithfully flatness of Perfectoids]. Nonzero flat $\mathcal{O}_K^a/(\varpi)$-algebras are faithfully flat, so does t-adically complete flat K^{0a}-algebras. In particular, $\mathrm{Perfd}_{\mathcal{O}_K^a/(\varpi)}$ and $\mathrm{Perfd}_{\mathcal{O}_K^a}$ are all faithfully flat modules. ⌟

Proof: If $K^{0a}/\pi \to A$ is not faithfully flat, then there is an ideal $J \subset K^{0a}/\pi$ that $K^0/J \neq 0$ but $A/J = 0$. Now this implies $J \subsetneq I$, so there is a $\varpi \in I - J$ hence $J \subset (\varpi)$. Hence $A/\varpi = 0$ as well. Now there are exact sequences $0 \to K^{0a}/\varpi^n \xrightarrow{\varpi} K^{0a}/\varpi^{n+1} \to K^{0a}/\varpi \to 0$, so tensoring with A and induct, we get $K^{0a}/\varpi^n \otimes A = 0$, but $|\varpi^n| < |\pi|$ for some n, so $A = 0$.

The other case is similar, now $A/\varpi = 0$, so use(5.7.3.3), $A_*/\varpi \subset (A/\varpi)_* = 0$, but A_* is also t-adically complete, so $A_* = 0$, and $A = (A_*)^a = 0$. □

Prop. (11.2.9.4) [Examples of Perfectoid Algebras].

- If $\mathrm{char}\, K = p$, then a K-Banach algebra is perfectoid iff it is uniform and perfect. Likewise, a π-adically complete and π-torsion free K^{0a}-algebra is perfectoid iff it is perfect.
- Let $A = \mathcal{O}_K[x_1^{\frac{1}{p^\infty}}, \ldots, x_n^{\frac{1}{p^\infty}}]^\wedge$, then $A^a \in \mathrm{Perfd}_{\mathcal{O}_K^a}$, and $R = A[\pi^{-1}] \in \mathrm{Perfd}_K$ in the Banach metric as in(14.2.4.8).

⌟

Proof: 1: a perfectoid algebra of char$p$ is perfect, because by semi-perfectness, $x = x_1^p + \pi z_1 = x_1^p + \pi x_2^p + \pi^2 z_2 = \ldots$, so $x = (x_1 + \pi^{\frac{1}{p}} x_2 + \pi^{\frac{2}{p}} x_3 + \ldots)^p$. In fact, uniformity is automatically implied by perfectness, by(11.2.5.12). The case of $\mathcal{O}_K^a$-algebra is similar.

2: A^a is K^{0a}-flat because A_* does, because it is a colimit of completions of polynomial algebras over I and I is flat over K^0(11.2.8.6). and R is perfectoid by(14.2.4.8) because A is totally integrally closed in R, because $K^0[x_1^{\frac{1}{p^\infty}}, \ldots, x_n^{\frac{1}{p^\infty}}]$ does(trivially), and use(5.7.2.10). □

Tilting Equivalence

Prop. (11.2.9.5) [Tilting Equivalence]. There are canonical isomorphisms of categories:

$$\mathrm{Perfd}_K \cong \mathrm{Perfd}_{K^{0a}} \cong \mathrm{Perfd}_{K^{0a}/\pi},$$

where the first map is by $R \mapsto R^{0a}$ and $A \to A_*[t^{-1}]$ just as in(14.2.4.8). The second map is reduction by π.

In particular, using tilting(11.2.8.11), there are canonical isomorphisms of categories:

$$\mathcal{P}\mathrm{erfd}_K \cong \mathcal{P}\mathrm{erfd}_{K^{0a}} \cong \mathcal{P}\mathrm{erfd}_{K^{0a}/\pi} = \mathcal{P}\mathrm{erfd}_{K^{\flat 0a}/t} \cong \mathcal{P}\mathrm{erfd}_{K^{\flat 0a}} \cong \mathcal{P}\mathrm{erfd}_{K^\flat}.$$

If $R \in \mathcal{P}\mathrm{erfd}_K$ corresponds to $S \in \mathcal{P}\mathrm{erfd}_{K^\flat}$, then we call $S = R^\flat$ the **tilting** of R and $R = S^\sharp$ the **untilting** of S. ⌟

Proof: [$\mathcal{P}\mathrm{erfd}_K \cong \mathcal{P}\mathrm{erfd}_{K^{0a}}$]

Firstly, if $R \in \mathcal{P}\mathrm{erfd}_K$, then $A = R^{0a} \in \mathcal{P}\mathrm{erfd}_{K^{0a}}$: $R^0/\pi^{\frac{1}{p}} \to R^0/\pi$ is surjective by definition, for injectivity, if $x^p/\pi \in R^0$, then $x/\pi^{\frac{1}{p}}$ is also power bounded, thus in R^0. And by(14.2.4.8), A is π-adically complete and π-torsion-free, hence R-flat by(5.4.1.12).

Next we show if $A \in \mathcal{P}\mathrm{erfd}_{K^{0a}}$, then A_* is π-adically complete, t-torsion free and p-root closed in $A[\pi^{-1}]$, hence is an left inverse to the mapping $R \to R^{0a}$, by(5.7.3.5). It is complete by(5.7.3.3)2,3.

For p-root closedness, by(5.7.3.3), $A_*/\pi^{\frac{1}{p}} \subset (A/\pi^{\frac{1}{p}})_* \hookrightarrow (A/\pi)_*$ by Frobenius, and then so does $A_*/\pi^{\frac{1}{p}} \to A_*/\pi$. Now if $x \in A_*[\pi^{-1}]$ satisfies $x^p \in A_*$, then $y = \pi^{\frac{k}{p}}x \in A_*$ for some k, and we want to lower k by 1 inductively, thus showing $x \in A_*$: As $y^p \in \pi A_*$, $y \in \pi^{\frac{1}{p}}A_*$ by what we have proved, thus $\pi^{\frac{k-1}{p}}x \subset A_*$.

For surjectivity of Frob: $A_*/\pi \to A_*/\pi$, notice first it is almost surjective, because $(A_* \to A_*/\pi)^a = A \to (A_*/\pi)^a \subset (A/\pi)^a_* = A/\pi$ is surjective by hypothesis, then by(5.7.2.3), it suffices to show that Frob is surjective on A/IA. For some $x \in A^*$, choose $0 < 1 < c$, almost surjectivity shows that $\pi^c x \equiv y^p \mod \pi A_*$, so $(y/p^{\frac{c}{p}})^p \in A_*$, thus $y \in p^{\frac{c}{p}}A_*$, thus $x \equiv (y/p^{\frac{c}{p}})^p \mod \pi^{1-c}A_* \subset IA$, so we are done.

Finally, this is also a right inverse, because we know that $A_* \cong R^0$ by(5.7.3.5), thus $A \cong R^{0a}$ in Mod^a_R. □

Proof: [$\mathcal{P}\mathrm{erfd}_{K^{0a}} \cong \mathcal{P}\mathrm{erfd}_{K^{0a}/\pi}$]

Firstly the reduction is a perfectoid K^{0a}/π-algebra: it is flat because flatness is stable under base change, and the rest are trivial. To construct a converse is a problem of deformation theory, we need to lift from K^{0a}/π-algebra via K^{0a}/π^n-algebras to a K^{0a}-algebra, suppose each lifting is unique up to isomorphism and the lift A_n is flat over K^{0a}/π^n, then we can form their inverse limit, which is flat, because it is π-torsion-free: if $\pi(x_n) = 0$, then by $0 \to \pi^n K^{0a}/\pi^{n+1} \to K^{0a}/\pi^{n+1} \xrightarrow{\pi} K^{0a}/\pi^n \to 0$ and the flatness of A_{n+1}, $x_{n+1} \in \pi^n A_{n+1}$, thus $x_n = 0$, and $x = 0$.

Now $0 \neq A \in \mathcal{P}\mathrm{erfd}_{K^{0a}/\pi}$, then A is faithfully flat by(11.2.9.3), then by(5.7.1.8), $A_{!!}$ is faithfully flat, and $(-)_{!!}$ is preserves all colimits and also Frobenius, so $A_{!!}$ is relatively perfect. Then we use the above argument, and(7.1.4.1) to show that there is a $\widetilde{A} \in \mathcal{C}$ which is π-adically complete and K^0-flat, then $\widetilde{A} = (\widetilde{A_{!!}})^a$ is also p-adically complete and K^{0a}-flat, by(5.7.3.3).

And we check $\widetilde{A}/\pi = (\widetilde{A_{!!}/\pi})^a = (A_{!!})^a = A$ as $(-)_{!!}$ commutes with colimits, and conversely, if $A \in \mathcal{P}\mathrm{erfd}_{K^{0a}}$, we need to show $A = \widetilde{A/\pi}$, notice by hypothesis, $A_{!!}$ is faithfully flat K^0-algebra that is relatively flat over K^0/π, now it is also complete, because $A_{!!} \to A_*$ is an injection(because $(-)^a$ is exact) and almost isomorphism, so the cokernel is π-torsion, and A_* is complete, so does $A_{!!}$, by(5.2.3.9). Now $A_{!!}/\pi = (A_{!!}/\pi)$ as $(-)_{!!}$ commutes with colimits, so $A_{!!}$ is just the lift, and $(\widetilde{A_{!!}/\pi})^a = A^a_{!!} \cong A$. □

Cor. (11.2.9.6) [Tilting via Fountain's Functors]. The tilt $R^\flat$ is just the Foutain's tilting, i.e. $R^\flat = R^{0\flat}[t^{-1}]$, and $R^\flat = \lim_{x \mapsto x^p} R$, $R^{0\flat} = (R^\flat)^0$. ⌟

Proof: Consider the diagram

$$\begin{array}{ccccc} K^{\flat 0}/t^{p^n} & \xrightarrow[\cong]{\varphi^{-n}} & K^{\flat 0}/t \cong K^0/\pi & \longrightarrow & R^0/t \\ & \searrow & \downarrow{\scriptstyle \varphi^n} & & \downarrow{\scriptstyle \varphi^n} \\ & & K^{\flat 0}/t \cong K^0/\pi & \longrightarrow & R^0/t \end{array}$$

Then the upper row is just the unique flat and relative perfect lifting along $K^{\flat 0}/t^{p^n} \to K^{\flat 0}/t$. Taking inverse limit, we get the structure map $K^{\flat 0} \to R^{\flat 0}$, so after almostification, this is just the lifting we are looking for, because it is unique. So $(R^{0\flat})^a = (R^{\flat 0})^a$, and $R^\flat = R^{0\flat}[t^{-1}]$ unwinding the tilting equivalence.

For $R^\flat$, notice there is a map

$$R^\flat \cong (\lim_{x\mapsto x^p} R^0)[t^{-1}] \to \lim_{x\mapsto x^p}(R^0[\pi^{-1}]) \cong \lim_{x\mapsto x^p} R$$

Now injectivity is clear as t is non-zero-divisor, and if $(f_n) \in \lim_{x\mapsto x^p} R$, then $\pi^c f_n \in R^0$ for some c, then $\pi^{\frac{c}{p^n}} f_n \in R^0$ because R^0 is p-root closed(5.7.3.5), so $t^c(f_n) \subset R^{0\flat}$.

For the last assertion, it is true if $R^{0\flat}$ is totally integrally closed in $R^\flat$, by(5.7.3.5). For this, if $t^c f^{\mathbb{N}} \subset R^{0\flat}$, then $\pi^c(f^\sharp)^{\mathbb{N}} \subset R^0$, thus $f^\sharp \in R^0$. And by p-root closedness, p^n-th roots of $f^\sharp$ are all in R^0, so $f = (f_n) \in \lim_{x\mapsto x^p} R$ is in $R^{0\flat}$. □

Prop. (11.2.9.7)[Fountain's Functor θ]. Given a perfectoid field K, the kernel of the Fontaine's map $\theta : A_{\mathrm{inf}}(K) \to K^0$(5.5.1.15) is generated by a non-zero-divisor, in fact, if char$K = 0$, the generator can be chosen to be any element that maps to a generator of $\ker \overline{\theta}$ and if char$K = p$ this diagram is trivial. In particular, the diagram is a pushout. ⌟

Proof: See the proof of(8.9.3.6) in the p-torsionfree case. □

Prop. (11.2.9.8)[Untilting via A_{inf}]. For any perfect $\mathcal{O}_K^\flat$-algebra A, by deformation theory(or in fact Witt theory) there is a unique lifting $W(A)$ lifting it to $A_{\mathrm{inf}}(K^{0\flat})$. And then pushout $W(A) \otimes_{A_{\mathrm{inf}}(K^0)} K^0$ is just the lifting of A/π, because the diagram above is pushout. This is in fact the method of [Kedlaya-Liu] used to prove the tilting-equivalence without the use of almost mathematics and deformation theory. ⌟

Cor. (11.2.9.9) [Limits and Colimits]. Any of the categories in(11.2.9.5) has arbitrary limits and colimits. ⌟

Proof: We construct for $\mathcal{P}\mathrm{erfd}_{K^{0\flat a}}$: The limits is just the limits of topological rings, as the properties of t-adically complete, t-torsion free and perfect is preserved by limits(5.2.3.19). For the colimit, just use the t-adic completion of the left perfection of the colimits in the category of $K^{0\flat a}$-algebras, its t-torsion is almost zero because of perfectness, thus it is almost flat(5.7.3.3). □

Remark (11.2.9.10). Note also for further reference that in the category $\mathcal{P}\mathrm{erfd}_{K^{0a}}$, a filtered colimits is just the π-adically completion of the filtered limits as rings, because perfectness and flatness is preserved(5.4.1.6). ⌟

Prop. (11.2.9.11) [Tilting Equivalence Identifies Fields]. $R \in \mathcal{P}\mathrm{erfd}_K$ is a perfectoid field iff its tilt $R^\flat$ is a perfectoid field. ⌟

Proof: It is proven that if R is a perfectoid field, then $R^\flat$ is a perfectoid field. Conversely, R is a perfectoid field if the spectral norm given by $||x|| = \inf\{|t|^{-1}|t \in R^*, tx \in R^0\}$ is the Banach valuation of R and R is a field.

For the multiplicativeness of $||-||_R$, notice that $R^\flat$ is a perfectoid field, so its non-Archimedean valuation coincides with the spectral norm of $||-||_{R^\flat}$, and this equals $||-||_R \circ \sharp$, because $R^{0\flat} = R^{\flat 0}$, an element $f \in R^{\flat 0}$ iff $f^\sharp \in R^0$. Now the norm extends that of K and commutes with scalar multiplication, so for any f, g, we may assume $f, g \in R^0 - 0\pi^{\frac{1}{p}}R^0$, now choose $a, b \in R^\flat$ that $a^\sharp - f, b^\sharp - g \in \pi R^0$, this can be done because $R^{\flat 0} = R^{0\flat} \to R^0/\pi$ is surjective, then $a, b, ab \notin tR^{\flat 0}$ because $R^{0\flat} = R^{\flat 0}$. Then clearly $||f||_R = ||a||_{R^\flat}, ||g|| = ||b||_{R^\flat}, ||fg||_R = ||ab||_{R^\flat}$, so it is multiplicative by the multiplicativeness of $R^\flat$.

To show R is a field, consider and $f \in R - \pi^{\frac{1}{p}}R$, choose $a \in R^\flat$ that $f = a^\sharp + \pi g$, then as $R^\flat$ is a field, there is a b that $ab = 1$. Now $||\pi||_R < ||\pi^{\frac{1}{p}}||_R \subset ||f||_R = ||a||_{R^\flat} \leq 1$, so we get $||\pi b^\sharp g|| < 1$, then

$$f^{-1} = \frac{1}{a^\sharp + \pi g} = \frac{b^\sharp}{1 + \pi b^\sharp g} = b^\sharp(\sum(-\pi b^\sharp g)^k)$$

can be constructed in R. □

Perfectoid Affinoid Algebra

Def. (11.2.9.12) [Perfectoid Affinoid K-algebras]. An **affinoid K-algebra** (R, R^+) is just an affinoid Tate ring over (K, K^0). It is called a **perfectoid affinoid K-algebra** iff R is a perfectoid algebra. ⌟

Prop. (11.2.9.13) [Affinoid Tilting Equivalence]. The categories of perfectoid affinoid algebras(11.2.9.12) over K and $K^\flat$ are equivalent, where (R, R^+) is identified with $(R^\flat, R^{\flat+})$ iff $R^\flat$ is the tilting of R and

$$\begin{array}{ccc} R^+/\mathfrak{m}R^0 & \xrightarrow{\cong} & R^{\flat+}/\mathfrak{m}^\flat R^{\flat 0} \\ \downarrow & & \downarrow \\ R^0/\mathfrak{m}R^0 & \xrightarrow{\cong} & R^{\flat 0}/\mathfrak{m}^\flat R^{\flat 0} \end{array}.$$

Moreover, in this case, R^+/π is semi-perfect, and $R^{+\flat} \cong R^{\flat+}$ as a subring of $R^{0\flat} \cong R^{\flat 0}$. ⌟

Proof: The case $R^+ = R^0$ is already known by tilting equivalence(11.2.9.5) and(11.2.9.6).

By(11.2.5.11) and(11.2.5.14), $\mathfrak{m}R^0 = R^{00} \subset R^+ \subset R^0$, thus $R^+ \to R^0$ is an almost isomorphism and R^+ is determined by its image $\overline{R^+} \subset R^0/\mathfrak{m}R^0$, which is integrally closed if R^+ does, so the identification is clear.

For the semi-perfectness: as $R^+/\mathfrak{m}R^0$ is integrally closed, it is perfect. Now $R^+ \to R^0$ is an almost isomorphism, so Frob on R^+/π is almost surjective because it does on R^0/π by definition, and now we know Frob is surjective on R^+/π by(5.7.2.3).

To show $R^{+\flat} \cong R^{+\flat}$, we show there is a Cartesian diagram $\begin{array}{ccc} R^{+\flat} & \longrightarrow & R^{\flat+}/\mathfrak{m}^\flat R^{\flat 0} \\ \downarrow & & \downarrow \\ R^\flat & \longrightarrow & R^\flat/\mathfrak{m}^\flat R^{\flat 0} \end{array}$, but this is the Cartesian diagram $\begin{array}{ccc} R^+/\pi & \longrightarrow & R^+/\mathfrak{m}R^0 \cong R^{\flat+}/\mathfrak{m}^\flat R^{\flat 0} \\ \downarrow & & \downarrow \\ R^0/\pi & \longrightarrow & R^0/\mathfrak{m}^\flat R^0 \end{array}$ applied the functor $(-)^{\text{perf}}$, which preserves limits(5.5.1.9). (Notice that $R^+/\mathfrak{m}R^0 \cong R^{\flat+}/\mathfrak{m}^\flat R^{\flat 0}$ is already perfect). □

Cor. (11.2.9.14). Notice that the proof also shows that $R^+ \to R^0$ is an almost isomorphism, thus if R is a perfectoid K-algebra, then R^+ is automatically a perfectoid K^{0a}-algebra by(11.2.9.1). ⌟

Cor. (11.2.9.15) [Perfectoid Affinoid Field]. A perfectoid affinoid K-algebra (R, R^+) is called a **perfectoid affinoid field** iff R is a perfectoid field and R^+ is an open valuation ring.

Notice this is equivalent to $R^+/\mathfrak{m}R^0$ is a valuation ring in $R^0/\mathfrak{m}R^0$. In particular, combining with(11.2.9.11), affinoid perfectoid fields are preserved under tilting and untilting. ⌟

Cor. (11.2.9.16). The tilting equivalence also shows that for any perfectoid affinoid K-algebra (R, R^+), the tilting induces an equivalence of categories $\mathcal{P}\mathrm{erfd}_R \cong$ ⌟

Prop. (11.2.9.17) [Filtered Colimits of Perfectoid Affinoid K-Algebras]. The category of perfectoid affinoid K-algebras has filtered colimits, and it is just the colimits in the category of complete uniform affinoid Tate rings(17.8.2.26). In particular, the filtered colimits of (A_i, A_i^+) is $(\operatorname{colim}_i A_i, \operatorname{colim} A_i^+)$. ⌟

Proof: The colimit is perfectoid because the filtered colimits is exact. □

10 Almost Purity Theorem

Thm. (11.2.10.1) [Almost Purity Theorem]. For $R \in \mathcal{P}\mathrm{erfd}_K$ with tilt S(11.2.9.5),

- Almost purity in characteristic p: (take $(-)_*$ and)Inverting t gives an equivalence $S^0_{a\,\text{fét}} \cong S_{\text{fét}}$.
- Almost purity in characteristic 0: Inverting π gives an equivalence $R^0_{a\,\text{fét}} \cong R_{\text{fét}}$.
- Tilting and untilting functors induce equivalences $R^0_{a\,\text{fét}} \cong S^0_{a\,\text{fét}}$.

In particular, there are equivalences

$$S_{\text{fét}} \xleftarrow{a} S^{0a}_{a\,\text{fét}} \xrightarrow{b} (S^{0a}/t)_{a\,\text{fét}} \cong (R^{0a}/\pi)_{a\,\text{fét}} \xleftarrow{c} R^{0a}_{a\,\text{fét}} \xrightarrow{d} R_{\text{fét}},$$

⌟

Proof: The map a is already given in(5.7.2.14) by passing the power bounded-elements(equivalently, S_*) and inverting t. And it is an isomorphism.

The equivalence of b and c follows from[Almost Ring theory, Thm5.3.27]**?**.

The functor d is given by $A \to A_*[t^{-1}]$. Firstly, A is a perfectoid K^{0a}-algebra. This is because it is almost finite projective thus almost flat, and $R^{0a}/\pi \to A/\pi$ is weakly relative perfect by(5.7.2.15), so does $K^{0a}/\pi \to A/\pi$ because relative perfect is stable under composition. And it is finite projective thus almost direct summand of a finite free module.

So now the tilting equivalence(11.2.9.5) shows that $A_*[t^{-1}] \in R_{\text{fét}}$: it is finite etale because the A_* is finite projective by the right adjointness of $(-)_*$, and unramified is defined in terms of A_*. The converse of d is supposed to be the functor that extract from A_* from $A_*[t^{-1}]$ the total integral closure A_{tic} of R^0, which is functorial. We already know that A_* is totally integrally closed in $A_*[t^{-1}]$ by(11.2.9.5), so $A_{tic} \subset A_*$. Conversely, as A is almostly finitely generated over R^0, for $f \in A_*$, $\pi f^{\mathbb{N}}$ lies in a f.g. R^0-submodule of A_*, so $f^{\mathbb{N}}$ is totally integral over R^0, so $A_* = A_{tic}$.

It's left to show that d is essentially surjective, but this uses perfectoid spaces. For now, we only check that this is true for R being a perfectoid field(of char 0).For this, we show directly that the untilting functor $\sharp : K^\flat_{\text{fét}} \to K_{\text{fét}}$ is essentially surjective. Now $\sharp$ is an equivalence of categories

$\mathcal{P}\mathrm{erfd}_{K^\flat} \to \mathcal{P}\mathrm{erfd}_K$, and it preserves degree, at least for field extensions, so it preserves Galois extensions. Now that finite étale algebra over fields are just disjoint of finite separable extensions(5.4.7.19), so it suffices to show that any finite extension of K is contained in some $L^\sharp$.

Consider $M = \widehat{\overline{K^\flat}}$, it is alg.closed of char$p$ so clearly a perfectoid field, and by(11.2.8.16) $M^\sharp$ is alg.closed. $M^\sharp$ is just the colimit in the category of uniform Banach K-algebras, so its valuation ring is just the completion of the valuation ring of $L^\sharp$ for $L/K^\sharp$ finite Galois. Then if $N = \cup L^\sharp$, then N is dense in $M^\sharp$, and N/K is clearly algebraic and in particular Hensel. So $N \subset \overline{N} \subset M^\sharp$ is dense, so by Krasner's lemma(14.2.1.37), $N = \overline{N}$. Now $N = \cup L^\sharp$ is an alg.closure of K, so every finite extension of K is contained in some $L^\sharp$.

The proof of the general case of the essentially surjectivity of d is continued at(17.8.7.10). □

11.3 Real Analysis(Functions on $\mathbb{R}^n$)

Basic references are [Fol99], [?], [?], [?], [Measure theory and fine properties of functions, Evans] and [Real Analysis and Probability, Dudley], [Real and Complex Analysis, Rudin], [Lan93] and [Stein, Real Analysis].

Notation (11.3.0.1).

- Use notations defined in Topology I.
- Use notations defined in Formal Power Series.

⌟

1 Measures

Def. (11.3.1.1) [σ-Algebras]. For $A \in \mathcal{S}\mathrm{et}$, an **algebra of subsets** of A is a subset of $\mathscr{P}(A)$ that is closed under finite intersections and finite unions. A **σ-algebra** on A is an algebra of subsets of A that is closed under countable unions. ⌟

Def. (11.3.1.2) [Measurable Space]. A **measurable space** is a tuple $(X, \mathcal{M})$ where X is a set and $\mathcal{M}$ is a σ-algebra on X. ⌟

Def. (11.3.1.3) [Measures]. Let $(X, \mathcal{M})$ be a measurable space(11.3.1.2), then a **measure** on X is a function $\mu : \mathcal{M} \to [0, \infty]$ that

- $\mu(\varnothing) = 0$.
- If E_i is a countable family of disjoint sets in $\mathcal{M}$, then $\mu(\cup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} \mu(E_i)$, where the sum converges absolutely if $\mu(\cup_{i=1}^{\infty} E_i) < \infty$.

A **measure space** is a measurable space together with a measure μ. A **probabilistic measure** is a measure μ on $(X, \mathcal{M})$ that $\mu(X) = 1$. ⌟

Def. (11.3.1.4)[Signed Measures]. Let $(X, \mathcal{M})$ be a measurable space(11.3.1.2), then a **signed measure** on X is a function $\mu : \mathcal{M} \to [-\infty, \infty]$ that

- $\mu(\varnothing) = 0$.
- μ assumes at most one of the values $\pm\infty$.
- If E_i is a countable family of disjoint sets in $\mathcal{M}$, then $\mu(\cup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} \mu(E_i)$, where the sum converges absolutely if $\mu(\cup_{i=1}^{\infty} E_i) \in (-\infty, \infty)$.

μ is called a **finite signed measure** if $\mathrm{Im}(\mu) \subset (-\infty, \infty)$. ⌟

Prop. (11.3.1.5). Let $X \in \mathcal{S}\mathrm{et}$ and $\mathcal{M}$ be an algebra on X, then a finitely-additive real-valued function μ on $\mathcal{M}$ is countably-additive iff $\lim_n \mu(A_n) = 0$ for any sequence $(A_n)_{n\in\mathbb{N}} \subset \mathcal{M}$ s.t. $A_0 \supset A_1 \supset \ldots \supset A_n$ and $\cap_n A_n = \varnothing$. ⌟

Proof: [Dudley, P86]. □

Def. (11.3.1.6) [Outer Measures]. Let $X \in \mathcal{S}\mathrm{et}$ and $\mathcal{A}$ be an algebra on X, then for any countably-additive function μ on $\mathcal{A}$ with values in $[0, \infty]$, if we define

$$\mu^* : \mathscr{P}(X) \to [0, \infty] : \mu^*(E) = \inf\{\sum_n \mu(A_n) | A_n \in \mathcal{A}, E \subset \cup_n A_n\},$$

then μ^* restricts to a measure(11.3.1.3) on the σ-algebra $\mathcal{M}$(11.3.1.1) generated by $\mathcal{A}$, called the **outer measure** generated by μ. ⌟

Proof: □

Prop. (11.3.1.7) [Hahn Decomposition Theorem]. Let $(X, \mathcal{M})$ be a measurable space and μ a singed measure on X, a set $E \in \mathcal{M}$ is called **positive(resp. negative/null) for** μ if $\mu(F) \geq 0$(resp. $\mu(F) \leq 0/\mu(F) = 0$) for any $F \in \mathcal{M} \cap \mathscr{P}(E)$.

Then there exists a disjoint decomposition $X = P \coprod N, P, N \in \mathcal{M}$, s.t. P is positive for μ and N is positive for μ. Such a decomposition is unique up to a null subset of μ. ⌟

Proof: Cf.[Follan, P86].**?** □

Def. (11.3.1.8) [Orthogonal Measures]. Let $(X, \mathcal{M})$ be a measurable space, then two singed measures μ, ν on X is called **orthogonal measures** if there is a decomposition $X = E \coprod F, E, F \in \mathcal{M}$ s.t. E is null for μ and F is null for ν. Orthogonal measures are denoted by $\mu \perp \nu$. ⌟

Prop. (11.3.1.9) [Jordan Decompositions]. Let $(X, \mathcal{M})$ be a measurable space and μ a singed measure on X, then there exists a unique positive measures μ^+ and μ^- on X s.t. $\mu = \mu^+ - \mu^-$. Such a decomposition is called the **Jordan decomposition of measure**.

$|\mu| = \mu^+ + \mu^-$ is called the **total variation** of μ. And μ is called finite/σ-finite iff $|\mu|$ is finite/σ-finite. ⌟

Proof: This follows immediately from the Hahn Decomposition Theorem(11.3.1.7). □

Def. (11.3.1.10) [Complex Measure]. A **complex measure** on a measurable space $(X, \mathcal{M})$ is a function $\nu : \mathcal{M} \to \mathbb{C}$ that

- $\nu(\varnothing) = 0$.
- If E_i is a countable family of disjoint sets in $\mathcal{M}$, then $\mu(\cup_{i=1}^\infty E_i) = \sum_{i=1}^\infty \mu(E_i)$, where the series converges absolutely.

⌟

Def. (11.3.1.11) [Lebesgue Space]. A one-point subset with positive measure is called an **atomic measure space**. A **Lebesgue space** is a finite measure space that is isomorphic to a finite union of intervals and countably many atomic measure spaces. ⌟

Borel Measures

Def. (11.3.1.12) [Radon Measure]. For $X \in \mathcal{T}op$, a **Borel measure** on X is a measure defined on the σ-algebra generated by open sets.

A Borel measure μ is called **inner regular** on a Borel set E iff $\mu(E) = \inf\{\mu(K) | K \subset E \text{ compact}\}$ for every Borel set E. It is called **outer regular** iff $\mu(E) = \sup\{\mu(U) | E \subset U \text{ open}\}$.

A **Radon measure** is a Borel measure that is finite on compact set, outer regular on Borel sets, inner regular on open sets. ⌟

Thm. (11.3.1.13) [Borel Isomorphism Theorem]. A Polish space is a second countable, completely metrizable topological space, and a standard Borel subset is a Borel subset of some Polish space. It is equipped with a standard Borel measure.

Then any two standard Borel measurable spaces are isomorphic iff they have the same cardinality. ⌟

Proof: Cf.[AN ELEMENTARY PROOF OF THE BOREL ISOMORPHISM THEOREM]. □

Prop. (11.3.1.14) [Discrete Measures and Continuous Measures]. A complex Borel measure μ on $\mathbb{R}^n$ is called a **discrete measure** if there exists a countable set $\{x_i\} \subset \mathbb{R}^n$ and $c_j \in \mathbb{C}$ s.t. $\sum |c_j| < \infty$, and $\mu = \sum c_j \delta_{x_i}$. And μ is called a **continuous measure** if $\mu(\{x\}) = 0$ for any $x \in \mathbb{R}^n$. ⌟

Prop. (11.3.1.15). Every Radon measure is inner regular on all of its σ-finite sets. ⌟

Proof: Cf.[Folland, Real Analysis, P216]. □

Cor. (11.3.1.16). Every σ-finite Radon measure is regular. In particular, if X is σ-compact, then every Radon measure is regular. ⌟

Measurable Maps

Def. (11.3.1.17) [Measurable Map]. A **measurable map** or a measurable function $f : (X, \mathcal{M}) \to (Y, \mathcal{N})$ between two measurable spaces is a map $f : X \to Y$ that $f^{-1}(E) \in \mathcal{M}$ for any $E \in \mathcal{N}$. ⌟

Def. (11.3.1.18) [Non-Singular Maps]. A **non-singular measurable map** is a measurable map of measure spaces that the preimage of every set of measure0 has measure0. ⌟

Prop. (11.3.1.19) [convergences]. There are three different kinds of convergences:

- **almost everywhere convergence** iff $f_n(x) \to f(x)$ a.e.
- **almost uniform convergence** iff for any $\delta > 0$, there is a measurable subset E_δ that f_n convergent to f uniformly on $E - E_\delta$.
- **convergence in measure** iff $\lim_{k\to\infty} m(\{x \in E || f_n(x) - f(x)| > \varepsilon\}) = 0$.

⌟

Prop. (11.3.1.20) [Relations between Convergences].

- (Egoroff) If $m(E) < \infty$ and f_k converges to f a.e. then f_k converges to f almost uniformly.
- If f_k converges to f almost uniformly, then f_k converges to f in measure.
- (Riesz) If f_k converges to f in measure, then there is a subsequence f_{n_k} that converges to f a.e..

⌟

Proof: 1: Cf.[实变函数周明强 P113].
2: Trivial.
3: Cf.[实变函数周明强 P118]. □

2 Integrations

Def. (11.3.2.1) [Simple Functions]. ⌟

Def. (11.3.2.2) [Integrable Functions]. Let $(X, \mathcal{M})$ be a measurable space. If μ is a measure, **?**

If μ is a singed measure, then define $L^1(\mu) = L^1(|\mu|) = L^1(\mu^+) \cap L^1(\mu^-)$(11.3.1.9). And f is called an **extended integrable function** if either f^+ or f^- is integrable. ⌟

Def. (11.3.2.3) [Locally Integrable Functions]. A measurable function $f : \mathbb{R}^n \to \mathbb{C}$ is called **locally integrable** if $\int_K |f(x)| dx < \infty$ for every bounded measurable set K of $\mathbb{R}$. The set of locally integrable function is denoted by $L^1_{\text{loc}}(\mathbb{R}^n)$. ⌟

Prop. (11.3.2.4). A function f is real analytic on an open set of $\mathbb{R}$ iff there is a extension to a complex analytic function to an open set of $\mathbb{C}$. And this is equivalent to: For every compact subset, there is a constant C that for every positive integer k, $|\frac{d^k f}{dx^k}(x)| \leq C^{k+1}k!$. ⌟

Proof: Use Lagrange residue(中值定理) to show that it will converge to f. □

Prop. (11.3.2.5) [Monotone-convergence-theorem]. ⌟

Prop. (11.3.2.6) [Dominant Convergence Theorem]. ⌟

Prop. (11.3.2.7). The set E of nowhere differentiable functions are of second category in $C[0,1]$, and its complement set is of first category. ⌟

Proof: let A_n be the sets of functions f that there exists a s that for any $|h| \leq 1/n$, $|\frac{f(s+h)-f(s)}{h}| \leq n$. It is easy to see that $C[0,1] - E \subset \cup_n A_n$, so it suffices to show each A_n is of first category.

Firstly A_n is closed, because if $s \notin A_n$, then for any s, there is a $|h_s| \leq 1/n$ that $|f(s+h_s) - f(s)| > n|h_s|$. So by continuity, there is a $\varepsilon_s > 0$ and some nbhd J_s of s that $|f(\sigma - h_s) - f(\sigma)| > n|h_s| + 2\varepsilon_s$ for all $\sigma \in J_s$. Then there are f.m. J_{s_i} that covers $[0,1]$, so let $\varepsilon = \min\{\varepsilon_i\}$, then if $||g - f|| < \varepsilon$, then $g \notin A_n$.

And A_n has no interior point, because for any $f \in A_n$, f can be approximated by a polynomial g, by Stone-Weierstrass theorem(11.3.8.1), and by Mean-value theorem, there is a M that $|g(s+h) - g(s)| \leq M|h|$ for all s and $|h| < 1/n$. So if p is a pairwise-linear function that $||p||$ is small and the slopes of p are bigger than $M + n$, then $g + p$ is near f but $g + p \notin A_n$.

Finally, E is of second category by Baire theorem(4.4.9.2). □

Prop. (11.3.2.8) [Fubini-Tonelli]. For two σ-finite measure spaces X, Y,

- If $f \in L^+(X \times Y)$, then $f_x \in L^+(Y)$ and $f^y \in L^+(X)$, and

$$\int_{X\times Y} f dx dy = \int_Y \int_X f dx dy = \int_X \int_Y f dy dx.$$

- If $f \in L^1(X \times Y)$, then $f_x \in L^1(Y)$ and $f^y \in L^1(X)$, a.e. and the product formula is definable and holds.

⌟

Proof: Cf.[Folland P67]. □

Def. (11.3.2.9) [Lebesgue-Stieltjes Integrals]. ⌟

Prop. (11.3.2.10). ⌟

Prop. (11.3.2.11). Let $(X, \mathcal{M})$ be a measurable space with a positive measure μ, and f is an extended μ-integrable function(11.3.2.2), then we can define a singed measure ν on X by

$$\nu(E) = \int_E f \mathrm{d}\mu, \quad E \in \mathcal{M}.$$

This relation is denoted by $\mathrm{d}\nu = f\mathrm{d}\mu$. It is clear that $\nu \ll \mu$. ⌟

Cor. (11.3.2.12). Let $(X, \mathcal{M})$ be a measurable space with a positive measure μ, and $f \in L^1(\mu)$, then it follows from(11.3.3.2) that: For any $\varepsilon \in \mathbb{R}_+$, there exists $\delta \in \mathbb{R}_+$ s.t. $|\int_E f \mathrm{d}\mu| < \varepsilon$ whenever $\mu(E) < \delta$. ⌟

Miscellaneous

Lemma (11.3.2.13) [Smooth Test Functions]. If $[t_0, t_1] \subset \mathbb{R}$ is an interval and $f \in C([t_0, t_1])$ s.t. $\int_{t_0}^{t_1} f(t)h(t)\mathrm{d}t = 0$ for any $h(t) \in C^\infty([t_0, t_1])$ that $h(t_0) = h(t_1) = 0$, then $f = 0$. ⌟

Proof: Use bump functions as a test function. □

Lemma (11.3.2.14). If $f : \mathbb{R}_{\geq 1} \to \mathbb{R}$ is a non-decreasing function and $\int_1^\infty \frac{f(t)-t}{t^2}\mathrm{d}t$ converges, then $f(x) \sim x, x \to \infty$. ⌟

Proof: Let $F(x) = \int_1^x \frac{f(t)-t}{t^2}\mathrm{d}t$, then the hypothesis implies that for any $\lambda > 1$ and $\varepsilon > 0$, $|F(\lambda x) - F(x)| < \varepsilon$ for x large.

Suppose there exists $\lambda \in \mathbb{R}_{>1}$ and a sequence $(x_n)_{n\in\mathbb{Z}_+}$ s.t. $\lim_{n\to\infty} x_n = \infty$, and $f(x_n) \geq \lambda x_n$ for each n, then

$$F(\lambda x_n) - F(x_n) = \int_{x_n}^{\lambda x_n} \frac{f(t)-t}{t^2}\mathrm{d}t \geq \int_{x_n}^{\lambda x_n} \frac{\lambda x_n - t}{t^2}\mathrm{d}t = \int_1^\lambda \frac{\lambda - t}{t^2}\mathrm{d}t = C$$

where C is a positive constant independent of n. This clearly contradicts the statement above.

A similar statement shows that there are no $\lambda \in \mathbb{R}_{>1}$ and sequences $(x_n)_{n\in\mathbb{Z}_+}$ s.t. $\lim_{n\to\infty} x_n = \infty$, and $f(x_n) \leq \lambda^{-1} x_n$ for each n. So $f(x) \sim x, x \to \infty$. □

Henstock-Kurzweil integrations

Prop. (11.3.2.15). For $f : \mathbb{R} \to \mathbb{C}$, $f \in L^1(m)$ iff both f^+ and f^- are Henstock-Kurzweil integrable. ⌟

Proof: □

Thm. (11.3.2.16). If $a < b \in \mathbb{R}$ and $f : [a, b] \to \mathbb{R}$ is Henstock-Kurzweil integrable and $F(x) = {}^{HK}\int_a^x f(x)\mathrm{d}x$, then

$$F'(x) = f(x).$$

⌟

Proof: □

Thm. (11.3.2.17). If $a < b \in \mathbb{R}$ and $F : [a, b] \to \mathbb{R}$ is differentiable, then

$$F(b) - F(a) = {}^{HK}\int_a^b F'(x)\mathrm{d}x.$$

⌟

3 Differentiations

Absolute Continuity

Def. (11.3.3.1) [Absolutely Continuity]. Let $(X, \mathcal{M})$ be a measurable space with a positive measure μ. A signed measure ν on X is called **absolutely continuous** w.r.t. μ(denoted by $\nu \ll \mu$) if for any $E \in \mathcal{M}$, $\mu(E) = 0 \implies \nu(E) = 0$. ⌟

Prop. (11.3.3.2). Let $(X, \mathcal{M})$ be a measurable space with a positive measure μ, and ν a finite singed measure on X, then $\nu \ll \mu$ iff for any $\varepsilon \in \mathbb{R}_+$, there exists $\delta \in \mathbb{R}_+$ s.t. $|\nu(E)| < \varepsilon$ whenever $\mu(E) < \delta$. ⌟

Proof: Cf.[Folland]P89. □

Lemma (11.3.3.3). Let $(X, \mathcal{M})$ be a measurable space and μ, ν are positive measures on X, then either $\nu \perp \mu$, or there exists $\varepsilon \in \mathbb{R}_+$ and $E \in \mathcal{M}$ s.t. $\mu(E) > 0$, and E is a positive set for $\nu - \varepsilon\mu$. ⌟

Proof: Cf.[Folland]P90. □

Thm. (11.3.3.4) [Lebesgue-Radon-Nikodym]. Let $(X, \mathcal{M})$ be a measurable space and μ is positive σ-finite measures on X. Then for any σ-finite signed measures ν on X, there exists unique σ-finite signed measure λ, ρ on X s.t.

$$\lambda \perp \mu, \quad \rho \ll \mu, \quad \nu = \lambda + \rho.$$

.

Moreover, there exists an extended μ-integrable function $f : X \to \mathbb{R}$ s.t. $\mathrm{d}\rho = f\mathrm{d}\mu$, and f is determined a.e. w.r.t. μ. Such f is called the **Radon-Nikodym derivative** of ρ s.t. μ, and denoted by $\mathrm{d}\rho/\mathrm{d}\mu$.

The same is true for complex measures. ⌟

Proof: This is a special case of the Freudenthal Spectral Theorem(11.9.4.18). Cf.[Folland]P90. □

Prop. (11.3.3.5) [Total Variation of Complex Measures]. Cf.[Folland]P93. ⌟

Differentiation on Euclidean Spaces

Lemma (11.3.3.6) [Vitali Covering Theorem]. Let $\mathcal{C}$ be a collection of balls in $\mathbb{R}^n$, and let $U = \cup_{B\in\mathcal{C}} B$. Then if $c > m(U)$, then there exists disjoint $B_1, \ldots, B_k \in \mathcal{C}$ that $\sum_{i=1}^k m(B_k) > 3^{-n}c$. ⌟

Proof: □

Lemma (11.3.3.7). If $f \in L^1_{\mathrm{loc}}$ and $A_r f(x) = \frac{1}{\mathrm{Vol}(B(r,x))}\int_{B(r,x)} f(y)dy$, then $A_r f$ is continuous in both r and x. ⌟

Proof: Cf.[Folland P96]. □

Prop. (11.3.3.8). If $f \in L^1_{\mathrm{loc}}$, then $\lim_{r\to 0} A_r f(x) = f(x)$ for a.e. $x \in \mathbb{R}^n$. ⌟

Proof: Cf.[Folland P97]. □

Prop. (11.3.3.9) [Fermat]. Let $x_0 \in \mathbb{R}, \delta \in \mathbb{R}_+, f$ is a function on $U(x_0, \delta)$. If x_0 is an extreme point of f, and $f'(x_0)$ exists, then $f'(x_0) = 0$. ⌟

Proof: By changing f to $-f$ if necessary, we can assume x_0 is a supremum point. Then for $0 < h < \delta$, $\frac{f(x_0+h)-f(x_0)}{h} \le 0$, and for $-\delta < h < 0$, $\frac{f(x_0+h)-f(x_0)}{h} \ge 0$, so $f'(x) = 0$. □

Lemma (11.3.3.10) [Rolle's Mean Value Theorem]. If $a < b \in \mathbb{R}$, $f \in C([a, b])$ is differentiable on $[a, b]$, and $f(a) = f(b)$, then there exists some $\xi \in (a, b)$ s.t. $f'(\xi) = 0$. ⌟

Proof: As f is continuous on $[a, b]$, which is compact, f has minimum m and maximum M on $[a, b]$. If $m = M$, then f is constant, and any $\xi \in (a, b)$ will do. If $M > m$, then $M \ne f(a)$ or $m \ne f(a)$. Suppose WLOG the first case happens, then if $f(\xi) = M, \xi \in (a, b)$, then $f'(\xi) = 0$ by Fermat's theorem(11.3.3.9). □

Thm. (11.3.3.11) [Lagrange's Mean Value Theorem]. If $a < b \in \mathbb{R}$, $f \in C([a,b])$ is differentiable on $[a,b]$, then there exists some $\xi \in (a,b)$ s.t. $f^\backprime(\xi) = \frac{f(b)-f(a)}{b-a}$. ⌟

Proof: This follows from Rolle's mean value theorem by considering the function

$$F(x) = f(x) - [f(a) + \frac{f(b)-f(a)}{b-a}(x-a)].$$

□

Cor. (11.3.3.12) [Cauchy's Mean Value Theorem]. If $a < b \in \mathbb{R}$, $f, g \in C([a,b])$ is differentiable on $[a,b]$, and $g^\backprime \neq 0$. then there exists some $\xi \in (a,b)$ s.t. $\frac{f(b)-f(a)}{g(b)-g(a)} = \frac{f^\backprime(\xi)}{g^\backprime(\xi)}$. ⌟

Proof: This follows from Rolle's mean value theorem by considering the function

$$G(x) = f(x) - [f(a) + \frac{f(b)-f(a)}{g(b)-g(a)}(g(x)-g(a))].$$

□

Cor. (11.3.3.13) [Integral Mean Value Theorem]. For $a < b \in \mathbb{R}, f, g \in C([a,b])$, there exists $\xi \in (a,b)$ s.t.

$$\int_a^b f(t)g(t)\mathrm{d}t = f(\xi)\int_a^b g(t).$$

⌟

Proof: Consider

$$H(x) = \int_a^x f(t)g(t)\mathrm{d}t, \quad G(t) = \int_a^x g(t)\mathrm{d}t,$$

then it follows from Cauchy's mean value theorem(11.3.3.12) that there exists $\xi \in (a,b)$ s.t.

$$\frac{H(b)-H(a)}{G(b)-G(a)} = \frac{\int_a^b f(t)g(t)\mathrm{d}t}{\int_a^b g(t)\mathrm{d}t} = \frac{H^\backprime(\xi)}{G^\backprime(\xi)} = f(\xi).$$

□

Prop. (11.3.3.14) [Commutativity of Integration]. Let $n \in \mathbb{Z}_+, n \geq 2, \Omega \subset \mathbb{R}^n$ be open and $f \in C(\Omega)$. If $1 \leq j < k \leq n$ and $\frac{\partial}{\partial x_j}\frac{\partial}{\partial x_k}f, \frac{\partial}{\partial x_k}\frac{\partial}{\partial x_j}f$ exist and continuous on Ω, then

$$\frac{\partial}{\partial x_j}\frac{\partial}{\partial x_k}f = \frac{\partial}{\partial x_k}\frac{\partial}{\partial x_j}f.$$

In particular, this holds for $f \in C^2(\Omega)$. ⌟

Proof: For simplicity we prove for $n = 2, i = 1, j = 2$, and the general case is verbatim. For $\mathbf{x} = (x,y) \in \Omega$, if $\Delta x, \Delta y$ is sufficiently small, define

$$I(\Delta x, \Delta y) = \frac{f(x_0+\Delta x, y_0+\Delta y) - f(x_0+\Delta x, y_0)}{\Delta x \Delta y} - \frac{f(x_0, y_0+\Delta y) - f(x_0, y_0)}{\Delta x \Delta y}$$

and

$$g(x) = f(x, y_0+\Delta y) - f(x, y_0), \quad h(y) = f(x_0+\Delta x, y) - f(x_0, y).$$

Then by mean value theorem(11.3.3.11),

$$\begin{aligned}I(\Delta x,\Delta y)&=\frac{g(x_0+\Delta x)-g(x_0)}{\Delta x\Delta y}\\&=\frac{g`(x_0+\theta_1\Delta x)}{\Delta y}\\&=\frac{\frac{\partial}{\partial x}f(x_0+\theta_1\Delta x,y_0+\Delta y)-\frac{\partial}{\partial x}f(x_0+\theta_1\Delta x,y_0)}{\Delta y}\\&=\frac{\partial}{\partial y}\frac{\partial}{\partial x}f(x_0+\theta_1\Delta x,y_0+\theta_2\Delta y)\end{aligned}$$

where $\theta_1,\theta_2\in[0,1]$, and

$$\begin{aligned}I(\Delta x,\Delta y)&=\frac{h(y_0+\Delta y)-h(y_0)}{\Delta x\Delta y}\\&=\frac{h`(y_0+\theta_3\Delta y)}{\Delta x}\\&=\frac{\frac{\partial}{\partial y}f(x_0+\Delta x,y_0+\theta_3\Delta y)-\frac{\partial}{\partial x}f(x_0,y_0+\theta_3\Delta y)}{\Delta x}\\&=\frac{\partial}{\partial x}\frac{\partial}{\partial y}f(x_0+\theta_4\Delta x,y_0+\theta_3\Delta y)\end{aligned}$$

where $\theta_3,\theta_4\in[0,1]$. Then we get

$$\frac{\partial}{\partial y}\frac{\partial}{\partial x}f(x_0+\theta_1\Delta x,y_0+\theta_2\Delta y)=\frac{\partial}{\partial x}\frac{\partial}{\partial y}f(x_0+\theta_4\Delta x,y_0+\theta_3\Delta y).$$

Now let $\Delta x,\Delta y\to 0$ and use the fact $\frac{\partial}{\partial x_j}\frac{\partial}{\partial x_k}f,\frac{\partial}{\partial x_k}\frac{\partial}{\partial x_j}f$ are continuous to finish the proof. □

Thm. (11.3.3.15) [Taylor's Expansion with Integral Remainder]. Let $n\in\mathbb{Z}_+,k\in\mathbb{N},f\in C^{k+1}(\mathbb{R}^n)$, then for $\underline{x}\in\mathbb{R}^n$,

$$f(\underline{x})=\sum_{j=0}^k\frac{1}{j!}\Big((\sum_i x_iD^i)^jf\Big)(0)+\int_0^1\frac{(1-t)^k}{k!}\Big((\sum_i x_iD^i)^{k+1}f\Big)(t\underline{x})\mathrm{d}.$$

Equivalently,

$$f(\underline{x})=\sum_{|\alpha|\le k}D^\alpha f(0)\frac{\underline{x}^\alpha}{\alpha!}+(k+1)\sum_{|\alpha|=k+1}\Big(\int_0^1(1-t)^kD^\alpha f(t\underline{x})\mathrm{d}t\Big)\frac{\underline{x}^\alpha}{\alpha!}.$$

⌟

Proof: Consider the function $\varphi(u)=f(u\underline{x}),u\in\mathbb{R}$, it is reduced to the $n=1$ case. Thus it suffices to prove that

$$f(x)-\sum_{j=0}^kf^{(i)}(0)\frac{x^j}{j!}=\int_0^1(1-t)^k\frac{x^{k+1}}{k!}f^{(k+1)}(tx)\mathrm{d}t=\int_0^x\frac{(x-t)^k}{k!}f^{(k+1)}(t)\mathrm{d}t.$$

Use induction on k: For $k=0$, this is just the fundamental theorem of calculus. In general, it suffices to notice that if $f\in C^{k+2}(\mathbb{R}^n)$,

$$\int_0^x \frac{(x-t)^k}{k!} f^{(k+1)}(t)\mathrm{d}t = \Big(-\frac{(x-t)^{k+1}}{(k+1)!} f^{(k+1)}(t)\Big)\Big|_0^x + \int_0^x \frac{(x-t)^{k+1}}{(k+1)!} f^{(k+2)}(t)\mathrm{d}t$$
$$= f^{(k+1)}(0)\frac{x^{k+1}}{(k+1)!} + \int_0^x \frac{(x-t)^{k+1}}{(k+1)!} f^{(k+2)}(t)\mathrm{d}t.$$

□

Cor. (11.3.3.16) [Taylor's Expansion with Lagrangian Remainder]. Let $n\in\mathbb{Z}_+, k\in\mathbb{N}, f\in C^{k+1}(\mathbb{R}^n)$, then for $\underline{x}\in\mathbb{R}^n$,

$$f(\underline{x}) = \sum_{j=0}^k \Big((\sum_i x_i D^i)^j f\Big)(0)\frac{x^j}{j!} + \frac{1}{(k+1)!}\Big((\sum_i x_i D^i)^{k+1} f\Big)(\theta\underline{x})$$

for some $\theta\in(0,1)$. ⌟

Proof: It follows from(11.3.3.15) and the integral mean value theorem(11.3.3.13) that there exists some $\theta\in(0,1)$ s.t.

$$f(\underline{x}) - \sum_{|\alpha|\le k} D^\alpha f(0)\frac{\underline{x}^\alpha}{\alpha!} = \int_0^1 \frac{(1-t)^k}{k!}\Big((\sum_i x_i D^i)^{k+1} f\Big)(t\underline{x})\mathrm{d}t$$
$$= \Big((\sum_i x_i D^i)^{k+1} f\Big)(\theta\underline{x})\int_0^1 \frac{(1-t)^k}{k!}\mathrm{d}t$$
$$= \frac{1}{(k+1)!}\Big((\sum_i x_i D^i)^{k+1} f\Big)(\theta\underline{x})$$

□

Cor. (11.3.3.17)[Taylor's Expansion with Peano Remainder]. Let $n\in\mathbb{Z}_+, k\in\mathbb{N}, f\in C^{k+1}(\mathbb{R}^n)$, then for $\underline{x}\in\mathbb{R}^n$,

$$f(\underline{x}) = \sum_{j=0}^k \Big((\sum_i x_i D^i)^j f\Big)(0)\frac{x^j}{j!} + o(|\underline{x}|^k)$$

for some $\theta\in(0,1)$. ⌟

Proof: This follows from(11.3.3.16) and the continuity(thus local boundedness) of the derivatives of f. □

Functions of Bounded Variation

Prop. (11.3.3.18) [Bounded Variations]. For a function $F:\mathbb{R}\to\mathbb{C}$, define the **totally variation function** of F:

$$T_F:\mathbb{R}\to\mathbb{R}_{\ge0}: T_F(x) = \sup\{\sum_{j=1}^n |F(x_j)-F(x_{j-1})| : n\in\mathbb{N}, -\infty < x_0 < x_1 < \ldots < x_n = x\}.$$

Then T_F is a non-decreasing function, and for $a < b \in \mathbb{R}$,

$$T_F(b) - T_F(a) = \sup\{\sum_{j=1}^n |F(x_j) - F(x_{j-1})| : n \in \mathbb{N}, a = x_0 < x_1 < \ldots < x_n = x\}.$$

Then F is called a **function of bounded variation** if $T_F(\infty) = \lim_{x\to\infty} T_F(x) < \infty$. The space of functions of bounded variation is denoted by $\mathrm{BV}(\mathbb{R})$.

Similarly we can define the totally variation function for a function $F : [a, b] \to \mathbb{C}$, where $a < b \in \mathbb{R}$, by regarding it as a function on $\mathbb{R}$ s.t. $F(x) = F(a)$ if $x < a$ and $F(x) = F(b)$ if $x > b$. So we can define $\mathrm{BV}([a, b])$. ⌟

Prop. (11.3.3.19) [Properties of Bounded Variations].

- $F \in \mathrm{BV}(\mathbb{R})$ iff $\mathrm{Re}\, F, \mathrm{Im}\, F \in \mathrm{BV}(\mathbb{R})$.
- For $F : \mathbb{R} \to \mathbb{R}$, $F \in \mathrm{BV}$ iff F is the difference of two bounded non-decreasing functions. And if this is the case, then these functions can be chosen to be $\frac{1}{2}(T_F + F)$ and $\frac{1}{2}(T_F - F)$, which is called the **Jordan decomposition** of F.
- If $F \in \mathrm{BV}(\mathbb{R})$, then $F(x-), F(x+)$ exists for any $x \in \mathbb{R}$. And also $F(\pm\infty)$ exist.
- If $F \in \mathrm{BV}(\mathbb{R})$, then F has at most countably many discontinuous points.
- If $F \in \mathrm{BV}(\mathbb{R})$ and $G(x) = F(x+)$, then F' and G' exist, and they are equal.

⌟

Proof: Cf.[Folland]P103. □

Def. (11.3.3.20) [Normalized Bounded Variations]. The space NBV of **normalized bounded variation functions** consists of functions $F \in \mathrm{BV}(\mathbb{R})$ s.t. $F(-\infty) = 0$ and F is right-continuous. ⌟

Prop. (11.3.3.21) [Bounded Variations and Measures]. If μ is a complex Borel measure on $\mathbb{R}$, and $F(x) = \mu((-\infty, x])$ for any $x \in \mathbb{R}$, then $F \in \mathrm{NBV}$. Conversely, if $F \in \mathrm{NBV}$, then there exists a unique complex Borel measure μ_F on $\mathbb{R}$ s.t. $F(x) = \mu_F((-\infty, x])$. Moreover, $|\mu_F| = \mu_{T_F}$. ⌟

Proof: Cf.[Folland]P104. □

Def. (11.3.3.22) [Absolute Continuity]. For $a < b \in [-\infty, \infty]$, $f \in C([a, b])$ is called **absolutely continuous** on $[a, b]$ if for any $\varepsilon > 0$, there exists $\delta < 0$ s.t. for any f.m. disjoint intervals $(a_i, b_i), i \leq N$,

$$\sum_{i=1}^N (b_i - a_i) < \delta \implies \sum_{i=1}^N |F(b_i) - F(a_i)| < \varepsilon.$$

⌟

Prop. (11.3.3.23). For $F \in \mathrm{NBV}$, F is absolutely continuous iff $\mu_F \ll \mathrm{m}$(11.3.3.21). ⌟

Proof: Cf.[Folland]P105. □

Prop. (11.3.3.24). For $a < b \in [-\infty, \infty]$, $f \in C([a, b])$ is differentiable and F' is bounded, then F is absolutely continuous. ⌟

Proof: This follows from the fact $|F(b_i) - F(a_i)| \leq (\sup |F'|)|b_i - a_i|$ by mean value theorem(11.3.3.11). □

Thm. (11.3.3.25) [Fundamental Theorem of Calculus for Lebesgue Measure]. If $a < b \in \mathbb{R}$ and $F \in C([a,b])$, then the following are equivalent:

- F is absolutely continuous on $[a,b]$.
- $F(x) - F(a) = \int_a^x f(t)\mathrm{d}t$ for some $f \in L^1([a,b],m)$.
- F is differentiable a.e. on $[a,b]$, $F' \in L^1([a,b],m)$, and $F(x) - F(a) = \int_a^x F'(t)dt$.

In particular, this is the case for F everywhere differentiable and F' bounded, by(11.3.3.24). ⌟

Proof: Cf.[Fol99]P106. □

Def. (11.3.3.26) [Lebesgue-Stieltjes Integral]. For $F \in$ NBV and any good function $G : \mathbb{R} \to \mathbb{C}$, denote $\int g\mathrm{d}\mu_F$ by $\int g\mathrm{d}F$, which is called the **Lebesgue-Stieltjes integral**. ⌟

Thm. (11.3.3.27) [Integration by Parts]. If $F, G \in$ NBV and at least one of them is continuous, then for $a < b \in \mathbb{R}$,

$$\int_{(a,b]} F\mathrm{d}G + \int_{(a,b]} G\mathrm{d}F = F(b)G(b) - F(a)G(a).$$

⌟

Proof: Cf.[Fol99]P107. □

4 Smooth Functions

Thm. (11.3.4.1) [Implicit Function Theorem]. ⌟

5 Series

Lemma (11.3.5.1). For a sequence $(a_n)_{n\in\mathbb{N}}$ in $\mathbb{R}_+$,

$$\varliminf_{n\to\infty} \frac{a_{n+1}}{a_n} \le \varliminf_{n\to\infty} a_n^{1/n} \le \varlimsup_{n\to\infty} a_n^{1/n} \le \varlimsup_{n\to\infty} \frac{a_{n+1}}{a_n}$$

⌟

Proof: Let $\varliminf_{n\to\infty} a_n^{1/n} = R$. If $R > 0$, then by definition, for any $\varepsilon > 0$ and $M \in \mathbb{Z}_+$, there exists some $m \ge M$ s.t. $a_m^{1/m} < R + \varepsilon$. Then for such M, $a_m/a_1 \le (R+\varepsilon)^m/a_1$. So for some $k \le m$, $a_k/a_{k-1} \le ((R+\varepsilon)^m/a_1)^{m-1}$. Then if M is very large, $a_k/a_{k-1} < R + 2\varepsilon$. Thus $\varliminf_{n\to\infty} \frac{a_{n+1}}{a_n} \le R$.

Then $\varlimsup_{n\to\infty} a_n^{1/n} \le \varlimsup_{n\to\infty} \frac{a_{n+1}}{a_n}$ follows from this by considering the sequence $b_n = a_n^{-1}$. The other inequality is trivial. □

Def. (11.3.5.2) [Euler's Constant]. The limit

$$\lim_{N\to\infty} \Big[\sum_{n=1}^N \frac{1}{n} - \log N\Big]$$

exists, and is denoted by γ, called the **Euler's constant**. ⌟

Proof: As

$$\sum_{n=1}^N \frac{1}{n} - \log N = \sum_{n=1}^{N-1} \int_n^{n+1} [\frac{1}{n} - \frac{1}{x}]\mathrm{d}x,$$

this sequence is increasing. And

$$\sum_{n=1}^{N-1} \int_n^{n+1} [\frac{1}{n} - \frac{1}{x}]\mathrm{d}x + \frac{1}{N} < \sum_{n=1}^{N-1} \frac{1}{n(n+1)} + \frac{1}{N} = 1,$$

so it converges. □

Power Series

Prop. (11.3.5.3) [Cauchy-Hadamard]. For any power series $a_0 + a_1x + \ldots + a_nx^n + \ldots$ in $\mathbb{R}$, take $1/R = \overline{\lim}\,|a_n|^{1/n}$, where we assume $1/0 = \infty$ and $1/\infty = 0$, then

- The series converges absolutely for every $|x| < R$, and if $\rho < R$, then the convergence is uniform for $|x| \leq \rho$.
- If $|x| > R$, the terms are unbounded, and the series diverges.

And R is called the **radius of convergence** of the sequence. ⌟

Proof: 1: For $0 < \rho < R$, take $\rho_1 \in (\rho, R)$, then the definition of R implies that for some $N \in \mathbb{Z}_+$ and any $n \geq N$, $|a_n| \leq R^{-n} < \rho_1^{-n}$, so $|a_nx^n| \leq (\rho/\rho_1)^n$, so $\sum_{n\in\mathbb{N}} a_nx^n$ converges absolutely and uniformly for $|x| \leq \rho$.

2: For $R < |x|$, the definition of R implies that for any $N \in \mathbb{Z}_+$, there exists $n \geq N$ s.t. $|a_n| \geq R^{-n}$, so $|a_nx^n| \geq |x/R|^n > 1$, so this sequence cannot be convergent. □

Prop. (11.3.5.4). For any power series $a_0+a_1x+\ldots+a_nx^n+\ldots$ in $\mathbb{R}$, by(11.3.5.1), if $\lim_{n\to\infty} |\frac{a_{n+1}}{a_n}| = \rho \in [0, \infty]$, then the radius of convergence(11.4.3.1) $R = 1/\rho$, where we assume $1/0 = \infty$ and $1/\infty = 0$. ⌟

Divergent Series

Prop. (11.3.5.5) [Borel Summation]. Suppose $\sum_{n\in\mathbb{N}} a_nx^n$ is a power series with zero radius of convergent, and suppose that the **exponential generating function**

$$g(x) = \sum_{n\in\mathbb{N}} a_n \frac{x^n}{n!}$$

is convergent on some nbhd of 0, and analytically extends to a smooth function on $[0, \infty)$, and satisfies that $g(x) = O(x^N)$.

Then we can define a **Borel summation** of this power series as

$$I(x) = \int_0^\infty g(xu)e^{-u}\mathrm{d}u = x^{-1}\int_0^\infty g(u)e^{-\frac{u}{x}}\mathrm{d}u = x^{-1}(\mathcal{L}g)(x^{-1})\text{(11.11.2.17)}.$$

Then $I(x)$ is convergent on $[0, \frac{1}{N})$, and has the Taylor expansion $\sum_{n\in\mathbb{N}} a_nx^n$ at the origin. ⌟

Proof: Take derivatives, and notice that for $n \in \mathbb{N}$, $\int_0^\infty x^ne^{-x}\mathrm{d}x = n!$. □

Example (11.3.5.6). Consider the power series

$$\sum_{n\in\mathbb{N}} (-1)^n n! x^n,$$

then $g(x) = \sum_{n\in\mathbb{N}}(-1)^nx^n = \frac{1}{1+x}$, so

$$I(x) = \int_0^\infty \frac{e^{-u}}{1+xu}\mathrm{d}u = x^{-1}e^{1/x}E_1(\frac{1}{x}),$$

where $E_1(x) = \int_x^\infty \frac{e^{-u}}{u}\mathrm{d}u$ is the integral exponential. ⌟

6 L^p-spaces

Lemma (11.3.6.1) [Hölder]. if $\sum x_i = 1, x_i \geq 0$, then for any $a_i \geq 0$

$$\prod a_i^{x_i} \leq \sum a_i x_i.$$

⌟

Proof: □

Thm. (11.3.6.2) [Hölder-Cauchy-Bunyakovsky-Schwarz Inequality]. Let X be a measure space, and $1 \leq p, q \leq \infty$ satisfies $1/p + 1/q = 1$, then

$$||fg||_1 \leq ||f||_p ||g||_q$$

More generally, if $\sum_{i=1}^n 1/p_i = 1$, then

$$||\prod f_i||_1 \leq \prod ||f_i||_{p_i}$$

⌟

Proof: The both sides are homogenous for f_i, so we may assume $||f_i||_{p^i} = 1$, then use Hoder's Lemma(11.3.6.1) for $x_i = q/p_i$. □

Prop. (11.3.6.3) [Dual of $L^p(\mu)$]. For a σ-finite measurable space $(X, \mathcal{M}, \mu)$, for $1 \leq p < \infty$

$$L^p(X, \Omega, \mu)^* = L^q(X, \Omega, \mu).$$

⌟

Proof: Firstly, Holder inequality(11.3.6.2) shows that a $g \in L^q(X, \Omega, \mu)$defines a functional by $f \mapsto \int fg d\mu$. Conversely, if given a functional F, define a measure $v(E) = F(\chi_E)$ for all measurable set $E \in \Omega$. It is countably additive: first it is finitely additive, and if E_n is a descending sequence of measurable sets that $\cap E_n = \varnothing$, then

$$v(E_n) \leq ||F|| ||\chi_{E_n}||_{L^p} = ||F|| \mu(E_n)^{\frac{1}{p}} \to 0.$$

(where we used the fact $p < \infty$). And it is clearly absolutely continuous w.r.t. μ.

So by Radon-Nikodym(11.3.3.4), there is a measurable function g that $v(E) = \int_E g d\mu$. So for all simple function f, $F(f) = \int f(x) g(x)$. Next we want to prove $||g||_q \leq ||F||$, because any measurable function f can be approximated by simple functions f_i in L^p norm(11.3.8.5), so

$$|\int (f(x) - f_i(x)) g(x) d\mu| \leq ||f - f_i||_p ||g||_q \leq ||f - f_i||_p ||g||_q$$

So $F(f) = \lim F(f_i) = \lim \int f_i g d\mu = \int fg d\mu$.

To prove this, if $1 < p$, then let $E_t = \{x | |g(x)| \leq t\}$, and $f = \chi_{E_t} |g|^{q-2} g$, then

$$\int_{E_t} |g|^q d\mu = \int fg d\mu = F(f) \leq ||F|| ||f||_{L^p} = ||F|| (\int_{E_t} |g|^q d\mu)^{\frac{1}{p}}$$

which is equivalent to $||g \chi E_t||_{L^q} \leq ||F||$. Let $t \to \infty$, then the monotone convergence theorem(11.3.2.5) gives us the result.

If $p = 1$, then $q = \infty$. For any $\varepsilon > 0$, let $A = \{x | |g(x)| > ||F|| + \varepsilon\}, E_t = \{x | |g(x)| \leq t\}$, and let $f = \chi_{E_t \cap A} \operatorname{sgn}(g)$, then $||f||_{L^1} = \mu(E_t \cap A)$, and

$$\mu(E_t \cap A)(||F|| + \varepsilon) \leq \int_{A \cap E_t} |g| d\mu = \int fg d\mu \leq ||F|| \mu(E_t \cap A)$$

If $\mu(A) \neq 0$, then let $t \to \infty$, this is a contradiction. So $||g||_\infty \leq ||F||$. □

Prop. (11.3.6.4) [Hilbert Basis for Products]. For two σ-finite measure spaces M, N and Hilbert basis(11.7.4.9) $\{e_i\}$ of $L^2(M)$ and $\{f_j\}$ of $L^2(N)$, $\{e_i \otimes f_j\}$ gives a Hilbert basis for $L^2(M\times N)$. (Use Fubini). ┘

Proof: It is easily verified that $e_i\otimes f_j$ are mutually orthogonal, and if some $f\in L^2(M\times N)$ satisfies $(f, e_i\otimes f_j)=0$ for all i,j, then

$$\int_M e_i(x)\int_N f(x,y)f_j(y)=0$$

for all i. But $\int_N f(x,y)f_j(y)\in L^2(M)$ for a.e. $x(f(x,y)\in L^2(N)$ a.e. x by Fubini-Tonelli), thus it vanishes. So $f_x(y)=f(x,y)=0\in L^2(N)$ for a.e. x, so by Fubini-Tonelli again, $||f||_{L^2(M\times N)}=0$, thus $f=0$. □

Prop. (11.3.6.5) [Minkowski's Inequality]. Let $(X,\mathcal{M},\mu),(Y,\mathcal{N},\nu)$ be σ-finite measure spaces, and f a $(\mathcal{M}\otimes\mathcal{N})$-measurable function on $X\times Y$.

- If $f\geq 0$ and $1\leq p<\infty$, then

$$[\int(\int f(x,y)d\nu(y))^p d\mu(x)]^{1/p}\leq \int[\int f(x,y)^p d\mu(x)]^{1/p}d\nu(y).$$

- If $1\leq p\leq\infty$, $f(\cdot,y)\in L^p(\mu)$ for a.e. y, and the function $y\mapsto ||f(\cdot,y)||_p$ is in $L^1(\nu)$, then $f(x,\cdot)\in L^1(\nu)$ for a.e. x, and the function $x\mapsto\int f(x,y)d\nu(y)$ is in $L^p(\mu)$, and

$$||\int f(\cdot,y)d\nu(y)||_p\leq\int ||f(\cdot,y)||_p d\nu(y).$$

┘

Proof: 1: If $p=1$, then this is just Tonelli's theorem(11.3.2.8), and when $1<p<\infty$, let $q^{-1}+p^{-1}=1$, and $g\in L^q(\mu)$, then by Tonelli's theorem and Holder's inequality(11.3.6.2),

$$\int[\int f(x,y)d\nu(y)]|g(x)|d\mu(x)=\int\int f(x,y)|g(x)|d\mu(x)d\nu(y)\leq ||g||_q\int[f(x,y)^p d\nu(y)]^{1/p}d\nu(y).$$

So we finish by(11.3.6.3).

2 follows from 1 and Fubini's theorem. And when $p=\infty$, this is trivial. □

L^2-Space

Def. (11.3.6.6). Let X be a measure space, then there is a map

$$\star: L^2(X\times X)\times L^2(X\times X)\to L^2(X\times X):(K_1\star K_2)(u,v)=\int_X K_1(u,x)K_2(x,v)dx.$$

By Schwarz inequality, $||K_1\star K_2||_2\leq ||K_1||_2\star||K_2||_2$, thus $\star$ makes $L^2(G\times G)$ into a Banach algebra(without a unit).

This Banach algebra can left and right act on $L^2(X)$, also denoted by $\star$, then for $K\in L^2(X\times X), P,Q\in L^2(X)$,

$$(P\otimes Q)\star K=P\otimes(Q\star K),\quad K\star(P\otimes Q)=(K\star P)\otimes Q.$$

And also for $S,T\in L^2(X)$,

$$(P\otimes Q)\star(\overline{S}\otimes T)=(Q,S)_{L^2}P\otimes T.$$

┘

Prop. (11.3.6.7).

- An element $K \in L^2(X \times X)$ has the form $P \otimes Q$ iff $K \star K' \star K$ is proportional to K for all $K' \in L^2(X \times X)$.
- Let $K_1 = P_1 \otimes Q_1$ and $K_2 = P_2 \otimes Q_2$, then P_1 and P_2 are proportional iff $K_1 \star K$ and $K_2 \star K$ are proportional for all pure tensors $K \in L^2(X \times X)$. Similarly, Q_1 and Q_2 are proportional iff $K \star K_1$ and $K \star K_2$ are proportional for all pure tensor K.
- For any uniform transformation $s : L^2(X \times X) \to L^2(X \times X)$ respecting $\star$, there exists a unitary transformation $s_0 : L^2(X) \to L^2(X)$ s.t. $s(P \otimes \overline{Q}) = s_0(P) \otimes \overline{s_0(Q)}$. And it can be chosen to be invertible iff s is.

⌟

Proof: Cf.[Bump, P527].? □

L^∞-Spaces

Def. (11.3.6.8)[Slowly Oscillating Functions]. A **slowly oscillating function** on $\mathbb{R}^n$ is a function $f \in L^\infty(\mathbb{R}^n)$ s.t. for any $\varepsilon \in \mathbb{R}_+$, there exists $A, \delta \in \mathbb{R}_+$ s.t. $|f(x) - f(y)| < \varepsilon$ whenever $|x| > A, |y| > A, |x - y| < \delta$. ⌟

7 Estimations

Prop. (11.3.7.1). $\lim_{n\to\infty} n^{1/n} = 1$. ⌟

Proof: Let $n^{1/n} = 1 + \delta_n, \delta_n > 0$, then $n = (1 + \delta_n)^n \geq 1 + \frac{n(n-1)}{2}\delta_n^2$, so $\delta_n \leq \sqrt{2/n}$, and $\lim_{n\to\infty} \delta_n = 0$. □

Prop. (11.3.7.2). For any $x \in (0, \frac{\pi}{2})$, $\frac{2}{\pi}x < \sin x < x$. ⌟

Proof: it suffices to show that $\frac{\sin x}{x}$ is decreasing on $x \in (0, \frac{\pi}{2})$:

$$(\frac{\sin x}{x})' = \frac{x\cos x - \sin x}{x},$$

and $x\cos x - \sin x < 0$ because

$$(x\cos x - \sin x)' = -x\sin x < 0.$$

□

8 Approximations

Prop. (11.3.8.1) [Stone-Weierstrass Approximation]. Let X be a compact Hausdorff space, and A is a a unital *-subalgebra of $C(X)$ that separates points, then A is dense in $C(X)$. ⌟

Proof: This is a consequence of Bishop theorem(11.8.3.18) because in this case the real functions in A separate points, so all A-antisymmetric sets consists of one point. □

Cor. (11.3.8.2). The set of Polynomial functions are dense in $C([0,1]^n)$ for any $n \in \mathbb{Z}_+$. ⌟

Cor. (11.3.8.3). The set of trigonometric polynomials are dense in $\mathbb{C}([0,1]^n)$ for any $n \in \mathbb{Z}_+$. ⌟

Prop. (11.3.8.4) [Simple Function Approximation]. Let E be a measure space,

- If $f(x)$ is a non-negative measurable function on E, then there is an ascending sequence of simple functions $(\varphi_n(x))$ that converges to f point-wise.
- If $f(x)$ is a measurable function on E, then there is a sequence of simple functions φ_n that $|\varphi_k(x)| \leq |f(x)|$, and converges to f pointwise.
- If $f(x)$ is bounded, then the convergence can be chosen to be uniform.

⌟

Proof: Cf.[实变函数周明强 P110]. □

<u>**L^p-Approximation**</u>

Prop. (11.3.8.5) [Simple Function Approximation]. Any function in L^p can be approximated by compactly supported simple functions in L^p norm. ⌟

Proof: □

Prop. (11.3.8.6). for $1 \leq p < +\infty$, $C_c(X)$ are dense in $L^p(X)$ for a Radon measure, but not for $p = \infty$. ⌟

Proof: Use compactly supported simple function approximation(11.3.8.5) and then use outer regular approximation(11.3.1.12) and then Tietz extension. □

Prop. (11.3.8.7) [Lusin]. If f is almost everywhere finite on E, then for any $\delta > 0$, there is a closed subset $F \subset E$ that f is continuous function on F. ⌟

Proof: First if f is a simple function $f = \sum_{i=1}^n c_i\chi_{E_i}$, then for each E_i, choose a closed subset $F_i \subset E_i$ that $m(E_i - F_i) < \frac{\delta}{n}$, and then $\cup F_i$ satisfies the required condition.

Now if f is arbitrary, let $g(x) = \frac{f(x)}{1+|f(x)|}$ to make it bounded, then by(11.3.8.4), there is a sequence of simple functions φ_k converging to f, and for each k, we choose a closed subset F_k that $m(E - F_k) < \frac{\delta}{2^k}$, so if we let $F = \cap F_k$, then φ_k are all continuous on F, so by the uniform convergence, f is also continuous on F. □

Cor. (11.3.8.8). If f is measurable function on E that is a.e. finite, then for any δ, there is a continuous function g that $m(\{x \in E | f(x) \neq g(x)\}) < \delta$. And if E is bounded, g can be chosen to be compactly supported. ⌟

Proof: Now that there is a closed subset F that $m(E - F) < \delta$ and f is continuous on F, we can use Tietze extension(4.4.6.4), there is a function g that equals f on F.

If $E \subset B(0, R)$, the we can choose a bump function to multiply with g. □

Prop. (11.3.8.9). for $1 \leq p < +\infty$, trigonometric polynomials are dense in $L^p(\mathbb{T})$ and $C(\mathbb{T})$, but not for $p = \infty$. So $e^{2\pi inx}$ forms an orthogonal basis in $L^2(\mathbb{T})$.

Thus, the Parseval's identity holds. ⌟

Proof: Just use the fact that Fejer kernels are an approximate identity. □

Prop. (11.3.8.10). For a integrable function u that has compact support, $u_\delta = j_\delta * u$ is a smooth function of compact support that $||u_\delta - u||_{C^k} \to 0$ when $u \in C^k$. Where j_δ is the scaling of a smooth function of compact support. So Smooth function of compact support are dense in C_0^k. ⌟

Prop. (11.3.8.11). $D(\mathbb{R}^n)$ is dense in $W^{m,p}(\mathbb{R}^n)$. ⌟

Proof: Use the fact that C_0 are dense in L^p by(11.3.8.10). And $f_\delta \to f$ in L^p norm for $f \in C_0$. So we can use the three-part argument applied to $D_\alpha u$ to get $D_\alpha(u_\delta) \to D_\alpha u$ in L^p norm for $|\alpha| \le m$. Thus the result. □

9 Convolutions

Prop. (11.3.9.1). Convolution with a smooth function makes the function smooth, in particular, $\frac{\partial}{\partial x}(f * g) = \frac{\partial}{\partial x} f * g$. ⌟

Prop. (11.3.9.2) [Young's Inequality]. $||f * g||_r \le ||f||_p ||g||_q$ for all $1 \le r, p, q \le \infty$ and

$$1 + \frac{1}{r} = \frac{1}{p} + \frac{1}{q}.$$

In particular, $||K * f||_p \le ||K||_1 ||f||_p$. ⌟

Proof: By Riesz representation(11.10.1.10), it suffices to show that: for $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 2$,

$$\int\int f(x)g(y-x)h(y) \le ||f||_p ||g||_q ||h||_r.$$

write the LHS as

$$\int\int (f^p(x)g(y-x)^q)^{1-\frac{1}{r}} (f^p(x)h^r(y))^{1-\frac{1}{q}} (g^q(y-x)h^r(y))^{1-\frac{1}{p}}$$

and use Holder inequality for three functions(11.3.6.2). □

10 Example of Calculations

Prop. (11.3.10.1). For $s \in \mathbb{C}, \mathrm{Re}(s) > 1/2$, then

$$\int_{-\infty}^{\infty} (1+x^2)^{-s} e^{\mathrm{i}\, k \arctan(-\frac{1}{x})} \mathrm{d}x = (-\mathrm{i})^k \sqrt{\pi} \frac{\Gamma(s)\Gamma(s-\frac{1}{2})}{\Gamma(s+\frac{k}{2})\Gamma(s-\frac{k}{2})}.$$

⌟

Proof: Cf.[Bump, Automorphic Forms and Representations, P230]. □

11 Hausdorff Measures

12 Area and Coarea Formulas

13 Inequalities

References are [HLP88].

Limits

Prop. (11.3.13.1) [e]. For $x \in \mathbb{R}_+$,

$$\lim_{x\to\infty} (\frac{x+1}{x})^x = e.$$

⌟

Proof: □

Convex Functions

Def. (11.3.13.2) [Convex Functions]. Let $X \subset \mathbb{R}^n$ be a convex set, then a **convex function** on X is a function $f : X \to \mathbb{R}$ s.t. for any $x, y \in X$ and $t \in [0,1]$,

$$f((1-t)x+ty) \le (1-t)f(x)+tf(y).$$

⌟

Prop. (11.3.13.3). A convex function on $\mathbb{R}$ is absolutely continuous. ⌟

Proof: This is because it is absolutely continuous. □

Prop. (11.3.13.4). Let $\varphi : \mathbb{R}_+ \to \mathbb{R}$ be a non-decreasing function s.t. $\varphi(0) = 0$, and $\varphi(e^\xi)$ is a convex function of ξ. Suppose $\lambda_1 \ge \lambda_2 \ge \ldots \ge \lambda_m \in \mathbb{R}_+$, $\kappa_i \in \mathbb{R}$ satisfy

$$\lambda_1 \le \kappa_1, \quad \lambda_1\lambda_2 \le \kappa_1\kappa_2, \quad \ldots \quad \lambda_1\ldots\lambda_m \le \kappa_1\ldots\kappa_m,$$

then

$$\sum_i \varphi(\lambda_i) \le \sum_i \varphi(\kappa_i).$$

⌟

Proof: For $z \in \mathbb{R}_{\ge 0}$, define

$$f(z) = \prod_i \max(1, \kappa_i z), \quad g(z) = \prod_i \max(1, \lambda_i z),$$

then by argue case by case, $g(z) \le f(z)$.

Notice if there exists an increasing function $\psi : [0,\infty) \to \mathbb{R}$ s.t. for any $\lambda \in \mathbb{R}_+$,

$$\varphi(\lambda) = \int_{\lambda^{-1}}^\infty \log(\lambda z) \mathrm{d}\psi(z),$$

where the RHS is the Lebesgue-Stieltjes integral, then

$$\sum_i \varphi(\lambda_i) = \int_0^\infty \log g(z) \mathrm{d}\psi(z) \le \int_0^\infty \log f(z) \mathrm{d}\psi(z) = \sum_i \varphi(\kappa_i).$$

Denote $G(\xi) = \varphi(e^\xi)$, then we show that $\psi(z) = -G^\backprime(-\log z)$ suffices: If $\xi = \log \lambda$, then

$$\int_{\lambda^{-1}}^\infty \log(\lambda z) \mathrm{d}\psi(z) = \int_{-\xi}^\infty (\xi + t) \mathrm{d}(-G^\backprime(-t)) = G(\xi) = \varphi(\lambda).$$

Where we used integration by parts**??** and the fact $\lim_{t\to-\infty} tG^\backprime(t) = 0$, which is because $\lim_{t\to-\infty} G(t) = 0$ and

$$tG^\backprime(t) \le 2\int_t^{t/2} G^\backprime(t)\mathrm{d}t = 2[G(\frac{t}{2}) - G(t)].$$

□

Hardy Inequality

Thm. (11.3.13.5) [Hardy Inequality]. For $p \in \mathbb{R}_{>1}$ and a measurable function $f(x)$ on $(0, \infty)$ s.t. $f(x) \geq 0$,

$$\int_0^\infty \Big(\frac{1}{x}\int_0^x f(t)\mathrm{d}t\Big)^p \mathrm{d}x \leq \Big(\frac{p}{p-1}\Big)^p \int_0^\infty f(x)^p \mathrm{d}x.$$

⌟

Proof: Let $F(x) = \int_0^x f(t)\mathrm{d}t$, then $\frac{\partial}{\partial x}F(x)^p = pF(x)^{p-1}f(x)$. So by integration by part, for any $\alpha < A \in \mathbb{R}_+$,

$$\int_\alpha^A \Big(\frac{F(x)-F(\alpha)}{x}\Big)^p \mathrm{d}x = -\frac{A^{1-p}}{p-1}(F(A)-F(\alpha))^p + \frac{p}{p-1}\int_\alpha^A \Big(\frac{F(x)-F(\alpha)}{x}\Big)^{p-1} f(x)\mathrm{d}x$$

$$(11.3.6.2) \leq \frac{p}{p-1}\Big(\int_\alpha^A \Big(\frac{F(x)-F(\alpha)}{x}\Big)^p \mathrm{d}x\Big)^{(p-1)/p}\Big(\int_\alpha^A f(x)^p\Big)^{1/p},$$

which implies that

$$\int_\alpha^A \Big(\frac{F(x)-F(\alpha)}{x}\Big)^p \mathrm{d}x \leq \Big(\frac{p}{p-1}\Big)^p \int_\alpha^A f(x)^p \mathrm{d}x.$$

Then the result follows by taking limit $A \to \infty$ and then take limit $\alpha \to 0$. □

Cor. (11.3.13.6) [Hardy-Landau Inequality]. If $p \in \mathbb{R}_{>1}$ and $(a_k)_{k\in\mathbb{Z}_+} \subset \mathbb{R}_+$ is a sequence of positive real numbers, then

$$\sum_{n=1}^\infty \Big(\frac{1}{n}\sum_{k=1}^n a_k\Big)^p \leq \Big(\frac{p}{p-1}\Big)^p \sum_{n=1}^\infty a_n^p.$$

⌟

Proof: We may assume that $a_1 > a_2 > \ldots$, and $\sum_{n=1}^\infty a_n^p < \infty$. Define $f : (0,\infty) \to \mathbb{R}_+ : x \mapsto a_{\lceil x\rceil}$, then $f \in L^p(0,\infty)$, and

$$\frac{1}{x}\int_0^x f(t)\mathrm{d}t = \frac{\sum_{k\leq x} a_k + a_{\lceil x\rceil}(x - \lfloor x\rfloor)}{x},$$

which is decreasing in x.

Then

$$\sum_{n=1}^\infty \Big(\frac{1}{n}\sum_{k=1}^n a_k\Big)^p \leq \sum_{n=1}^\infty \Big(\int_{n-1}^n \frac{1}{x}\int_0^x f(t)\mathrm{d}t\Big)^p \mathrm{d}x \leq \Big(\frac{p}{p-1}\Big)^p \int_0^\infty f(x)^p \mathrm{d}x = \Big(\frac{p}{p-1}\Big)^p \sum_{n=1}^\infty a_n^p$$

□

Cor. (11.3.13.7) [Carleman Inequality]. If $(a_k)_{k\in\mathbb{Z}_+} \subset \mathbb{R}_+$ is a sequence of positive real numbers, then

$$\sum_{n=1}^\infty (a_1\ldots a_n)^{1/n} \leq e\sum_{n=1}^\infty a_n.$$

⌟

Proof: By Hardy-Landau Inequality, for any $p \in \mathbb{R}_{>1}$,

$$\Big(\frac{p}{p-1}\Big)^p \sum_{n=1}^\infty a_n \geq \sum_{n=1}^\infty \Big(\frac{1}{n}\sum_{k=1}^n a_k^{1/p}\Big)^p \geq \sum_{n=1}^\infty (a_1\ldots a_n)^{1/n}.$$

Then we use the fact $\lim_{p\to\infty}\big(\frac{p}{p-1}\big)^p = e$(11.3.13.1). □

Cor. (11.3.13.8)[Pólya-Knopp Inequality]. For any measurable function $f(x)$ on $(0,\infty)$ s.t. $f(x) > 0$,

$$\int_0^\infty \exp\Big(\frac{1}{x}\int_0^x \log f(t)\mathrm{d}t\Big)\mathrm{d}x \le e\int_0^\infty f(x)\mathrm{d}x.$$

⌟

Proof: The proof is similar in essence to that of Carleman Inequality. □

Thm. (11.3.13.9)[Copson Inequality]. If $p \in \mathbb{R}_{>1}$ and $(a_k)_{k\in\mathbb{Z}_+} \subset \mathbb{R}_+$ is a sequence of positive real numbers, then

$$\sum_{n=1}^\infty \Big(\sum_{k=n}^\infty \frac{a_k}{k}\Big)^p \le p^p \sum_{n=1}^\infty a_n^p.$$

⌟

Proof: □

11.4 Complex Analysis I

References are [Ahl78], [S-S03], [T-W06] and [Li04].

Notation (11.4.0.1).

- Use notations defined in Real Analysis(Functions on $\mathbb{R}^n$).
- Let Ω be a region(11.4.1.1).

⌟

1 Basics

Def. (11.4.1.1) [Regions]. A **region** is a nonempty connected open subset of $\mathbb{C}$. ⌟

Def. (11.4.1.2) [Conjugations]. The non-zero element in $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is denoted by $\mathtt{c}$. And for $z \in \mathbb{C}$, $\mathtt{c}(z)$ is also denoted by $\overline{z}$.

For $z \in \mathbb{C}$, denote $\mathrm{Re}(z) = \frac{z+\overline{z}}{2}, \mathrm{Im}(z) = \frac{z-\overline{z}}{2\,\mathrm{i}}$, called the **real part** and **complex part** of z resp.. So

$$z = \mathrm{Re}(z) + \mathrm{i}\,\mathrm{Im}(z), \quad \overline{z} = \mathrm{Re}(z) - \mathrm{i}\,\mathrm{Im}(z).$$

⌟

Prop. (11.4.1.3) [$\mathbb{C}$ is Complete]. The natural extended value from $\mathbb{R}$ to $\mathbb{C}$ is of the form $|x + \mathrm{i}\,y| = \sqrt{x^2 + y^2}$. In particular, it is easy to prove that $\mathbb{C}$ is a complete valued field. ⌟

Def. (11.4.1.4) [Derivatives]. We introduce the following notations:

$$\frac{\partial}{\partial z} = \frac{1}{2}(\frac{\partial}{\partial x} - \mathrm{i}\,\frac{\partial}{\partial y}), \quad \frac{\partial}{\partial \overline{z}} = \frac{1}{2}(\frac{\partial}{\partial x} + \mathrm{i}\,\frac{\partial}{\partial y}), \quad \mathrm{d}z = \mathrm{d}x + \mathrm{i}\,\mathrm{d}y \quad \mathrm{d}\overline{z} = \mathrm{d}x - \mathrm{i}\,\mathrm{d}y.$$

Then $\mathrm{d}z$ is dual to $\frac{\partial}{\partial z}$ and $d\overline{z}$ is dual to $\frac{\partial}{\partial \overline{z}}$. And for any function $f \in C^1(\mathbb{C})$,

$$\mathrm{d}f = \frac{\partial}{\partial x} f \mathrm{d}x + \frac{\partial}{\partial y} \mathrm{d}y = \frac{\partial}{\partial z} f \mathrm{d}z + \frac{\partial}{\partial \overline{z}} f \mathrm{d}\overline{z}.$$

And also,

$$\mathrm{d}z\mathrm{d}\overline{z} = 2\mathrm{d}x\mathrm{d}y = 2r\mathrm{d}r\mathrm{d}\theta$$

⌟

Prop. (11.4.1.5) [Orientations]. For $f \in C^1(\mathbb{C})$,

$$\mathrm{Jac}_f(z) = \frac{\partial}{\partial x} f \frac{\partial}{\partial y} f = |\frac{\partial}{\partial z} f|^2 - |\frac{\partial}{\partial \overline{z}} f|^2.$$

Thus f preserves orientations at z iff $|\frac{\partial}{\partial z} f| > |\frac{\partial}{\partial \overline{z}} f|$. ⌟

Def. (11.4.1.6) [Cross Ratios]. For any three pts $z_2, z_3, z_4 \in \overline{\mathbb{C}}$, there is a unique linear transformation that maps them to $1, 0, \infty$. In fact, the linear transformation is just $Sz = \frac{z-z_3}{z-z_4} / \frac{z_2-z_3}{z_2-z_4}$.

Then for any for point z_1, z_2, z_3, z_4, the **cross ratio** $(z_1, z_2, z_{3,4})$ is the image of z_1 under the linear transformation that carries z_2, z_3, z_4 to $1, 0, \infty$. ⌟

Prop. (11.4.1.7). The cross ratio is invariant under linear transformation, and it is real iff z_1, z_2, z_3, z_4 are colinear or cocycle. ⌟

Proof: The first is because there is only one linear transformation that maps z_2, z_3, z_4 to $1, 0, \infty$.

For the second, notice by(11.4.1.6), $\arg(z_1, z_2, z_{3,4}) = \arg\frac{z_1 - z_3}{z_1 - z_4} - \arg\frac{z_2 - z_3}{z_2 - z_4}$, and this is real iff $\angle z_4 z_2 z_3 = \angle z_4 z_1 z_3$ or $\pi - \angle z_4 z_1 z_3$, which is equivalent to cocycle. For other degenerate cases, we need some other argument. □

Cor. (11.4.1.8). A linear transformation maps colinear/cocycle points to colinear/cocycle points. ⌟

Lemma (11.4.1.9) [Invariant Factor]. If $a, b, c, d \in \mathbb{R}$, then

$$\operatorname{Im}(\frac{az+b}{cz+d}) = \frac{ad-bc}{|cz+d|^2}\operatorname{Im}(z).$$

⌟

Analytic Functions

Def. (11.4.1.10) [Analytic Functions]. For an open subset $\Omega \subset \mathbb{C}$, a complex-valued function f on Ω is called **analytic** or **holomorphic** if $\frac{\partial}{\partial \bar{z}} f(z) = 0$ for any $z \in \Omega$(11.4.1.4). Equivalently,

$$\frac{\partial}{\partial x} f = -\mathrm{i}\frac{\partial}{\partial y} f, \quad \text{i.e.} \begin{cases} \frac{\partial}{\partial x}\operatorname{Re}(f) = \frac{\partial}{\partial y}\operatorname{Im}(f) \\ \frac{\partial}{\partial x}\operatorname{Im}(f) = -\frac{\partial}{\partial y}\operatorname{Re}(f) \end{cases}$$

i.e. f has the same derivative vertically and horizontally, hence in every direction.

The space of analytic functions on Ω is denoted by $\mathcal{O}(\Omega)$. More generally, if $\Omega \subset \mathbb{C}$ is any subspace, $\mathcal{O}(\Omega) = C(\Omega) \cap \mathcal{O}(\Omega^o)$.

For $f \in \mathcal{O}(\Omega)$, denote

$$f'(z) = \frac{\partial}{\partial z} f(z) = \frac{\partial}{\partial x} f(z) = -\mathrm{i}\frac{\partial}{\partial y} f(z).$$

and for $n \in \mathbb{N}$, denote inductively

$$f^{(0)} = f, \quad f^{(1)} = f', \quad f^{(n+1)} = (f^{(n)})'.$$

⌟

Lemma (11.4.1.11). Let $\Omega \subset \mathbb{C}$ be a region and $f \in \mathcal{O}(\Omega)$ s.t. $f' = 0$, then f is a constant function. ⌟

Proof: This follows from the fact any two points in Ω can be connected by a path consisting of vertical or horizontal segments, and use the fundamental theorem of calculus(11.3.3.25). □

Prop. (11.4.1.12) [$\bar{\partial}$-Equation]. Let $\Omega \subset \mathbb{C}$ be a region and $f \in C^k(\Omega), k \geq 1$, then locally near every point, there exists a C^k-function g s.t.

$$\frac{\partial}{\partial \bar{z}} g = f.$$

And such a function is defined up to an analytic function. ⌟

Proof: Taking a bump function, we may assume $f \in C_c^k(\Omega)$. Then define

$$g(z) = \frac{1}{2\pi\mathrm{i}}\int_{\mathbb{C}} \frac{f(\zeta)}{\zeta - z} d\zeta \wedge d\bar{\zeta} = \frac{1}{2\pi\mathrm{i}}\int_{\mathbb{C}} \frac{f(\zeta + z)}{\zeta} d\zeta \wedge d\bar{\zeta}.$$

This singular integration is convergent because $h(\zeta) = \frac{1}{\zeta - z}$ is locally L^1(this follows from(11.4.1.4)). And the integration is uniformly convergent in z. Then the differentiation commutes with integration and shows g is C^k. Moreover,

$$\frac{\partial}{\partial \overline{z}} g(z) = \lim_{\varepsilon \to 0} \frac{1}{2\pi \mathrm{i}} \int_{\mathbb{C} \setminus \mathbb{D}(0,\varepsilon)} \frac{\partial}{\partial \overline{\zeta}} f(\zeta) \frac{\mathrm{d}\zeta \wedge \mathrm{d}\overline{\zeta}}{\zeta - z} = \lim_{\varepsilon \to 0} \frac{1}{2\pi \mathrm{i}} \int_{\partial \mathbb{D}(0,\varepsilon)} f(\zeta) \frac{\mathrm{d}\zeta}{\zeta - z} = f(z)$$

by Stoke's formula and continuity. □

2 Complex Integration

Lemma (11.4.2.1). If f is analytic on a rectangle R minus f.m. points ζ_i and if $\lim_{z \to \zeta_i} (z - \zeta_i) f(z) = 0$, then $\int_{\partial R} f(z) \mathrm{d}z = 0$. ⌟

Proof: We consider first the case that no points are omitted. Cut the rectangle R into 4 rectangles R^1, R^2, R^3, R^4 that is similar to R, then

$$\int_{\partial R} f(z) \mathrm{d}z = \sum_{i=1}^{4} \int_{\partial R^i} f(z) \mathrm{d}z.$$

Let $|\int_{\partial R} f(z) \mathrm{d}z| = T$, then there exists some R^i that $|\int_{\partial R^i} f(z) \mathrm{d}z| \geq \frac{1}{4} T$. Denote this R^i by R_1. Then we can do the same for R_1 to find an R_2 s.t. $|\int_{\partial R_2} f(z) \mathrm{d}z| \geq \frac{1}{4^2} T$. Continuing this process, we find a sequence $R_1 \supset R_2 \supset \ldots \supset R_n \supset$, and their intersection is a single point z_0 as R is compact. Now as f is analytic, for any $\varepsilon > 0$, for n sufficiently large, for any $z \in \partial R_n$,

$$\left|\frac{f(z) - f(z_0)}{z - z_0} - f'(z_0)\right| \leq \varepsilon.$$

Notice also by direct calculating that

$$\int_{\partial R_n} \mathrm{d}z = 0, \quad \int_{\partial R_n} z \mathrm{d}z = 0,$$

we have

$$\frac{T}{4^n} \leq \left|\int_{\partial R_n} f(z) \mathrm{d}z\right| = \left|\int_{\partial R_n} [f(z) - f(z_0) - f'(z_0)(z - z_0)] \mathrm{d}z\right| \leq \varepsilon \int_{\partial R_n} |z - z_0| |\mathrm{d}z| \leq \varepsilon \frac{dL}{4^n}$$

where d, L are the length of the diagonal and the perimeter of R. So $T \leq \varepsilon$. As ε is arbitrary, this means $T = 0$.

In general, by cutting into several rectangles, it suffices to prove for the case that only one point is omitted, and in this case, we can use what we have proved and the hypothesis to reduce the rectangle to any small enough rectangle R_0 around ζ_1 s.t. for any $z \in \partial R_0$,

$$f(z) \leq \frac{\varepsilon}{|z - \zeta_1|}.$$

And then

$$\left|\int_{\partial R_0} f(z) \mathrm{d}z\right| \leq \varepsilon \int_{\partial R_0} \frac{|\mathrm{d}z|}{|z - \zeta_1|} \leq 8\varepsilon$$

by elementary estimation. As ε is arbitrary, this means $\int_{\partial R_0} f(z) \mathrm{d}z = 0$. □

Thm. (11.4.2.2) [Cauchy]. If $\Omega \subset C$ is a simply-connected region and Ω' is the region obtained from Ω by omitting f.m. points ζ_i. Suppose $f \in \mathcal{O}(\Omega')$, and $\lim_{z\to\zeta_i}(z-\zeta_i)f(z) = 0$, then $\int_\gamma f(z)dz = 0$ for any closed piecewise C^1 curve $\gamma \subset \Omega'$.

Moreover, if $f \in \mathcal{O}(\overline{\Omega'})$, then $\int_\gamma f(z)dz = 0$ for any closed piecewise C^1 curve $\gamma \subset \overline{\Omega'}\backslash\{\zeta_1, \ldots, \zeta_i\}$.
⌟

Proof: Fix a $z_0 \in \Omega$, then for any $z \in \Omega$, choose a path γ from z_0 to z consisting of vertical or horizontal segments, and let $F(z) = \int_\gamma f(z)dz$. Then this F is well-defined: if there are two paths γ, γ', $\gamma - \gamma'$ is a sum oriented boundary of rectangles, and these rectangles must be contained in Ω because Ω is simply-connected. Thus the above lemme(11.4.2.1) shows that $F(z)$ is independent of the path chosen, and it is clear that $F(z)$ has the same derivative in both directions so analytic by definition(11.4.1.10). So clearly $\int_\gamma f(z)dz = F(z)\Big|_{\gamma(0)}^{\gamma(1)} = 0$.

For the last assertion, any such a closed piecewise C^1 curve $\gamma \subset \overline{\Omega'}\backslash\{\zeta_1, \ldots, \zeta_i\}$ can be uniformly approximated by a path in Ω'. □

Cor. (11.4.2.3) [Existence of Primitive]. If $\Omega \subset \mathbb{C}$ is a simply connected region and $f \in \mathcal{O}(\Omega)$, then there exists a function $F \in \mathcal{O}(\Omega)$ s.t. $F' = f$. ⌟

Proof: Take $z_0 \in \Omega$ and take $F(z) = \int_\gamma f(z)\mathrm{d}z$ for any path γ from z_0 to z. F is well-defined by the Cauchy theorem(11.4.2.2). □

Prop. (11.4.2.4) [Generating Analytic Functions]. If $\varphi(\zeta)$ is continuous on an arc γ, then the function
$$F_n(\zeta) = \int_\gamma \frac{\varphi(\zeta)}{(\zeta - z)^n}\mathrm{d}\zeta$$
is analytic on each connected component of $\mathbb{C}\backslash\gamma$, and its derivative is $F_n'(z) = nF_{n+1}(z)$. ⌟

Proof: Use induction on n: for $n = 1$, firstly we prove F_1 is continuous: for $z_0 \notin \gamma$, choose $\delta > 0$ s.t. $U(z_0, \delta) \cap \gamma = \varnothing$, then for $z \in U(z_0, \delta)$, $d(z, \gamma) > \delta/2$, and
$$|F_1(z) - F_1(z_0)| = |z - z_0|\left|\int_\gamma \frac{\varphi(\zeta)}{(\zeta - z)(\zeta - z_0)}\mathrm{d}\zeta\right| \leq |z - z_0|\frac{2}{\delta^2}\int_\gamma |\varphi||\mathrm{d}\zeta|,$$
thus F_1 is continuous. Moreover, the above argument applied to the function $\Phi(\zeta) = \varphi(\zeta)/(\zeta - z_0)$ implies that
$$\lim_{z\to z_0}\frac{F_1(z) - F_1(z_0)}{z - z_0} = \lim_{z\to z_0}\int_\gamma \frac{\varphi(\zeta)}{(\zeta - z)(\zeta - z_0)}\mathrm{d}\zeta = \lim_{z\to z_0}\int_\gamma \frac{\Phi(\zeta)}{(\zeta - z)}\mathrm{d}\zeta = \int_\gamma \frac{\Phi(\zeta)}{(\zeta - z_0)}\mathrm{d}\zeta = F_2(z_0),$$
hence $F_1' = F_2$.

For $n > 1$, suppose we have shown $F_{n-1}' = (n-1)F_n$, then with notations as above, we have
$$\begin{aligned} F_n(z) - F_n(z_0) &= \left[\int_\gamma \frac{\varphi(\zeta)}{(\zeta - z)^{n-1}(\zeta - z_0)}\mathrm{d}\zeta - \int_\gamma \frac{\varphi(\zeta)}{(\zeta - z_0)^n}\mathrm{d}\zeta\right] + (z - z_0)\int_\gamma \frac{\varphi(\zeta)}{(\zeta - z)^n(\zeta - z_0)}\mathrm{d}\zeta \\ &= \left[\int_\gamma \frac{\Phi(\zeta)}{(\zeta - z)^{n-1}}\mathrm{d}\zeta - \int_\gamma \frac{\Phi(\zeta)}{(\zeta - z_0)^{n-1}}\mathrm{d}\zeta\right] + (z - z_0)\int_\gamma \frac{\Phi(\zeta)}{(\zeta - z)^n}\mathrm{d}\zeta \end{aligned}$$
Then we see by induction hypothesis that $\lim_{z\to z_0} F_n(z) - F_n(z_0) = 0$ and F_n is continuous for any φ. Moreover,
$$\lim_{z\to z_0}\frac{F_n(z) - F_n(z_0)}{(z - z_0)} = \lim_{z\to z_0}\frac{1}{(z - z_0)}\left[\int_\gamma \frac{\Phi(\zeta)}{(\zeta - z)^{n-1}}\mathrm{d}\zeta - \int_\gamma \frac{\Phi(\zeta)}{(\zeta - z_0)^{n-1}}\mathrm{d}\zeta\right] + \int_\gamma \frac{\Phi(\zeta)}{(\zeta - z)^n}\mathrm{d}\zeta$$

$$= n\int_\gamma \frac{\Phi(\zeta)}{(\zeta - z_0)^n}\mathrm{d}\zeta + \int_\gamma \frac{\Phi(\zeta)}{(\zeta - z_0)^n}\mathrm{d}\zeta$$
$$= (n+1)F_{n+1}(z)$$

□

Prop. (11.4.2.5) [Index of a Point w.r.t a Curve]. If γ is a piecewise C^1 curve that doesn't pass a point a, then $\frac{1}{2\pi\mathrm{i}}\int_\gamma \frac{\mathrm{d}z}{z-a}$ is an integer $n(\gamma, a)$, called the **index of** a **w.r.t** γ, or the **winding number**.

And this index function is constant on each connected component of $\mathbb{C}\backslash\gamma$, and 0 on the unbounded component. In particular, if γ is a circle and a is contained in the interior of this circle, then $n(\gamma, a) = 1$. ⌟

Proof: Cf. [Ahl78]P115.**?**

this index function is constant on each connected component of $\mathbb{C}\backslash\gamma$, and 0 on the unbounded component by the continuity of the integral by(11.4.2.4).

For the last assertion, it suffices to show for $\gamma = \partial\mathbb{D}(0, R)$ and $a = 0$, by what we just said. And in this case,

$$\frac{1}{2\pi\mathrm{i}}\int_\gamma \frac{\mathrm{d}z}{z-a} = \frac{1}{2\pi\mathrm{i}}\int_0^{2\pi} \frac{\mathrm{i}\,Re^{i\theta}}{Re^{\mathrm{i}\,\theta}}\mathrm{d}\theta = 1$$

□

Cor. (11.4.2.6) [Cauchy Integral Formula, Cauchy1825]. if $\Omega \subset \mathbb{C}$ is a simply-connected region, $f \in \mathcal{O}(\Omega)$, then for any piecewise C^1 closed curve $\gamma \subset \Omega$ and $a \notin \gamma$,

$$\frac{1}{2\pi\mathrm{i}}\int_\gamma \frac{f(\xi)}{\xi - a}\mathrm{d}\xi = n(\gamma, a)f(a)\text{(11.4.2.5)}.$$

In particular, if γ is the boundary of a disk D contained in $\mathbb{C}$, then for any $a \in D$,

$$\frac{1}{2\pi\mathrm{i}}\int_\gamma \frac{f(\xi)}{\xi - a}\mathrm{d}\xi = f(a).$$

Moreover, if $f \in \mathcal{O}(\overline{\Omega})$, then this is true for any piecewise C^1 closed curve $\gamma \subset \Omega$ and $a \notin \gamma$. ⌟

Proof: Consider the function $F(z) = \frac{f(z)-f(a)}{z-a}$, then it is analytic for $z \neq a$, and at a it satisfies the condition of Cauchy theorem(11.4.2.2), so $\int_\gamma F(z)dz = 0$ which is $\int_\gamma \frac{f(z)dz}{z-a} = f(a)\int \frac{dz}{z-a}$, and use(11.4.2.5). □

Cor. (11.4.2.7) [Higher Derivations]. For any region Ω $f \in \mathcal{O}(\Omega)$, if $a \in \Omega$ and γ is a small circle γ in Ω centered at a,

$$f(a) = \frac{1}{2\pi\mathrm{i}}\int_\gamma \frac{f(\zeta)}{\zeta - a}\mathrm{d}\zeta$$

by Cauchy integral theorem(11.4.2.6). So derivatives of f are all analytic, and satisfy:

$$f^{(n)}(z) = \frac{n!}{2\pi\mathrm{i}}\int_\gamma \frac{f(\zeta)}{(\zeta - z)^{n+1}}\mathrm{d}\zeta.$$

In particular, $\mathcal{O}(\Omega) \subset C^\infty(\Omega)$. ⌟

Cor. (11.4.2.8) [Morera]. If f is continuous on a region Ω and if $\int_\gamma f \mathrm{d}z = 0$ for any piecewise closed curve $\gamma \subset \Omega$ consisting of vertical or horizontal segments, then $f(z) \in \mathcal{O}(\Omega)$. ⌟

Proof: There is an analytic function F that $F' = f$, by the same method of the proof of(11.4.2.2), so f is analytic, by(11.4.2.7). □

Cor. (11.4.2.9)[Cauchy Estimate]. If $f \in \mathcal{O}(\overline{\mathbb{D}(a,r)})$, and $|f| \leq M$ on the boundary, then $|f^{(n)}(a)| \leq Mn!r^{-n}$ for any $a \in \mathbb{D}$. ⌟

Cor. (11.4.2.10) [Liouville]. Any bounded holomorphic function on $\mathbb{C}$ is constant. ⌟

Proof: if $|f(z)| \leq M$, then the Cauchy estimate shows that $|f'(a)| \leq Mr^{-1}$, letting r tends to ∞, then $f'(a) = 0$ for all a, thus f is constant. □

Cor. (11.4.2.11) [Mean Value Property]. If $f \in \mathcal{O}(\mathbb{D})$, then $|f(0)| \leq \int_{\mathbb{D}} |f(z)| \mathrm{d}x\mathrm{d}y$. ⌟

Proof: $|f(0)| \leq \frac{1}{2\pi} \int f(re^{\mathrm{i}\theta}) \mathrm{d}\theta$, so if multiplied by $r\mathrm{d}r$ and integrate, then

$$|f(0)| \leq \int\int f(re^{\mathrm{i}\theta}) r \mathrm{d}r \mathrm{d}\theta = \int\int f(z) \mathrm{d}x\mathrm{d}y.$$

□

Prop. (11.4.2.12). For any $f \in \mathcal{O}(\overline{\mathbb{D}(0,R)})$, for $z \in \mathbb{D}(0,R)$:

$$f(z) = \frac{1}{2\pi \mathrm{i}} \int_{|\zeta|=R} \mathrm{Re}(\frac{\zeta + z}{\zeta - z}) f(\zeta) \frac{\mathrm{d}\zeta}{\zeta}.$$

⌟

Proof: Let $F(\zeta) = \frac{f(\zeta)}{\zeta - R^2/\overline{z}}$, then $F \in \mathcal{O}(\overline{\mathbb{D}(0,R)})$, and by Cauchy's theorem(11.4.2.2),

$$\int_{|\zeta|=R} \frac{f(\zeta)}{\zeta - R^2/\overline{z}} \mathrm{d}\zeta = 0.$$

And by Cauchy's integral formula,

$$\frac{1}{2\pi \mathrm{i}} \int_{|\zeta|=R} \frac{f(\zeta)}{\zeta - z} \mathrm{d}\zeta = f(z).$$

so

$$f(z) = \frac{1}{2\pi \mathrm{i}} \int_{|\zeta|=R} [\frac{f(\zeta)}{\zeta - z} - \frac{f(\zeta)}{\zeta - R^2/\overline{z}}] d\zeta = \frac{1}{2\pi \mathrm{i}} \int_{|\zeta|=R} [\frac{\zeta}{\zeta - z} + \frac{\overline{z}}{\overline{\zeta} - \overline{z}}] f(\zeta) \frac{d\zeta}{\zeta} = \frac{1}{2\pi \mathrm{i}} \int_{|\zeta|=R} \mathrm{Re}(\frac{\zeta + z}{\zeta - z}) f(\zeta) \frac{\mathrm{d}\zeta}{\zeta}$$

□

Prop. (11.4.2.13) [Invariance of Winding Numbers]. Let S be a smooth Jordan curve in $\mathbb{C}$, and let $(C_s)_{s \in S}$ be a smoothly varying family of smooth Jordan curves(i.e. there exists a diffeomorphism $J : S \times \partial\mathbb{D}(0,1) \cong \{(s,z) : s \in S, z \in C_s\}$), with $D_s = \mathrm{int}\, C_s$. Let $a, b, f : S \to \mathbb{C}$ be smooth functions s.t. $a(s), b(s) \in D_s$, and $f(s) \in C_s$, then

$$\int_S \frac{1}{f(s) - a(s)} \mathrm{d}s = \int_S \frac{1}{f(s) - b(s)} \mathrm{d}s$$

⌟

Proof: The use of the smoothly varying property is that: by isotopy extension theorem(12.1.7.2), we can extend J to a diffeomorphism

$$J : S \times \overline{\mathbb{D}(0,1)} \cong \{(s,z) : s \in S, z \in \overline{D_s}\},$$

so we can define a homotopy from $a(s)$ to $b(s)$ via

$$e_t(s) = J_s((1-t)J_s^{-1}(a(s)) + tJ_s^{-1}(b(s))).$$

□

Constructing Analytic Functions

Prop. (11.4.2.14)[Holomorphic Function Defined by Integrations]. Let $(X, \mathcal{M}, \mu)$ be a σ-finite measure space and $\Omega \subset \mathbb{C}$ be a region. For any $F \in L^1(\Omega \times X)$, if

- $F(z,x)$ is analytic in z for any $x \in X$.
- $z \mapsto \int_X |F(z,x)| \mathrm{d}x$ is uniformly convergent on compact subsets.

then $f(z) = \int_X F(z,x)\mathrm{d}x$ is an analytic function on Ω.

In particular, item2 holds if $F \in C(\Omega \times X)$ and X is compact. ⌟

Proof: This follows from Morera's theorem(11.4.2.8) and Fubini-Tonelli theorem(11.3.2.8). □

Cor. (11.4.2.15)[Weierstrass]. If $(f_n)_{n\in\mathbb{Z}_+}$ is a sequence of holomorphic functions on Ω that converges uniformly to f on every compact subset, then f is holomorphic on Ω. And for any $k \in \mathbb{N}$, $(f_n^{(k)})_{n\in\mathbb{Z}_+}$ converges uniformly on f on every compact subset. ⌟

Proof: For the last assertion, use Cauchy's integral formula(11.4.2.6). □

Local Properties of Analytic Functions

Prop. (11.4.2.16) [Taylor Expansions]. Let $\Omega \subset \mathbb{C}$ be a region and $f \in \mathcal{O}(\Omega)$, then if $D \subset \Omega$ be a closed disk with center z_0, then for any $z \in D$,

$$f(z) = \sum_{n\in\mathbb{N}} \frac{f^{(n)}(z_0)}{n!}(z-z_0)^n.$$

⌟

Proof: By Cauchy's integral formula(11.4.2.6), if C is the boundary of D, then

$$f(z) = \frac{1}{2\pi \mathrm{i}} \int_C \frac{f(\xi)}{\xi - z}\mathrm{d}\xi$$

But

$$\frac{1}{\xi - z} = \frac{1}{\xi - z_0}\frac{1}{1-(\frac{\xi - z}{\xi - z_0})} = \sum_{n\in\mathbb{N}} \frac{(\xi - z)^n}{(\xi - z_0)^{n+1}}$$

and the convergence is uniform on C, so by(11.4.2.7),

$$f(z) = \int_C \Big(\frac{1}{2\pi \mathrm{i}} \int_C \frac{f(\xi)}{(\xi - z_0)^{n+1}}\Big)(\xi - z)^n = \sum_{n\in\mathbb{N}} \frac{f^{(n)}(z_0)}{n!}(z-z_0)^n.$$

□

Cor. (11.4.2.17). For any region $\Omega \subset \mathbb{C}$ and $f \in \mathcal{O}(\Omega)$. If $z_0 \in \Omega$ and $f^{(n)}(z_0) = 0$ for any $n \in \mathbb{N}$, then $f = 0 \in \mathcal{O}(\Omega)$. ⌟

Proof: The subset $E = \{z_0 \in \Omega | f^{(n)}(z_0) = 0, \forall n \in \mathbb{N}\}$ is an open subset by the Taylor expansion(11.4.2.16), and the complement is also an open subset as all the derivatives are continuous. So $E = \Omega$, and Ω is connected. □

Prop. (11.4.2.18) [Removable Singularities]. Let $\Omega \subset \mathbb{C}$ and Ω' is the region obtained from Ω by omitting f.m. points ζ_i, $f \in \mathcal{O}(\Omega')$, then f can be extended to an analytic function $f \in \mathcal{O}(\Omega)$ iff $\lim_{z\to\zeta_i}(z - \zeta_i)f(z) = 0$ for each i. ⌟

Proof: The necessary is clear. For the other direction, choose for each ζ_i a disk $D(\zeta_i, \delta)$ contained in Ω with boundary γ, then for any $z_0 \in D(\zeta_i, \delta)$, by Cauchy theorem(11.4.2.2) applied to the analytic function $F(z) = \frac{f(z)-f(z_0)}{z-z_0}$ on $D(z_0, \delta)\backslash\{z_0, \zeta_i\}$, we see

$$\int_\gamma \frac{f(\xi)}{\xi - z_0} \mathrm{d}\xi = \int_\gamma \frac{f(z_0)}{\xi - z_0} = f(z_0)(11.4.2.5).$$

But by(11.4.2.4), $z \mapsto \int_\gamma \frac{f(\xi)}{\xi - z} \mathrm{d}\xi$ is a holomorphic function on $D(\zeta_i, \delta)$, and it extends $f(z_0)$. So f can be extended to an analytic function $f \in \mathcal{O}(\Omega)$. □

Def. (11.4.2.19)[Orders of Vanishing]. For any region $\Omega \subset \mathbb{C}$ and $f \neq 0 \in \mathcal{O}(\Omega)$, then for any $z_0 \in \Omega$, there exists a smallest $n \in \mathbb{N}$ s.t. $f^{(n)}(z_0) \neq 0$ by(11.4.2.17). So by repeatedly using(11.4.2.18) on $\frac{f(z)}{z-z_0}$, we get

$$f(z) = (z - z_0)^n f_n(z)$$

on a nbhd of z_0, where $f_n \in \mathcal{O}(\Omega')$ and $f_n(z_0) \neq 0$ for some nbhd Ω' of $z_0 \in \Omega$. Such an n is called the **order of vanishing** of f at z_0.

In particular, if $n > 0$, $f_n(z) \neq 0$ on a nbhd of z_0, so $f(z) \neq 0$ on nbhd of z_0, thus the vanishing point of f is isolated in Ω. ⌟

Cor. (11.4.2.20) [Uniqueness]. If the zeros of a holomorphic function f has a convergent point in the domain of definition, then $f = 0$. In particular, if $f, g \in \mathcal{O}(\Omega)$ satisfies $f(z) = g(z)$ for any $z \in E$, where $E \subset \Omega$ is a subset with convergence points in Ω, then $f = g \in \mathcal{O}(\Omega)$. ⌟

Prop. (11.4.2.21) [Singularities]. If $\Omega \subset C$ is region and Ω' is the region obtained from $\Omega\backslash E$ where $E = \{\zeta_1, \dots \zeta_n, \dots\} \subset \Omega$ is a discrete subset. Suppose $f \in \mathcal{O}(\Omega')$, then f is said to have a **singularity** at ζ_i. For each i, let $\zeta = \zeta_i$, the following are all the cases:

- $\lim_{z\to\zeta} |z - \zeta|^\alpha |f(z)| = 0$ for any $\alpha \in \mathbb{R}$. In this case, $f = 0 \in \mathcal{O}(\Omega)$.
- there exists $h \in \mathbb{R}$ s.t. $\lim_{z\to\zeta} |z - \zeta|^\alpha |f(z)| = \begin{cases} 0 & ,\alpha < h \\ \infty & ,\alpha > h \end{cases}$. In this case, $h \in \mathbb{Z}$, and z_0 is called a **zero** of f if $h > 0$ and **pole** of f if $h < 0$. And if $h = 0$, it is called a **removable singularity**, which is discussed in(11.4.2.18).
- Neither of the above holds. In this case, z_0 is called a **essential singularity** of f.

⌟

Proof: In case 1, f can be extended to a function on $\Omega' \cup \{\zeta\}$ with $f(\zeta) = 0$ by(11.4.2.18), and at this point, all the derivatives of f vanish by(11.4.2.19), so $f = 0 \in \mathcal{O}(\Omega)$ by(11.4.2.20).

In case 2, $|z-\zeta|^m|f(z)|=0$ for some $m\in\mathbb{Z}$ larger than h, so $(z-\zeta)^m f(z)$ can be extended to a function on $\Omega'\cup\{\zeta\}$. As f is not identically zero, $(z-\zeta)^m f(z)$ has a finite order of vanishing at ζ, so $(z-\zeta)^m f(z)=(z-\zeta)^k f_k(z)$ for some $k\in\mathbb{Z}$, and f_k is analytic on a nbhd of ζ, by(11.4.2.19). Thus $f(z)=(z-\zeta)^{k-m}f_k(z)$, and clearly h is an integer. □

Def. (11.4.2.22)[Meromorphic Functions]. Situation as in(11.4.2.21), if all the singularities of f on Ω are zeros or poles, f is called a **meromorphic function** on Ω. Notice the poles and zeros of f are discrete. The space of meromorphic functions on Ω is denoted by $\mathcal{M}(\Omega)$. $\mathcal{M}(\Omega)$ is a field. ⌟

Prop. (11.4.2.23). $\mathcal{M}(\Omega)$ is a field, and for any $f\in\mathcal{M}(\Omega)$ and $z_0\in\Omega$, either $f(z_0)\neq 0$, or $f(z)=(z-z_0)^{n_{z_0}}g(z)$ for some $n_{z_0}\in\mathbb{Z}$ and $g(z)\in\mathcal{M}(\Omega)$ s.t. $g(z_0)\neq 0$. ⌟

Proof: This follows from(11.4.2.21) and(11.4.2.18). □

Prop. (11.4.2.24)[Maximum Principle]. Let $f(z)$ be analytic and non-constant on a region Ω, then its absolute value attains no minimum or maximum on Ω. ⌟

Proof: This follows easily from Cauchy's integral formula(11.4.2.6). Notice if its attains an extremal at $z_0\in\Omega$, then the Cauchy integral implies that f is constant on a small circle surrounding z_0, so it is constant by uniqueness theorem(11.4.2.20). □

Prop. (11.4.2.25) [Analytic Functions on Annulus]. If $0\leq r<R\leq\infty$ and f is holomorphic on $\{z\in\mathbb{C}|r\leq|z|\leq R\}$, show that f has a series expansion

$$f=\sum_{n\in\mathbb{Z}}a_nz^n$$

⌟

Proof: For $\zeta\in C_R$,

$$\frac{1}{\zeta-z}=\frac{1}{\zeta}\cdot\frac{1}{1-\frac{z}{\zeta}}=\sum_{n\in\mathbb{N}}\frac{z^n}{\zeta^{n+1}},$$

and the convergence is uniform on C_R, so

$$\frac{1}{2\pi\mathrm{i}}\int_{C_R}\frac{f(\zeta)}{\zeta-z}\mathrm{d}\zeta=\sum_{n\in\mathbb{N}}\underbrace{\Big(\frac{1}{2\pi\mathrm{i}}\int_{C_R}\frac{f(\zeta)}{\zeta^{n+1}}\Big)}_{a_n}z^n.$$

Similarly, for $\zeta\in C_r$,

$$\frac{1}{\zeta-z}=\frac{1}{z}\cdot\frac{1}{1-\frac{\zeta}{z}}=\sum_{n\in\mathbb{N}}\frac{\zeta^n}{z^{n+1}},$$

and the convergence is uniform on C_R, so

$$\frac{1}{2\pi\mathrm{i}}\int_{C_r}\frac{f(\zeta)}{\zeta-z}\mathrm{d}\zeta=\sum_{n\in\mathbb{Z}+}\underbrace{\Big(\frac{1}{2\pi\mathrm{i}}\int_{C_r}f(\zeta)\zeta^{n-1}\Big)}_{a_{-n}}z^{-n}.$$

Thus it follows form the Cauchy integral formula(11.4.2.6) that

$$f(z)==\frac{1}{2\pi\mathrm{i}}\int_{C_R}\frac{f(\zeta)}{\zeta-z}\mathrm{d}\zeta-\frac{1}{2\pi\mathrm{i}}\int_{C_r}\frac{f(\zeta)}{\zeta-z}\mathrm{d}\zeta=\sum_{n\in\mathbb{Z}}a_nz^n,$$

and the convergence is uniform on the annulus. □

Residues

Def. (11.4.2.26) [Residues]. If $\Omega \subset \mathbb{C}$ is a simply-connected region and f is a function on Ω analytic except for isolated singularities $\{a_j\}$, then for each i, if $\mathbb{D}(a_i, \delta)$ is a nbhd of a_i contained in Ω and contains no other singularities of f, then define

$$\operatorname{res}_{z=a_i} f = \frac{1}{2\pi \mathrm{i}} \int_\gamma f(z)\mathrm{d}z,$$

where $\gamma = \partial\mathbb{D}(a_i, \delta)$. This quantity is invariant of the nbhd chosen by Cauchy's theorem(11.4.2.2), and is called the **residue** of f at a_i. ⌟

Thm. (11.4.2.27) [Residue theorem]. If $\Omega \subset \mathbb{C}$ is a simply-connected region and f is a function on Ω analytic except for isolated singularities $\{a_j\}$, then for any piecewise C^1 closed curve $\gamma \subset \Omega$ not passing through the singularities,

$$\frac{1}{2\pi \mathrm{i}} \int_\gamma f(z)\mathrm{d}z = \sum_i n(\gamma, a_i) \operatorname{res}_{z=a_i} f,$$

where the RHS is a finite sum. ⌟

Proof: This is because the interior of γ contains only f.m. singularity points, and γ is homologous to a linear combination of cycles around each singularity with multiplicity $n(\gamma, a_i)$. □

Prop. (11.4.2.28). For $n \in \mathbb{Z}$,

$$\operatorname{res}_{z=0} z^n = \begin{cases} 1 & , n = -1 \\ 0 & , n \neq -1 \end{cases}.$$

In particular, if locally near $z = 0$, $f(z) = \sum_{n\in\mathbb{Z}} a_n z^n$, then

$$\operatorname{res}_{z=0} f(z) = a_{-1}.$$

⌟

Proof:

$$\begin{aligned} \int_{|z|=r} z^n \mathrm{d}z = \int_0^{2\pi} z^n(t) z^\backprime(t)\mathrm{d}t = \int_0^{2\pi} \mathrm{i}\, r^{n+1} e^{\mathrm{i}(n+1)t}\mathrm{d}t \\ = \begin{cases} \frac{r^{n+1}}{n+1} e^{\mathrm{i}(n+1)t}\Big|_{t=0}^{2\pi} = 0 & , n \neq -1 \\ 2\pi \mathrm{i} & , n = -1 \end{cases} \end{aligned}$$

□

Prop. (11.4.2.29). If $\Omega \subset \mathbb{C}$ is a region and f is a function on Ω analytic with singularities. If f is analytic around $z_0 \in \Omega$, then for $n \in \mathbb{Z}_+$, by(11.4.2.7),

$$\operatorname{res}_{z=z_0} \frac{f(z)}{(z - z_0)^n} = \frac{f^{(n-1)}(z_0)}{(n-1)!}.$$

⌟

Prop. (11.4.2.30) [Generalized Argument Principle]. If $\Omega \subset \mathbb{C}$ is a simply-connected region and $f \in \mathcal{M}(\Omega)$ with zeros $\{a_i\}$ and poles $\{b_i\}$, and $g(z) \in \mathcal{O}(\Omega)$, then for any piecewise C^1 closed curve $\gamma \subset \Omega$ not passing through zeros or poles of f,

$$\frac{1}{2\pi\,\mathrm{i}}\int_\gamma g(z)\frac{f'(z)}{f(z)}\mathrm{d}z = \sum_i n(\gamma, a_i)g(a_i) - \sum_j n(\gamma, b_j)g(b_i)$$

where the RHS is a finite sum, and counted with multiplicity by the order.

Moreover, notice if Γ is the closed curve $f \circ \gamma$, then

$$\frac{1}{2\pi\,\mathrm{i}}\int_\gamma \frac{f'(z)}{f(z)}\mathrm{d}z = \frac{1}{2\pi\,\mathrm{i}}\int_\Gamma \frac{1}{z}\mathrm{d}z = n(\Gamma, 0).$$

⌟

Proof: Notice if $z_0 \in \Omega$ and $f(z) = (z - z_0)^h f_h(z)$ near z_0 where $h \in \mathbb{Z}$, $f_h(z)$ is analytic on a nbhd of z_0 and $f_h(z_0) = 0$, then

$$g(z)\frac{f'(z)}{f(z)} = \frac{hg(z)}{z - z_0} + f_h'(z)g(z),$$

so $\mathrm{res}_{z=z_0}[g(z)\frac{f'(z)}{f(z)}] = hg(z_0)$ by(11.4.2.29) and(11.4.2.5). Thus the assertion follows from the residue formula(11.4.2.27) applied to the meromorphic function $F = gf'/f \in \mathcal{M}(\Omega)$. □

Cor. (11.4.2.31) [Rouché]. If $\Omega \subset \mathbb{C}$ is a region and $\gamma \subset \Omega$ is a piecewise C^1 closed curve that is a boundary of a subset of Ω homeomorphic to a $\mathbb{D}$. Suppose $f, g \in \mathcal{O}(\Omega)$ satisfies $|f(z) - g(z)| < |f(z)|$ for $z \in \gamma$, then $f(z)$ and $g(z)$ have the same number of zeros or poles on the interior of γ. ⌟

Proof: This follows from the argument principle(11.4.2.30) applied to the meromorphic function $F = f/g \in \mathcal{M}(\Omega)$. Notice that $n(\gamma, a) = 1$ for any a in the interior of γ, and $n(F \circ \gamma, 0) = 0$ because

$$|F(z) - 1| < 1$$

For $z \in \gamma$ by hypothesis. □

Logarithm

Def. (11.4.2.32) [Branch of Logarithm]. Let $\Omega \subset \mathbb{C}^\times$ be a region, a branch of **logarithm** is an analytic function $\ell \in (\Omega)$ s.t. $e^{\ell(z)} = z$.

By connectedness, If no confusion is made, we will denote any branch of logarithm by log. ⌟

Prop. (11.4.2.33). If $\Omega \subset \mathbb{C}$ is a simply-connected region, and $f \in \mathcal{O}(\Omega)$ is non-vanishing, then there exists some $g \in \mathcal{O}(\Omega)$ s.t. $f(z) = e^{g(z)}$. ⌟

Proof: By(11.4.2.3), there exists $\ell \in \mathcal{O}(\Omega)$ s.t. $g' = \frac{f'}{f}$ and we can assume $e^{g(z_0)} = f(z_0)$ for some $z_0 \in \Omega$ because $\exp : \mathbb{C} \to \mathbb{C}^\times$ is clearly surjective. Then notice $[f(z)\exp(-g(z))]' = \exp(-g(z))(f'(z) - f(z)g'(z)) = 0$, so $f(z)\exp(-g(z)) = 0$. □

Cor. (11.4.2.34) [Existence of Logarithm]. If $\Omega \subset \mathbb{C}^\times$ be simply-connected region, then there exists a branch of logarithm on Ω, and also a branch of $\sqrt[n]{f}$ on Ω. ⌟

3 Series and Product Developments

Prop. (11.4.3.1) [Abel-Hadamard]. For any power series $a_0 + a_1 z + \ldots + a_n z^n + \ldots \in \mathbb{C}[[z]]$, take $1/R = \overline{\lim} |a_n|^{1/n}$, where we assume $1/0 = \infty$ and $1/\infty = 0$, then

- The series converges absolutely for every $|z| < R$, and if $\rho < R$, then the convergence is uniform for $|z| \leq \rho$.
- If $|z| > R$, the terms are unbounded, and the series diverges.

And R is called the **radius of convergence** of the sequence. Notice the radius of convergence is the same as that of $|a_0| + |a_1| z + \ldots + |a_n| z^n + \ldots$ in $\mathbb{R}$(11.3.5.3). ⌟

Proof: 1: For $0 < \rho < R$, take $\rho_1 \in (\rho, R)$, then the definition of R implies that for some $N \in \mathbb{Z}_+$ and any $n \geq N$, $|a_n| \leq R^{-n} < \rho_1^{-n}$, so $|a_n z^n| \leq (\rho/\rho_1)^n$, so $\sum_{n\in\mathbb{N}} a_n z^n$ converges absolutely and uniformly for $|z| \leq \rho$.

2: For $R < |z|$, the definition of R implies that for any $N \in \mathbb{Z}_+$, there exists $n \geq N$ s.t. $|a_n| \geq R^{-n}$, so $|a_n z^n| \geq |z/R|^n > 1$, so this sequence cannot be convergent. □

Cor. (11.4.3.2). By(11.3.5.4) and(11.4.3.1), for any power series $a_0 + a_1 x + \ldots + a_n x^n + \ldots$ in $\mathbb{R}$, if $\lim_{n\to\infty} \frac{|a_{n+1}|}{|a_n|} = \rho \in [0, \infty]$, then the radius of convergence(11.4.3.1) $R = 1/\rho$, where we assume $1/0 = \infty$ and $1/\infty = 0$. ⌟

Prop. (11.4.3.3). The power series $a_0 + a_1 z + \ldots + a_n z^n + \ldots$ defines an analytic function $f(z)$ on its disk of convergence. And also

$$f'(z) = \sum_{n\in\mathbb{N}} n a_n z^{n-1}.$$

In particular, $f(z)$ is infinite differentiable in its disk of convergence. ⌟

Proof: The partial sum converges to f uniformly on compact subset of the disk of convergence(11.4.3.1), so this follows from(11.4.2.15). □

Prop. (11.4.3.4). Any holomorphic function f defined on the punctured disk $0 < |z| < 1$ is of the form

$$f(z) = \sum_{n\in\mathbb{Z}} a_n z^n$$

where $\overline{\lim}_{n\to\infty} |a_n|^{1/n} \leq 1$, and $\lim_{n\to\infty} |a_{-n}|^{1/n} = 0$. ⌟

Proof:

□

Prop. (11.4.3.5). If $f \in C((0,1])$ has an expansion

$$f(x) = \sum_{\nu\in\Sigma} a(\nu) x^\nu$$

near $x = 0$, where $\Sigma \subset \mathbb{R}$ is a discrete subset bounded from below, then

$$\int_0^1 f(x) x^s \frac{dx}{x}$$

has meromorphic continuation to all $s \in \mathbb{C}$, and has only simple poles at $s \in -\Sigma$, and the residue at $s = -\nu$ is $a(\nu)$. Moreover, for any $N \in \mathbb{R}$, f is essentially bounded on $\mathrm{Re}(s) > -N$. ⌟

Proof: For any $N \in \mathbb{R}$, let

$$f(x) = \sum_{\nu\in\Sigma,\nu<N} a(\nu)x^\nu + R(x), \quad R(x) = O(x^N),$$

then

$$\int_0^1 f(x)x^s\frac{dx}{x} = \sum_{\nu\in\Sigma,\nu<N}\frac{a(\nu)}{s+\nu} + \int_0^1 R(x)x^s\frac{dx}{x}.$$

□

Prop. (11.4.3.6) [Trigonometric Functions]. The exponential function

$$\exp(z) = \sum_{n\in\mathbb{N}}\frac{z^n}{n!}(9.5.1.5)$$

is convergent and analytic on $\mathbb{C}$, by(11.4.3.1), and it is also denoted by e^z. We can also define the **trigonometric functions**

$$\cos(z) = \frac{e^{\mathrm{i}\,z}+e^{-\mathrm{i}\,z}}{2} = \sum_{n\in\mathbb{N}}(-1)^n\frac{z^{2n}}{(2n)!}, \quad \sin(z) = \frac{e^{\mathrm{i}\,z}-e^{-\mathrm{i}\,z}}{2\,\mathrm{i}} = \sum_{n\in\mathbb{N}}(-1)^n\frac{z^{2n+1}}{(2n+1)!},$$

which are analytic on $\mathbb{C}$. ⌟

Prop. (11.4.3.7) [Eulerian Identity]. The smallest positive real number ρ that $e^{\mathrm{i}\,\rho}+1=0$ is π. In particular, the Eulerian identity $e^{\pi\,\mathrm{i}}+1=0$ holds. ⌟

Proof: □

Prop. (11.4.3.8) [Infinite Products]. For a sequence $(b_n)\in\mathbb{C}\backslash\{-1\}$, the infinite product $\prod_{n\in\mathbb{Z}_+}(1+b_n)$ is said to **converge** if the sequence

$$\Pi_m = \prod_{n=1}^m(1+b_n)$$

converges. It is said to **converge absolutely** if $\prod_{n\in\mathbb{Z}_+}\log(1+b_n)$ converges absolutely. Then:

- If $\prod_{n\in\mathbb{Z}_+}(1+b_n)$ converges absolutely, then $\prod_{n\in\mathbb{Z}_+}(1+b_n)$ converges to a non-zero limit.
- $\prod_{n\in\mathbb{Z}_+}(1+b_n)$ converges absolutely iff $\sum_{n\in\mathbb{Z}_+}b_n$ converges absolutely.
- If $(a_n)\in\mathbb{C}$ and $\sum_{n\in\mathbb{Z}_+}a_n$ converges absolutely, then $\prod_{n\in\mathbb{Z}_+}(1+a_n)=0$ iff $a_k=-1$ for some k.

⌟

Proof: 1: $\prod_{n\in\mathbb{Z}_+}(1+b_n) = \exp(\sum_n\log(1+b_n))$.

2: It follows from the fact $\lim_{z\to 0}\frac{\log(1+z)}{z}=1$ that there exists a $0<\varepsilon<1/2$ that

$$(1-\varepsilon)|a_n| < |\log(1+a_n)| \le (1+\varepsilon)|a_n|$$

for n sufficiently large.

3: By omitting f.m. terms, this follows from item2. □

Prop. (11.4.3.9). If (F_n) is a sequence of holomorphic functions on a region Ω, and there exists constants $c_n > 0$ s.t.

$$\sum c_n < \infty, |F_n(z) - 1| \leq c_n, \forall z \in \Omega,$$

then

- The product $\prod_n F_n(z)$ converges uniformly on Ω to a holomorphic function $F(z)$.
- If $F_n \neq 0$ for any n, then

$$\frac{F'(z)}{F(z)} = \sum_n \frac{F_n'(z)}{F_n(z)}.$$

- If $F_n \neq 0$ for any n, then the zeros of $F(z)$ are exactly zeros of $F_n(z)$(counting multiplicity).

Proof: 1: The proof is the same as that of(11.4.3.8), and notice that the convergence is uniform so the resulting function is holomorphic.

2: we can omit f.m. terms, so we may assume that each F_n is non-vanishing. Let $G_N(z) = \prod_{k=1}^N F_n(z)$, then $G_N(z) \to F(z)$ uniformly on compact subsets. So by(11.4.2.15), G_N' converges to $F'(N)$ uniformly on compact subset, and

$$\frac{F'(z)}{F(z)} = \lim_{N\to\infty} \frac{G_N'(z)}{G_N(z)} = \sum_n \frac{F_n'(z)}{F_n(z)}.$$

3: This is because we can omit f.m. terms and assume that each F_n is non-vanishing. Then the resulting □

Partial Fractions

Def. (11.4.3.10).

Prop. (11.4.3.11).

$$\pi\cot(\pi z) = \frac{1}{z} + \sum_{n\neq 0\in\mathbb{Z}} (\frac{1}{z-n} + \frac{1}{n}) = \frac{1}{z} + \sum_{n\in\mathbb{Z}_+} \frac{2z}{z^2-n^2} = \frac{1}{z} - 2\sum_{k\in\mathbb{Z}_+} \zeta(2k) z^{2k-1}.$$

Proof: This follows from taking logarithmic derivative of the Hadamard product of $\sin(\pi z)$(11.4.3.23). □

Cor. (11.4.3.12).

$$\frac{\pi^2}{\sin^2(\pi z)} = \sum_{n\in\mathbb{Z}} \frac{1}{(z-n)^2}.$$

Proof: This follows form taking derivative of(11.4.3.12). □

Entire Functions

Thm. (11.4.3.13) [Product Development, Weierstrass].

- If f is an entire function, then the zeros of f is at most countable(counting multiplicity), and if they can be ordered by their modules, $|a_1| \leq |a_2| \leq \ldots \leq |a_n| \leq$ with $\lim_{n\to\infty} |a_n| = \infty$.
- If $S \subset \mathbb{Z}_+$, and $(a_n)_{n\in S} \subset \mathbb{C}$ be a sequence of complex numbers, which satisfies $\lim_{n\to\infty} a_n = \infty$ when $\#S = \infty$, then every entire function with (a_n) as zeros(counting multiplicity) can be written in the form

$$f(z) = z^m e^{g(z)} \prod_{n\in S} \Big[(1 - \frac{z}{a_n}) \exp(\frac{z}{a_n} + \frac{1}{2}(\frac{z}{a_n})^2 + \ldots + \frac{1}{m_n}(\frac{z}{a_n})^{m_n})\Big]$$

for some sequence $(m_n)_{n\in S}$ of positive integers.

⌟

Proof: Firstly, for any such sequence, the RHS converges to an entire function: for any $z \in \mathbb{C}$, we can discard f.m. terms s.t. $|a_n| \leq |z|$, and for $|a_n| > |z|$,

$$(1 - \frac{z}{a_n}) \exp(\frac{z}{a_n} + \frac{1}{2}(\frac{z}{a_n})^2 + \ldots + \frac{1}{m_n}(\frac{z}{a_n})^{m_n}) = \exp(-\frac{1}{m_n+1}(\frac{z}{a_n})^{m_n+1} - \frac{1}{m_n+2}(\frac{z}{a_n})^{m_n+2} - \ldots)$$

and the module of the exponent is bounded by

$$\frac{1}{m_n+1}(\frac{|z|}{|a_n|})^{m_n+1}(1 - \frac{|z|}{|a_n|})^{-1}$$

So if we choose $m_n = n$, the RHS converges in a nbhd of z, and it is entire.

Then any such function with the desired zeros differ by the RHS by an entire non-vanishing function, which must be of the form $\exp(g(z))$ by(11.4.2.34). □

Cor. (11.4.3.14). Any entire function on $\mathbb{C}$ is a quotient of two meromorphic functions. ⌟

Cor. (11.4.3.15). If $S \subset \mathbb{Z}_+$, and $(a_n)_{n\in S}, (A_n)_{n\in S} \subset \mathbb{C}$ be two sequence of complex numbers s.t. $a_m \neq a_n$ for $m \neq n$, which satisfies $\lim_{n\to\infty} a_n = \infty$ when $\#S = \infty$, then there exists an entire function $f(z)$ which satisfies $f(a_n) = A_n$. ⌟

Proof: Let $g(z)$ be an entire function satisfying $g(z)$ has simple zeros at a_n, then consider

$$f(z) = \sum_{n\in S} g(z) \frac{e^{\gamma_n(z-a_n)}}{z - a_n} \frac{A_n}{g'(a_n)}.$$

□

Def. (11.4.3.16) [Genus of Entire Functions and Canonical Products]. The **genus of an entire function** f is the smallest $h \in \mathbb{N}$ s.t. f can be written in the form

$$f(z) = z^m e^{g(z)} \prod_{n\in S} \Big[(1 - \frac{z}{a_n}) \exp(\frac{z}{a_n} + \frac{1}{2}(\frac{z}{a_n})^2 + \ldots + \frac{1}{h}(\frac{z}{a_n})^h)\Big]$$

where $S \subset \mathbb{N}, m \in \mathbb{N}, g(z)$ is a polynomial of degree$\leq h$. if no such h exists, f is said to have genus ∞.

In view of the Weierstrass theorem(11.4.3.13), this h is equal to the minimal non-negative integer s.t.

$$\sum_{n\in\mathbb{Z}_+} |a_n|^{-h-1} < \infty.$$

If f has finite genus, then the canonical form of f is unique. ⌟

Def. (11.4.3.17) [Order of Growth]. The **order of growth** of an entire function f is defined to be

$$\lambda = \overline{\lim_{r\to\infty}} \frac{\log\log \max_{|z|=r}|f(z)|}{\log r},$$

or equivalently the smallest number $\lambda \in \mathbb{R}\cup\{\infty\}$ s.t.

$$\max_{|z|=r}|f(z)| \le e^{r^{\lambda+\varepsilon}}$$

for any $\varepsilon > 0$. ⌟

Lemma (11.4.3.18). Let f be an entire function with order of growth ρ.

- For $r \in \mathbb{R}_+$, let $N(r)$ be the number of zeros of f in $\mathbb{D}(0, r)$, then for any $\varepsilon > 0$, there exists $C > 0$ s.t. $N(r) \le Cr^{\rho+\varepsilon}$ for r sufficiently large.
- Let $\{a_n\}_{n\in\mathbb{Z}_+}$ be the zeros of f, then for any $\varepsilon > 0$, $\sum_{k\in\mathbb{N}} |a_k|^{-\rho-\varepsilon} < \infty$.

⌟

Proof: 1: dividing $f(z)$ by a power of z, we may assume $f(0) \ne 0$. Then it follows from the Jensen formula(11.5.2.11) on the disk $\mathbb{D}(0, 2\rho)$ that

$$N(r)\log 2 \le \frac{1}{2\pi}\int_0^{2\pi} \log|f(2re^{\mathrm{i}\theta})|\mathrm{d}\theta - \log|f(0)| \le (2r)^{\rho+\varepsilon} - \log|f(0)|.$$

2: By item1, for n large, $n \le N(|a_n|) \le |a_n|^{\rho+\varepsilon/2}$, so

$$\sum |a_n|^{-\rho-\varepsilon} \le \sum_{n\in\mathbb{Z}_+} |n|^{-\frac{\rho+\varepsilon}{\rho+\varepsilon/2}} < \infty.$$

□

Lemma (11.4.3.19). If g is an entire function on $\mathbb{C}$, $\rho \in \mathbb{R}_+$ and there is a sequence of positive real numbers (r_n) that extends to infinity, and $u = \mathrm{Re}(g)$ satisfies

$$\max_{|z|=r_n} u(z) \le Cr_n^{\rho}$$

for each n, then g is a polynomial of degree$\le s$. ⌟

Proof: Let $g(z) = \sum_{n\in\mathbb{N}} a_n z^n$, then for any $k \in \mathbb{Z}_+$, let $r = r_k$, by Cauchy's formula

$$\frac{1}{2\pi}\int_0^{2\pi} g(re^{\mathrm{i}\theta})e^{-\mathrm{i}m\theta}\mathrm{d}\theta = \begin{cases} a_m r^m & , m \in \mathbb{N} \\ 0 & , n \in \mathbb{Z}_- \end{cases},$$

so by taking conjugation and adding,

$$\frac{1}{\pi}\int_0^{2\pi} \mathrm{Re}(g)(re^{\mathrm{i}\theta})e^{-\mathrm{i}n\theta}\mathrm{d}\theta = \begin{cases} a_n r^n & , n \in \mathbb{Z}_+ \\ \mathrm{Re}(a_0) & , n = 0 \end{cases}.$$

Then for $n \in \mathbb{Z}_+$,

$$|a_n| = \frac{1}{\pi r^n}\left|\int_0^{2\pi}[u(re^{\mathrm{i}\theta}) - Cr^{\rho}]e^{-\mathrm{i}n\theta}\mathrm{d}\theta\right| \le \frac{1}{\pi r^n}\int_0^{2\pi}[Cr^{\rho} - u(re^{\mathrm{i}\theta})]\mathrm{d}\theta = 2Cr^{s-n} - 2\,\mathrm{Re}(a_0)r^{-n}.$$

Then letting $r = r_k \to \infty$ finishes the proof. □

Thm. (11.4.3.20) [Hadamard]. The genus h and the order λ of an entire function f satisfies

$$0 \le h \le \lambda \le h+1 \le \infty.$$

(Notice if $\lambda \in \mathbb{Z}$, it might not be able to determine h from λ). ⌟

Proof: It follows from the proof of Weierstrass theorem(11.4.3.13) that is f is of genus $h < \infty$, then $\lambda \le h+1$(taking $m_n = h$ for each n). Conversely, if f has order of growth $\lambda < \infty$, then we need to show that $h \le \lambda$. Take $h = \lfloor \lambda \rfloor$, and let (a_n) are zeros of f(counting multiplicity and ordered by modulus), then firstly, we show that the product

$$\prod_{n\in S}\Big[(1-\frac{z}{a_n})\exp(\frac{z}{a_n}+\frac{1}{2}(\frac{z}{a_n})^2+\ldots+\frac{1}{h}(\frac{z}{a_n})^h)\Big]$$

converges: For this, by the proof of Weierstrass theorem(11.4.3.13), it suffices to show that $\sum_{n\in S}|a_n|^{-h-1}$ converges, and this follows from(11.4.3.18).

Then it's left to show that the entire function $g(z)$ as in(11.4.3.13) is a polynomial of degree$\le h$. For this, firstly we prove that if $\varepsilon > 0$ is small that $\rho+\varepsilon < h+1$, and $|z-a_n| \ge |a_n|^{h+1}$ for any $n \in S$, then there exists $C \in \mathbb{R}_+$ s.t.

$$\Big|\prod_{n\in S}\Big[(1-\frac{z}{a_n})\exp(\frac{z}{a_n}+\frac{1}{2}(\frac{z}{a_n})^2+\ldots+\frac{1}{h}(\frac{z}{a_n})^h)|\Big]\Big| \ge e^{-C|z|^{\rho+\varepsilon}}.$$

Deonte $E_h(s) = (1-s)\exp(s+\frac{1}{2}s^2+\ldots+\frac{1}{h}s^h)$, we use a lemma:

Lemma (11.4.3.21). there exists constant C s.t.

- If $|s| \le 1/2$, $|E_h(s)| \ge e^{-C|z|^{h+1}}$.
- If $|s| \ge 1/2$, $|E_h(s)| \ge |(1-s)|e^{-C|z|^h}$.

⌟

Proof: For $|s| \ge 1/2$,

$$|E_h(s)| \ge |(1-s)|e^{-|s|-\frac{|s|^2}{2}-\ldots-\frac{|s|^h}{h}} \ge |(1-s)|e^{-C|z|^h}.$$

And for $|s| \le 1/2$,

$$|E_h(s)| \ge |(1-s)|e^{-\frac{|s|^{h+1}}{h+1}-\frac{|s|^{h+2}}{h+}-\ldots} \ge e^{-C|z|^{h+1}}.$$

□

Then if $|a_n| \ge 2|z|$,

$$|E_h(\frac{z}{a_n})| \ge e^{-C|z/a_n|^{h+1}} \ge e^{-C|z/a_n|^{\rho+\varepsilon}},$$

and if $|a_n| \le 2|z|$, by the hypothesis,

$$|E_h(\frac{z}{a_n})| \ge |(1-\frac{z}{a_n})|e^{-C|z/a_n|^h} \ge |a_n|^{-h-2}e^{-C|z/a_n|^{\rho+\varepsilon}}.$$

Thus by(11.4.3.18),

$$\prod_{n\in S}|E_h(\frac{z}{a_n})| \ge e^{-C'z}\prod_{|a_n|\le 2|z|}|a_n|^{-h-2} \ge e^{-C'z}|2z|^{-(h+2)N(2|z|)} \ge e^{-C''|z|^{\rho+\varepsilon'}}$$

for any $\varepsilon' > \varepsilon$.

Finally, we get

$$e^{\mathrm{Re}(g(z))} = |e^{g(z)}| = |\frac{f(z)}{\prod_{n\in S}|E_h(\frac{z}{a_n})|}| \leq Ce^{\rho+\varepsilon}$$

whenever $|z-a_n| \geq |a_n|^{h+1}$ for any $n \in S$. Then as $\sum_n |a_n|^{h+1} < \infty$, we can apply(11.4.3.19) to show that g is a polynomial of degree $\leq \rho + \varepsilon < h+1$, thus we are done. □

Cor. (11.4.3.22). For an entire function f with order $\lambda \in \mathbb{R}_+ \setminus \mathbb{Z}_+$, then $\#f^{-1}(a) = \infty$ for any $a \in \mathbb{C}$. ⌟

Proof: As f and $f-a$ has the same order, it suffices to show that such an f has i.m. zeros. Suppose it has only f.m. zeros, then we can divide a polynomial $P(z)$ and see that $F(z) = f(z)/P(z)$ also has the same order but no zero. Thus $F(z) = e^{g(z)}$ for some entire g. But then g is a polynomial of degree λ, which is impossible. □

Example (11.4.3.23) [Canonical Forms].

$$\sin(\pi z) = \pi z \prod_{n\in\mathbb{Z}^\times}[(1-\frac{z}{n})e^{z/n}] = \pi z\prod_{n=1}^\infty(1-\frac{z^2}{n^2}).$$

is of genus 1 and order of growth 1. ⌟

Proof: $|\sin(\pi z)| \leq e^{\pi|z|}$, so it has order of growth≤ 1, and it has a simple zero at $z=0$, so by Hadamard's theorem(11.4.3.20),

$$\sin(\pi z) = \pi z e^{Az+B}\prod_{n\neq 0\in\mathbb{Z}}[(1-\frac{z}{n})e^{z/n}] = \pi z e^{Az+B}\prod_{n=1}^\infty(1-\frac{z^2}{n^2})$$

for some $A, B \in \mathbb{C}$. Letting $z \to 0$ implies that $B = 0$. And letting $z \to 1$ implies that

$$e^A = 2\prod_{n=1}^\infty(1-\frac{1}{n^2}) = 1,$$

so $A = 0$. □

4 Analytic Continuations

Lemma (11.4.4.1) [Symmetry Principle]. If $\Omega \subset \mathbb{C}$ is a region s.t. $\mathsf{c}(\Omega) = \Omega$, denote $\Omega^+ = \Omega \cap \mathscr{H}$, $\Omega^- = \mathsf{c}(\Omega^+)$, $I = \Omega \cap \mathbb{R}$. Suppose $f^+ \in \mathcal{O}(\overline{\Omega^+})$, $f^- \in \mathcal{O}(\overline{\Omega^-})$, and $f^+(z) = f^-(z)$ for $z \in \mathbb{R}$, then the function

$$f: \Omega \to \mathbb{C}: z \mapsto \begin{cases} f^+(z) & , z \in \overline{\Omega^+} \\ f^-(z) & , z \in \Omega^- \end{cases}$$

is analytic on Ω. ⌟

Proof: f is clearly continuous. Thus it is easily seen to be analytic by Morera's theorem(11.4.2.8). □

Prop. (11.4.4.2) [Schwarz Reflection Principle]. If $\Omega \subset \mathbb{C}$ is a region s.t. $\mathsf{c}(\Omega) = \Omega$, denote $\Omega^+ = \Omega \cap \mathscr{H}$, $\Omega^- = \mathsf{c}(\Omega^+)$, $I = \Omega \cap \mathbb{R}$. Suppose $f^+ \in \mathcal{O}(\overline{\Omega^+})$ satisfies $f(I) \subset \mathbb{R}$, then f^+ can be analytically extended to an analytic function on Ω. ⌟

Proof: For $z \in \Omega^-$, define $f(z) = \overline{f(\overline{z})}$, then f is a continuous function on Ω, because for $z \in I$, $f(z) = \overline{f(\overline{z})}$. To show that f is analytic, by(11.4.4.1), it suffices to show that f is analytic on Ω^-: For any $z_0 \in \Omega^-$, if z is close to z_0, then $\overline{z}, \overline{z}_0 \in \Omega^+$. By Taylor expansion of f around $\overline{z}_0$(11.4.2.16)

$$f(z) = \overline{f(\overline{z})} = \overline{\sum_{n\in\mathbb{N}} a_n(\overline{z} - \overline{z}_0)^n} = \sum_{n\in\mathbb{N}} \overline{a}_n (z - z_0)^n.$$

And this is a power series around z_0 with the same radius of convergence as that of $\overline{z}_0$, thus f is analytic around z_0. Because z_0 is arbitrary, f is analytic on Ω^-. □

Cor. (11.4.4.3). If $\Omega \subset \mathbb{C}^\times$ is a region that is stable under the involution $\iota : z \mapsto \overline{z}^{-1}$, denote $\Omega^+ = \Omega \cap \mathscr{H}$, $\Omega^- = \iota(\Omega^+)$, $I = \Omega \cap \partial\mathbb{D}$. Suppose $f^+ \in \mathcal{O}(\overline{\Omega^+})$ satisfies $f(I) \subset \mathbb{R}$, then f^+ can be analytically extended to an analytic function on Ω. ⌟

Proof: For $z \in \Omega^-$, define $f(z) = \overline{f(\iota(z))}$, then f is a continuous function on Ω, because for $z \in I$, $f(z) = \overline{f(\iota(z))}$. To show that f is analytic, by a similar lemma as(11.4.4.1), it suffices to show that f is analytic on Ω^-: For any $z_0 \in \Omega^-$, if z is close to z_0, then $\iota(z), \iota(z_0) \in \Omega^+$. By Taylor expansion of f around $\iota(z_0)$(11.4.2.16)

$$f(z) = \overline{f(\iota(z))} = \overline{\sum_{n\in\mathbb{N}} a_n(\iota(z) - \iota(z_0))^n} = \sum_{n\in\mathbb{N}} \frac{\overline{a}_n}{z_0} \frac{(z - z_0)^n}{z^n} = g(\frac{1}{z}),$$

where $g(z) = \sum_{n\in\mathbb{N}} (-1)^n \overline{a}_n (z - \frac{1}{z_0})^n$ is a power series around z_0 with the same radius of convergence as that of $\overline{z}_0$, so analytic around z_0^{-1}. Thus f is analytic around z_0. Because z_0 is arbitrary, f is analytic on Ω^-. □

5 Theorems

Prop. (11.4.5.1) [Runge's Theorem]. Let K be a compact subset of $\overline{\mathbb{C}}$ and let f be a function which is holomorphic on an open set containing K. If A is a set containing at least one complex number from every bounded connected component of $\overline{\mathbb{C}} \backslash K$, then there exists a sequence of rational functions which converges uniformly to f on K and all the poles of the functions are in A. ⌟

Proof: □

Prop. (11.4.5.2) [Mergelyan]. If K is compact in $\mathbb{C}$ and f is a continuous function on K that is holomorphic in $\mathrm{int}(K)$, then f can be uniformly approximated by polynomials. ⌟

Prop. (11.4.5.3) [Weierstrass]. For a ascending sequence of regions $\Omega_1 \subset \Omega_2 \subset \ldots$, $\cup_n \Omega_n = \Omega$, and f_n is analytic on Ω_n, and $f_n(z)$ converges to a function $f(z)$ in the compact-open topology, then $f(z)$ is also analytic, and moreover, $f'(z)$ converges to $f'(z)$ in the compact-open topology. ⌟

Proof: The analyticity follows from Morera's theorem(11.4.2.8) as the integration on a closed curve commutes with uniform convergence, the same argument applied to the limit of equations

$$f_n'(z) = \frac{1}{2\pi \mathrm{i}} \int_{\partial\mathbb{D}(0,r)} \frac{f_n(\zeta)d\zeta}{(\zeta - z)^2}$$

shows that the derivative also converges, and uniformly on $\overline{\mathbb{D}(0,\rho)}$ for $\rho < r$. □

Cor. (11.4.5.4) [Hurwitz]. Cf.[Ahlfors P178]. ⌟

Thm. (11.4.5.5) [Montel]. If $\Omega \subset \mathbb{C}$ is region and $\mathcal{S} = \{f_\alpha\}$ is a set of holomorphic functions on Ω bounded in the topology of $H(\Omega)$, i.e. inter convex uniform convergence, then $\mathcal{S}$ is sequentially compact in $H(\Omega)$. Equivalently, $\mathcal{O}(\Omega)$ has the Heine-Borel property. ⌟

Proof: By Arzela-Ascoli(4.4.8.8) that it suffices to show that $\mathcal{S}$ is uniformly bounded on any compact subset $K \subset \Omega$. Choose δ small s.t.

$$K_0 = \{z \in \mathbb{C} | d(z, K) \leq 2\delta\} \subset \Omega,$$

then $|f_\alpha(z)| \leq M$ for any $f_\alpha \in \mathcal{S}$ and $z \in K_0$ for some M. So by Cauchy's formula, $|f'_\alpha(z)| \leq \frac{M}{\delta}$ for any $z \in K, f_\alpha \in \mathcal{S}$. Thus it it clear $\mathcal{S}$ are equicontinuous on K. □

Thm. (11.4.5.6) [Little Picard Theorem]. The image of a non-constant entire function $f : \mathbb{C} \to \mathbb{C}$ is either $\mathbb{C}$ or $\mathbb{C}$ with one point omitted. ⌟

Proof: The modular curve $Y(2)$ is the sphere minus three points(19.3.3.4)(20.2.3.14)(20.2.3.16), and the linear transformations of S^1 is triply transitive, thus we can assume f is a analytic map $\mathbb{C} \to Y(2)$. As $\mathbb{C}$ is simply connected, we can lift this map to the covering of $Y(2)$, which is $\mathcal{H}$. But $\mathcal{H}$ is biholomorphic to the open disk, but a bounded entire function is constant(11.4.2.10), so f is constant. □

Thm. (11.4.5.7) [Phragmén-Lindelöf]. Let f be a function that is holomorphic in the upper part of a strip $\sigma_1 \leq \mathrm{Re}(s) \leq \sigma_2, \mathrm{Im}(s) > c$, such that $f(\sigma + \mathrm{i}\, t) = O(e^{t^\alpha})$ for some $\alpha > 0$ uniformly for any $\sigma_1 < \sigma < \sigma_2$. Suppose further that $f(\sigma + \mathrm{i}\, t) = O(|t|^b)$ for some b and $\sigma = \sigma_1$ or σ_2, then $f(\sigma + \mathrm{i}\, t) = O(t^b)$ uniformly for $\sigma_1 \leq \sigma \leq \sigma_2$. ⌟

Proof: First assume that $b = 0$, thus there exists M that $|\varphi(s)| \leq M$ for $\mathrm{Re}(s) = \sigma_i$. Now let $m \equiv 2 \mod 4$ and $m > \alpha$, then $\mathrm{Re}((\sigma + \mathrm{i}\,\tau)^m)$ is a polynomial of σ and τ with highest term of τ being $-\tau^m$, so we have

$$\mathrm{Re}(s^m) = -\tau^m + O(|\tau|^{m-1}), \quad |\tau| \to \infty$$

uniformly on the strip. So $\mathrm{Re}(s^m)$ has an upper bound N on the strip. Thus for any $\varepsilon > 0$,

$$|f(s)e^{\varepsilon s^m}| \leq Me^{\varepsilon N}$$

on the boundary of the strip and

$$|f(s)e^{\varepsilon s^m}| = O(e^{|t|^\alpha - \varepsilon |t|^m})$$

uniformly on the strip, thus converges uniformly to 0 as $|\mathrm{Im}(s)| \to \infty$.

Then we can use maximum principle to see that

$$|f(s)e^{\varepsilon s^m}| \leq Me^{\varepsilon N}$$

on the strip. Let $\varepsilon \to 0$, we get $|\varepsilon(s)| \leq M$, thus the theorem.

In general, if $b \neq 0$, define $\psi(s) = (s - \sigma_1 + 1)^b$, then $|\psi(s)| = |s - \sigma_1 + 1|^b \sim |\tau|^b$ when $|\tau| \to \infty$. Thus $f_1(s) = f(s)/\psi(s)$ satisfies the same condition as φ with $b = 0$, so $f(s)/\psi(s)$ is bounded on the strip, and thus $|f(s)| = O(|\tau|^b)$. □

Remark (11.4.5.8). Some condition on the growth rate of $|f(\sigma + it)|$ is necessary, otherwise we can consider $e^{e^{iz}}$ on the strip $-\frac{\pi}{2} \leq \mathrm{Re}(z) \leq \frac{\pi}{2}$, then it is bounded for $\mathrm{Re}(z) = \pm\frac{\pi}{2}$, but not bounded for $-\frac{\pi}{2} < \mathrm{Re}(z) < \frac{\pi}{2}$. ⌟

6 Calculating Definite Integrals

1

Prop. (11.4.6.1). If f has a primitive F, then for any arc γ,

$$\int_\gamma f(z)\mathrm{d}z = F(\gamma(1)) - F(\gamma(0)).$$

┘

Example (11.4.6.2). For $a > 0$, evaluate the integrals

$$\int_0^\infty e^{-ax}\cos(bx)dx, \quad \int_0^\infty e^{-ax}\sin(bx)dx.$$

┘

Proof:

$$\int_0^\infty e^{-(a+b\,\mathrm{i})z}\mathrm{d}z = \lim_{R\to\infty}\frac{-1}{a+b\,\mathrm{i}}e^{-(a+b\,\mathrm{i})z}\Big|_0^R = \frac{1}{a+b\,\mathrm{i}} - \lim_{R\to\infty}\frac{1}{a+b\,\mathrm{i}}e^{-(a+b\,\mathrm{i})R}.$$

As $|\frac{1}{a+b\,\mathrm{i}}e^{-(a+b\,\mathrm{i})R}| = \frac{1}{\sqrt{a^2+b^2}}e^{-aR} \to 0$ as $R\to\infty$,

$$\int_0^\infty e^{-(a+b\,\mathrm{i})z}\mathrm{d}z = \frac{1}{a+b\,\mathrm{i}}.$$

Then taking the real and imaginary part, we see that

$$\int_0^\infty e^{-ax}\cos(bx)dx = \frac{a}{a^2+b^2}, \quad \int_0^\infty e^{-ax}\sin(bx)dx = \frac{b}{a^2+b^2}.$$

□

From Real to Complex

Prop. (11.4.6.3). For any $\xi\in\mathbb{C}$,

$$e^{-\pi\xi^2} = \int_{-\infty}^\infty e^{-\pi x^2}e^{2\pi\,\mathrm{i}\,x\xi}\mathrm{d}x.$$

┘

Proof: Firstly we show that both sides are holomorphic functions in ξ: The LHS is clear. For the RHS, by(11.4.2.14), it suffices to show that

$$\xi \mapsto \int_{-\infty}^\infty e^{-\pi x^2}e^{-2\pi x\,\mathrm{Im}(\xi)}\mathrm{d}x$$

is a uniformly convergent on compact subsets. But because $\mathrm{Im}(z)$ is bounded on compact subsets, it suffices to show that $\int_{-\infty}^\infty e^{-\pi x^2}e^{Ax}\mathrm{d}x$ is convergent for any $A\in\mathbb{R}$. And by a change of variable, it suffices to notice that $\int_{-\infty}^\infty e^{-\pi x^2}\mathrm{d}x = 1$, by[Stein]P42.

It has been proven in Stein's book Page42**?** that the assertion is true for $\xi\in\mathbb{R}$. Then as both sides are holomorphic functions in ξ, this is true for all $\xi\in\mathbb{C}$, by the uniqueness theorem. □

Cor. (11.4.6.4). For any $a \in \mathbb{C}, \operatorname{Re} a > 0$ and $\xi \in \mathbb{C}$,

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\mathrm{i}\,\xi x - \frac{1}{2}ax^2} \mathrm{d}x = \frac{1}{\sqrt{a}} e^{-\frac{1}{2a}\xi^2}.$$

⌟

Proof: Firstly we show that both sides are holomorphic functions in a: The RHS is clear. For the LHS, by(11.4.2.14), it suffices to show that

$$a \mapsto \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\mathrm{i}\,\xi x - \frac{1}{2}ax^2} \mathrm{d}x$$

is a uniformly convergent on compact subsets. But because $\operatorname{Re}(a) > 0$ is bounded below on compact subsets, it suffices to show that $\int_{-\infty}^{\infty} e^{-Ax^2 - Bx} \mathrm{d}x$ is convergent for any $A \in \mathbb{R}_+$. And by a change of variable, it suffices to notice that $\int_{-\infty}^{\infty} e^{-\pi x^2} \mathrm{d}x = 1$, by[Stein]P42.

It follows from(11.4.6.3) and a change of variable that the assertion is true for $a \in \mathbb{R}_+$. Then as both sides are holomorphic functions in ξ, this is true for all a, by the uniqueness theorem. □

<u>**Rational Functions**</u>

Prop. (11.4.6.5). Let f, g be real polynomials, and $\deg(g) \geq \deg(f) + 2$, and $g(z)$ has no zeros on the real line. Then

$$\int_{-\infty}^{\infty} \frac{f(x)}{g(x)} \mathrm{d}x$$

can be calculated. ⌟

Proof: As the integral is absolutely convergent, we can take $R \in \mathbb{R}$, and γ to be the loop which consists of the line from $-R$ to R and the hemisphere with origin 0 and radius R from R to $-R$, then when R is large, we can assume all the zeros of $g(z)$ in $\mathscr{H}$ is enclosed by γ. Then the integral equals $2\pi\,\mathrm{i}$ times the sum of residues of $\frac{f(z)}{g(z)}$ at the zeros of $g(z)$ in $\mathscr{H}$. □

Example (11.4.6.6). Evaluate the integrals

$$\int_{-\infty}^{\infty} \frac{1}{1+x^4} \mathrm{d}x.$$

What are the poles of $1/(1+z^4)$? ⌟

Proof: $g(z) = 1 + z^4$ has two zeros $e^{\frac{\pi}{4}\mathrm{i}}$ and $e^{-\frac{3\pi}{4}\mathrm{i}}$ on the upper half plane, so the integral equals

$$\int_{\gamma_1} \frac{(x - e^{\frac{\pi}{4}\mathrm{i}})^{-1}(x - e^{\frac{5\pi}{4}\mathrm{i}})^{-1}(x - e^{\frac{7\pi}{4}\mathrm{i}})^{-1}}{x - e^{\frac{3\pi}{4}\mathrm{i}}} + \int_{\gamma_2} \frac{(x - e^{\frac{3\pi}{4}\mathrm{i}})^{-1}(x + -^{\frac{5\pi}{4}\mathrm{i}})^{-1}(x - e^{\frac{7\pi}{4}\mathrm{i}})^{-1}}{x - e^{\frac{\pi}{4}\mathrm{i}}}$$

which equals $2\pi\,\mathrm{i}$ times

$$(\frac{x^4+1}{x - e^{\frac{\pi}{4}\mathrm{i}}})^{-1}\Big|_{x=e^{\frac{\pi}{4}\mathrm{i}}} + (\frac{x^4+1}{x - e^{\frac{3\pi}{4}\mathrm{i}}})^{-1}\Big|_{x=e^{\frac{3\pi}{4}\mathrm{i}}}$$

so it equals

$$(2\pi\,\mathrm{i})[\frac{1}{4e^{\frac{3\pi}{4}\mathrm{i}}} + \frac{1}{4e^{\frac{9\pi}{4}\mathrm{i}}}] = \frac{\pi}{\sqrt{2}}$$

□

Prop. (11.4.6.7) [Fractional Powers]. Let f, g be real polynomials, and $\deg(g) \geq \deg(f)+2$, and $g(z)$ has at most one simple zero at the origin and no other zeros, then the integral

$$\int_0^\infty x^\alpha \frac{f(x)}{g(x)} \mathrm{d}x, 0<\alpha<1$$

can be evaluated. ⌟

Proof: The integral equals $2\int_0^\infty t^{2\alpha+1}\frac{f(t^2)}{g(t^2)}\mathrm{d}t$, and we can choose a branch of z^α that is defined on $\mathbb{C}\setminus\mathbb{R}_{\leq 0}$. Then we can integrate along the loop in $\mathscr{H}$ that consists of two hemisphere of radius ε, R centered at the origin, $[\varepsilon, R]\cup[-R,-\varepsilon]$. Then when $R\to\infty$ and $\varepsilon\to 0$, the integration on the hemisphere tends to 0, and the integration on $[\varepsilon, R]\cup[-R,-\varepsilon]$ tends to

$$\int_{-\infty}^\infty z^{2\alpha+1}\frac{f(z^2)}{g(z^2)}\mathrm{d}z = (1-e^{2\pi\mathrm{i}\alpha})\int_0^\infty t^{2\alpha+1}\frac{f(t^2)}{g(t^2)}\mathrm{d}t.$$

□

<u>4</u>

Prop. (11.4.6.8). Let f, g be real polynomials, and $\deg(g)\geq\deg(f)+1$, and $g(z)$ has no zeros on the real line, then

$$\int_{-\infty}^\infty \frac{f(x)}{g(x)} e^{\mathrm{i}x}\mathrm{d}x, \quad \int_{-\infty}^\infty \frac{f(x)}{g(x)}\cos(x)\mathrm{d}x, \quad \int_{-\infty}^\infty \frac{f(x)}{g(x)}\sin(x)\mathrm{d}x$$

can be calculated. ⌟

Proof: If $\deg(g)\geq\deg(f)+2$, then as before we can use the same hemisphere methods to evaluate, because on the hemisphere, we can bound

$$|\int_\gamma \frac{f(Re^{\mathrm{i}\theta})}{g(Re^{\mathrm{i}\theta})}\mathrm{i}Re^{\mathrm{i}z}\mathrm{d}\theta| \leq C\int_\gamma \frac{e^{-y}}{R}\mathrm{d}\theta \leq C\int_\gamma \frac{1}{R}\mathrm{d}\theta \leq \frac{2\pi C}{R}$$

which converges 0 as $R\to\infty$.

But if $\deg(g)=\deg(f)+1$, this hemisphere integral is no longer converging to 0, so we try another method: Integrate around the square with vertices

$$\{(X_1,0),(X_1,X_1+X_2),(-X_2,X_1+X_2),(-X_2,0)\}.$$

The integral on the vertical lines are bounded by

$$C\int_0^{X_1+X_2} e^{-y}\frac{\mathrm{d}y}{|z|} \leq C\frac{1}{X_2}\int_0^{X_1+X_2} e^{-y}\mathrm{d}y \leq \frac{C}{X_2}$$

And the same is true for the left vertical lines. And the horizontal line is bounded by

$$C\int_{-X_1}^{X_2}\frac{e^{-(X_1+X_2)}}{X_1+X_2}\mathrm{d}t = Ce^{-(X_1+X_2)}$$

and all these converge to 0 as $X_1, X_2\to\infty$. □

Prop. (11.4.6.9). Show that
$$\int_0^\infty \frac{\sin x}{x}\mathrm{d}x = \frac{\pi}{2}.$$
⌟

Proof: To do this one, we need a variation of the technique from above. Choose the semi-contour, then it equals the half of the integral
$$\int_\gamma \frac{e^{\mathrm{i}\,z}}{z}\mathrm{d}z = 2\pi\,\mathrm{i}$$
minus the integral
$$\int_\gamma \frac{e^{\mathrm{i}\,z}}{z}\mathrm{d}z$$
where $\gamma : [0,\pi] \to \mathbb{C} : t \mapsto \varepsilon e^{\mathrm{i}\,t}$. So the integral equals
$$\int_0^\pi e^{\mathrm{i}\,z}\,\mathrm{i}\,\mathrm{d}z$$
which converges to $\pi\,\mathrm{i}$. □

7 Biholomorphisms

Def. (11.4.7.1) [Biholomorphisms]. For regions $U, V \subset \mathbb{C}$, a **biholomorphism** from U to V is a holomorphic map $f : U \to V$ s.t. there is an inverse $g : V \to U$ which is also holomorphic, and $f \circ g = \mathrm{id}_V, g \circ f = \mathrm{id}_U$. ⌟

Prop. (11.4.7.2) [Analytic Functions are Open]. Let $\Omega \subset \mathbb{C}$ be a region, then any non-constant $f \in \mathcal{O}(\Omega)$ defines an open map $\Omega \to f(\Omega)$. ⌟

Proof: Let $z_0 \in \Omega, w_0 = f(z_0)$. by(11.4.2.20), we can find $\varepsilon > 0$ s.t. $\mathbb{D}(z_0, 2\varepsilon) \subset U$, and z_0 is the only zero of $f - w_0$ in $\mathbb{D}(z_0, 2\varepsilon)$. Let γ be the circle $|z - z_0| = \varepsilon$, and $\Gamma = f(\gamma)$. Then because $w_0 \notin \Gamma$, there exists δ s.t. $\mathbb{D}(w_0, \delta) \cap \Gamma = \varnothing$. Then by Rouché's theorem(11.4.2.31), for any $w \in \mathbb{D}(w_0, \delta)$, $f - w$ has a zero $z \in \mathbb{D}(z_0, \varepsilon)$. Thus $f(\mathbb{D}(z_0, \varepsilon)) \supset \mathbb{D}(w_0, \delta)$, and this implies f is open. □

Prop. (11.4.7.3) [Local Biholomorphisms]. A holomorphic map $f : U \to V \subset \mathbb{C}$ is a local bijection iff $f'(z) \neq 0$ for any $z \in U$. ⌟

Proof: For $z_0 \in U$, by discreteness of the zeros, there exists $\delta > 0$ s.t. $\overline{\mathbb{D}(z_0, \delta)} \subset U$ and $F(z) \neq 0$ for $0 < |z - z_0| < \delta$. Because $\{F(z) : |z - z_0| = \delta\}$ is compact, there exists some $\varepsilon > 0$ s.t. $\mathbb{D}(f(z_0), \varepsilon) \subset V$ and $|F(z)| \geq \varepsilon$ for any $|z - z_0| = \delta$.

If $F(z) = f(z) - f(z_0)$ has zero of order exactly 1 at z_0, then for $\xi \in \mathbb{D}(0, \varepsilon)$, by Rouché's theorem(11.4.2.31), $F(z) - \xi$ has exactly 1 zeros in $\mathbb{D}(z_0, \delta)$, which implies $F^{-1}(\mathbb{D}(0, \varepsilon)) \xrightarrow{F} \mathbb{D}(0, \varepsilon)$ is a bijection, and $z_0 \in F^{-1}(\mathbb{D}(0, \varepsilon))$. Thus F and also f is a local bijection z_0.

If $F(z) = f(z) - f(z_0)$ has zero of order $d \geq 1$ at z_0, then for $\xi \in \mathbb{D}(0, \varepsilon)$, by Rouché's theorem(11.4.2.31), $F(z) - \xi$ has exactly d zeros in $\mathbb{D}(z_0, \delta)$, which implies $F^{-1}(\mathbb{D}(0, \varepsilon')) \xrightarrow{F} \mathbb{D}(0, \varepsilon')$ is a d-fold covering for any $\varepsilon' < \varepsilon$, so F thus also f can never be a local bijection at z_0.

Thus f is a local bijection at z_0 iff $f(z) - f(z_0)$ has zero of order exactly 1 at z_0, which is also clearly equivalent to $f'(z_0) \neq 0$. So the assertion is true. □

Cor. (11.4.7.4). If U, V are regions of $\mathbb{C}$ and $f : U \to V$ is holomorphic and bijective, then $f'(z) \neq 0$ for any $z \in U$, and the inverse of f is also holomorphic. ⌟

Proof: To show the inverse is holomorphic, notice that for $w_0 = f(z_0) \in V$, if $w = f(z)$ is close to w_0, then

$$\frac{g(w)-g(w_0)}{w-w_0} = \frac{1}{\frac{w-w_0}{g(w)-g(w_0)}} = \frac{1}{\frac{f(z)-f(z_0)}{z-z_0}}.$$

Because when $z \to z_0$, $w \to w_0$, so we conclude that g is holomorphic at w_0, and its derivative is the reciprocal of the derivative of f. □

Cor. (11.4.7.5). For regions $U, V \subset \mathbb{C}$, any holomorphic bijection from U to V is a biholomorphism. ⌟

Def. (11.4.7.6) [Univalent Functions]. A **univalent function** is a holomorphic function that is injective. ⌟

Prop. (11.4.7.7). Any C^1 conformal map in $\mathbb{C}$ is holomorphic or anti-holomorphic. In higher dimension, conformal is equivalent to $\langle df_p(v_1), df_p(v_2)\rangle = \lambda^2(p)\langle v_1, v_2\rangle$. ⌟

Proof: Cf.[Ahlfors P74]. □

Prop. (11.4.7.8) [Automorphism Groups].

- The only holomorphic automorphisms of $\mathbb{D}$ fixing the origin are the rotations.
- $\mathrm{Aut}(\mathbb{D}) = \{e^{\mathrm{i}\,\theta}\frac{\alpha - z}{1-\overline{\alpha}z}, \alpha \in \mathbb{D}\}$. Moreover, we denote by ψ_α the automorphism $\psi_\alpha(z) = \frac{\alpha - z}{1-\overline{\alpha}z}$, then $\psi_\alpha^2 = \mathrm{id}$.
- $\mathrm{Aut}(\mathscr{H}) = \mathrm{PSL}(2,\mathbb{R})$.
- $\mathrm{Aut}(\overline{\mathbb{C}}) = \mathrm{PSL}(2,\mathbb{C})$.
- $\mathrm{Aut}(\mathbb{C}) = \mathbb{C} \ltimes \mathbb{C}^\times$.

⌟

Proof: 1: g, g^{-1} are both automorphisms of $\mathbb{D}$ that fixes the origin, so by Schwartz's lemma(11.5.1.3), $|g(z)| \le |z|, |g^{-1}(z)| \le |z|$. Thus $|g(z)| = |z|$ for any $z \in \mathbb{D}$, and by Schwartz's lemma(11.5.1.3), g is a rotation.

2: For any $f \in \mathrm{Aut}(\mathbb{D})$, there exists some $\alpha \in \mathbb{D}$ s.t. $f(\alpha) = 0$. Then $g = f \circ \psi_\alpha$ maps 0 to 0. Then by item1, $g(z) = e^{\mathrm{i}\,\theta}z$, and $f(z) = e^{-\mathrm{i}\,\theta}\psi_\alpha(z)$.

3: Firstly $SL(2,\mathbb{R})$ acts transitively on $\mathscr{H}$ it suffices to show that any $z \in \mathscr{H}$ can be mapped to i: $\begin{bmatrix} & -c^{-1} \\ c & \end{bmatrix}(z) = \frac{1}{c^2 z}$, so we may take $c \in \mathbb{R}$ s.t. $M_1 = \begin{bmatrix} & -c^{-1} \\ c & \end{bmatrix}$ maps z to z_1 with $\mathrm{Im}(z_1) = 1$, and then we can take some $b \in \mathbb{R}$ s.t. $M_2 = \begin{bmatrix} 1 & b \\ 1 & \end{bmatrix}$ maps z_1 to i.

Then for any $f \in \mathrm{Aut}(\mathscr{H})$, there exists some $\beta \in \mathscr{H}$ s.t. $f(\beta) = \mathrm{i}$. take some matrix γ s.t. $\gamma(\beta) = \mathrm{i}$, then $g = f \circ \gamma^{-1}$ preserves i. Let $F : \mathscr{H} \cong \mathbb{D} : z \mapsto \frac{z-\mathrm{i}}{z+\mathrm{i}}$ be a biholomorphism, then it can be checked that

$$F \circ \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \circ F^{-1} = e^{\mathrm{i}\,\theta} : \mathbb{D} \to \mathbb{D}.$$

Thus by Schwartz lemma(11.5.1.3), there exists some $\theta \in \mathbb{R}$ s.t. $g = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} = \kappa_\theta$, and then $f = \kappa_\theta \circ \gamma \in \mathrm{SL}(2;\mathbb{R})$.

4: For any distinct points $z_1, z_2, z_3 \in \mathbb{C} \cup \{\infty\}$,

$$F_{z_1,z_2,z_3} : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\} : z \mapsto \frac{z - z_2}{z - z_3} / \frac{z_1 - z_2}{z_1 - z_3}$$

satisfies $F_{z_1,z_2,z_3}(z_1) = 1, F_{z_1,z_2,z_3}(z_2) = 0, F_{z_1,z_2,z_3}(z_3) = \infty$, and

$$G_{z_1,z_2,z_3} : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\} : w \mapsto \frac{wz_3 \frac{z_1 - z_2}{z_1 - z_3} - z_2}{w \frac{z_1 - z_2}{z_1 - z_3} - 1}$$

is an inverse of f_{z_1,z_2,z_3}, so f_{z_1,z_2,z_3} is a bijection.

Now consider $h = F_{f(1),f(0),f(\infty)} \circ f$, then h is also a bijection and $h(1) = 1, h(0) = 0, h(\infty) = \infty$. Thus h is entire, and by(11.4.2.23) $h(z) = zL(z)$ for some $L(z) \in \mathcal{M}(\mathbb{C})$ entire and $L(1) = 1, L(\infty) = 0$, so by Liouville's theorem(11.4.2.10), $L = 1$, and $h(z) = z$.

Thus $f(z) = G_{f(1),f(0),f(\infty)}$ is of the form $\frac{az+b}{cz+d}$. To show that $ad - bc \neq 0$, notice if $ad - bc = 0$, then $f(z)$ is constant, contradiction.

5: Notice $g(z) = (f(z) - f(0))/(f(1) - f(0))$ is also injective and entire, and $g(0) = 0, g(1) = 1$. But by Picard's great theorem, $g(z)$ is meromorphic at ∞. So $g(\infty) = \infty$, otherwise g is entire and bounded, contradicting Liouville's theorem(11.4.2.10). So $g(z) = z$, by item4. Thus $f(z) = (f(1) - f(0))z + f(0)$ is linear. □

Riemann Mapping Theorem

Lemma (11.4.7.9) [Limits of Univalent Functions are Univalent]. A limit of a sequence of univalent holomorphic functions in the compact-open topology is univalent or constant. ⌟

Proof: If $f = \lim_{n\to\infty} f_n$ is non-constant and $f(z_1) = f(z_2)$, we can take a Jordan curve γ surrounding z_1 and z_2 s.t. $0 \notin f(\gamma)$. Then f_n converges uniformly to f on γ, and then it follows from Rouché's theorem(11.4.2.31) that when n is large, $f_n - f(z_1)$ has two zeros inside γ, contradiction. □

Thm. (11.4.7.10) [Riemann Mapping Theorem, Koebe]. Let $\Omega \subset \mathbb{C}$ be a simply-connected region and $\Omega \neq \mathbb{C}$, then for any $z_0 \in \Omega$, there exists a unique biholomorphism $F : \Omega \to \mathbb{D}$ s.t. $F(z_0) = 0$ and $F'(z_0) \in \mathbb{R}_+$. ⌟

Remark (11.4.7.11). This theorem can be generalized to other simply-connected Riemann surfaces, see(12.8.9.2). ⌟

Proof: For the uniqueness, if there are two such maps φ and φ', then $h = \varphi' \circ \varphi^{-1}$ is an automorphism of $\mathbb{D}$ s.t. $h(0) = 0$ and $h'(0) \in \mathbb{R}_+$. Then it follows from(11.4.7.8) that $h = \mathrm{id}$.

For the existence, let $\mathscr{F}$ be the space of univalent holomorphic functions on Ω with values in $\mathbb{D}$. Then $\mathscr{F} \neq 0$: Let $a \neq b \in \partial\Omega$, then by the map $g(z) = \frac{z-a}{z-b}$, we may assume that $\{0, \infty\} \subset \partial\Omega$. Then $\sqrt{\ }$ has two branches on Ω, denoted by h_+ and h_-. Suppose $w_0 \in h_-(\Omega)$ with $\mathbb{D}(w_0, \delta) \subset h_-(\Omega)$, then the function

$$f_0 : z \mapsto \frac{\delta}{h_+(z) - w_0} \in \mathscr{F}.$$

Let

$$\alpha = \sup_{f \in \mathscr{F}} |f'(z_0)|.$$

If $\mathbb{D}(z_0, \delta_1) \subset \Omega$, then by Cauchy's formula, $0 < |f^{\backprime}(z_0)| \leq \delta_1^{-1}$, so $\alpha \in (0, \infty)$, and there exists $f_n \in \mathscr{F}$ s.t. $|f^{\backprime}(z_0)| \geq \alpha - \frac{1}{n}$. Then it follows from Montel's theorem(11.4.5.5) that there is a subsequence of $\{f_n\}$ that converges to a holomorphic function f in compact-open topology, and $|f^{\backprime}(z_0)| = \alpha > 0$ by Weierstrass theorem(11.4.5.3). Notice f is also univalent by(11.4.7.9), so $f \in \mathscr{F}$.

It remains to show that $f(z_0) = 0$ and $f_0(\Omega) = \Delta$, as a rotation of f will satisfy the requirement. If $f(z_0) = \beta \neq 0$, then take

$$f'(z) = \psi_\beta \circ f$$

then $f' \in \mathscr{F}$, and

$$|(f')^{\backprime}(z_0)| = |\frac{f^{\backprime}(z_0)}{1 - |\beta|^2}| > |f^{\backprime}(z_0)|,$$

contradicting the maximality of $|f^{\backprime}(0)|$.

If $w \in \mathbb{D} \backslash f(\Omega)$, then $\psi(z) = \psi_\beta \circ f$ is non-vanishing on Ω, thus $\sqrt{\ }$ has a branch h on $\psi(\Omega)$. Now suppose

$$f'(z) = \psi_{h(z_0)} \circ h,$$

then

$$f = \psi_w^{-1} \circ (z \mapsto z^2) \circ \psi_{h(w)}^{-1} \circ f',$$

where $\Phi^{\backprime} = \psi_w^{-1} \circ (z \mapsto z^2) \circ \psi_{h(w)}^{-1}$ is an automorphism of $\mathbb{D}$ that fixes 0, so $|\Phi^{\backprime}(0)| < 1$ by Schwartz's lemma(11.5.1.3), and

$$|f^{\backprime}(0)| = |\Phi^{\backprime}(0)||(f')^{\backprime}| \leq |(f')^{\backprime}|,$$

contradicting the maximality of $|f^{\backprime}(0)|$. □

Cor. (11.4.7.12). Let $\Omega \subset \overline{\mathbb{C}}$ be a simply-connected region, then D is biholomorphic to exactly one of the following:

- $\mathbb{D} \cong \mathscr{H}$, in which case $\#\partial\Omega > 1$, and Ω is said to be of **hyperbolic type**.
- $\mathbb{C}$, in which case $\#\partial\Omega = 1$.
- $\overline{\mathbb{C}}$, in which case $\#\partial\Omega = 0$.

⌟

Proof: If $\#\partial\Omega > 1$, by a fractional transformation, we can assume $\Omega \subset \mathbb{C}$, and $\Omega \neq \mathbb{C}$, so $\Omega \cong \mathbb{D}$ by(11.4.7.10). If $\#\partial\Omega = 1$, then clearly $\Omega = \overline{\mathbb{C}} \backslash \{z_0\} \cong \mathbb{C}$. □

Cor. (11.4.7.13). Any two simply-connected regions $\Omega, \Omega' \subset \mathbb{C}$ are homeomorphic. ⌟

Injective Holomorphic Maps

Thm. (11.4.7.14) [Bieberbach Conjecture1916, de Branges1984]. Let $f(z) = z + a_2 z^2 + \ldots \in \mathcal{O}(\mathbb{D})$ is an injective map, then $|a_n| \leq n$. And the equation holds iff f is a rotation composed with the Koebe function. ⌟

Proof: Cf.[李忠]. □

11.5 Complex Analysis II

References are [Ahl78], [S-S03], [T-W06] and [Li04].

Notation (11.5.0.1).

- Use notations defined in Real Analysis(Functions on $\mathbb{R}^n$).
- Let Ω be a region(11.4.1.1).

⌟

1 Poincaré Metric

Def. (11.5.1.1) [Hyperbolic Metric]. For any region $\Omega \subset \mathbb{C}$ of hyperbolic type**??**, there exists a covering $\mathbb{D} \to \Omega$, and different coverings differ by an automorphism of $\mathbb{D}$. Thus we can define a **Poincaré metric** on Ω by pushforward of the Poincaré metric $\mathrm{d}^P s = \rho_\Omega(s)|\mathrm{d}z|$ on $\mathbb{D}$. Then this is well-defined and independent of the covering map. ⌟

Proof: It is well-defined because for any two local inverse map $\Omega \to \mathbb{D}$ differ by a Deck transformation which is an automorphism of $\mathbb{D}$ thus preserves the Poincaré metric**?**. And any two covering $\mathbb{D} \to \Omega$ differ by a covering map which is also an automorphism of $\mathbb{D}$, thus preserves the Poincaré metric. □

Prop. (11.5.1.2) [Hyperbolic Metrics].

- $\rho_{\mathscr{H}}(z) = 1/\operatorname{Im}(z)$.
- $\rho_{\mathbb{D}(0,(0,r))}(z) = 1/(|z| \log \frac{r}{|z|})$.

⌟

Proof: 1: **?**.
2: There is a covering map $\mathscr{H} \to \mathbb{D}(0,(0,r)) : z \mapsto re^{\mathrm{i} z}$, so we can plug in the inverse map $w = \mathrm{i} \log z$ into $|\mathrm{d}w|/\operatorname{Im} w$ to get the desired formula. □

Thm. (11.5.1.3)[Schwartz Lemma]. If $f \in \mathcal{O}(\mathbb{D})$ and satisfies $|f(z)| \leq 1$, $f(0) = 0$, then $|f(z)| \leq |z|$, and $|f'(0)| \leq 1$. Moreover, if $|f(z)| = |z|$ for some z or $|f'(0)| = 1$, then $f(z) = cz$ for some $|c| = 1$. ⌟

Proof: The function $g(z) = f(z)/z$ is analytic on $0 < |z| < 1$ with a removable singularity at 0(11.4.2.18) and extends to an analytic function on $|z| < 1$ with $g(0) = f'(0)$, and $\lim_{|z|\to 1} |g(z)| \leq 1$, thus by maximal principle(11.4.2.24), $|g(z)| \leq 1$ for any $|z| < 1$, thus we are done. The last assertion also follows from(11.4.2.24). □

Lemma (11.5.1.4) [Schwartz-Pick]. Let $f \in \mathcal{O}(\mathbb{D})$, and $f(\mathbb{D}) \subset \mathbb{D}, f(0) = 0$, then in the Poincaré metric, for any $z_1, z_2 \in \mathbb{D}$,

$$d^P(f(z_1), f(z_2)) \leq d^P(z_1, z_2).$$

And if the equality holds for some $z_1 \neq z_2$, then $f \in \operatorname{Aut}(\mathbb{D})$. ⌟

Proof: Cf.[李忠]P29. □

Prop. (11.5.1.5) [Generalized Schwartz Lemma]. Let Ω_1, Ω_2 be regions of hyperbolic type with Poincaré metrics $\mathrm{d}s_1 = \sigma_1(z)|\mathrm{d}z|$ and $\mathrm{d}s_2 = \sigma_2(z)|\mathrm{d}z|$, then for any holomorphic map $f : \Omega_1 \to \Omega_2$,

$$\sigma_2(f(z))|f'(z)| \leq \sigma_1(z).$$

In particular, if $\Omega_1 \subset \Omega_2$, then $\sigma_2(z) \leq \sigma_1(z)$. ⌟

Proof: Let $h_1 : \mathbb{D} \to \Omega_1, h_2 : \mathbb{D} \to \Omega_2$ be covering maps, then $f : \Omega_1 \to \Omega_2$ lifts to a holomorphic map $F : \mathbb{D} \to \mathbb{D}$. Thus Schwartz-Pick lemma implies that $\sigma_{\mathbb{D}}(F(z))|F'(z)| \leq \sigma_{\mathbb{D}}(z)$. And this implies that

$$\sigma_1(z) \geq \sigma_{\mathbb{D}}(F \circ \psi_1(z))|(F \circ \psi_1)'(z)| = \sigma_{\mathbb{D}}(\psi_2 \circ f(z))|(\psi_2 \circ f)'(z)| = \sigma_2(f(z))|f'(z)|.$$

□

Montel-Normal Family

Def. (11.5.1.6) [Montel-Normal Family]. If $\Omega \subset \mathbb{C}$ is a region, then a set $\mathcal{S} = \{f_\alpha\}$ of holomorphic functions on Ω is called a **Montel-normal family** if for any sequence of functions in $\mathcal{S}$, there exists a subsequence that converges uniformly in Ω to ∞ or to a holomorphic function. Or equivalently, for any compact subset $D \subset \Omega$, there exists a subsequence that converges uniformly in the compact-open topology of $C(D, \mathbb{P}^1(\mathbb{C}))$.

$\mathcal{S}$ is called normal at a point $z \in \mathbb{C}$ if there exists a region $z \in \Omega$ s.t. $\mathcal{S}|_\Omega$ is a Montel-normal family. ⌟

Prop. (11.5.1.7). If $\Omega, \Omega' \subset \mathbb{C}$ is a region, and $\{f_\alpha\}$ is a Montel-normal family of holomorphic maps from Ω to Ω'. Suppose $g \in \mathcal{O}(\Omega')$, then $\{g \circ f_\alpha\}$ is also Montel-normal on Ω. ⌟

Prop. (11.5.1.8) [Montel]. If $\Omega \subset \mathbb{C}$ is a region, and $\mathcal{S} = \{f_\alpha\}$ is a set of holomorphic functions on Ω s.t.

$$\mathcal{S}' = \{\frac{|f_\alpha'(z)|}{1 + |f_\alpha(z)|^2}\}$$

is a set of functions on Ω bounded in the compact-open topology, then $\mathcal{S}$ is a Montel-normal family. ⌟

Proof:

□

Thm. (11.5.1.9) [Montel]. If $\Omega \subset \mathbb{C}$ is a region, and $\mathcal{S} = \{f_\alpha\}$ is a set of holomorphic functions on Ω s.t. there exists $a, b \in \mathbb{C}$ s.t. $f(z) \neq a, b$ for any $f \in \mathcal{S}, z \in \Omega$, then $\mathcal{S}$ is a Montel-normal family(11.5.1.6). ⌟

Proof: By Riemann-mapping theorem, there is a covering map $\rho : \mathbb{D} \to \mathbb{C} \setminus \{0, 1\}$. Then each map f_α lifts via ρ to a map $\widetilde{f}_\alpha : \Omega \to \mathbb{D}$. Then $\widetilde{f}$ is bounded, and it follows form the formula $f'(z) = \frac{1}{2\pi}\int_\gamma \frac{f(\zeta)}{(\zeta - z)^2} d\zeta$ that the derivatives of $\widetilde{f}_\alpha$ are also uniformly bounded. Thus $\widetilde{f}_\alpha$ is equicontinuous and uniformly bounded, so Montel-normal by Arzela-Ascoli. Finally, by(11.5.1.7), $\{f_\alpha\}$ is also Montel-normal. □

Prop. (11.5.1.10). If $\Omega \subset \mathbb{C}$ is a region and $f \in \mathcal{M}(\Omega)$, then for $k \in \mathbb{Z}_+$, the family $\{f^{(n)}\}_{n \in \mathbb{Z}_+}$ is Montel-normal on Ω iff the family $\{f^{(kn)}\}_{n \in \mathbb{Z}_+}$ is Montel-normal on Ω. ⌟

$\rho_{0,1}(z)$

Prop. (11.5.1.11) [$\rho_{0,1}$]. Suppose the Poincaré metric on $\mathbb{D} \setminus \{0, 1\}$ is $\rho_{0,1}(z)|dz|$, then

- $\rho_{0,1}(z) = \rho_{0,1}(1 - z)$.
- $\rho_{0,1}(1/z) = \rho_{0,1}(z)/z^2$.

- $\rho_{0,1}(z) = \rho_{0,1}(1-z) > \frac{1}{4|z|}$ when $|z|$ is small.
- $\rho_{0,1}(z) \leq \frac{1}{|z|\log|\frac{1}{z}|}$.

⌟

Proof: 1, 2 follows from the uniqueness of the Poincaré metric.
3 follows from [李忠]P46.?
4: This follows from(11.5.1.2) and generalized Schwartz lemma(11.5.1.5). □

Prop. (11.5.1.12). Let $\eta = \min\{\rho_{0,1}(z) : |z| = 1\}$, then $\eta = \rho_{0,1}(-1) = 4\pi^2/\Gamma^4(\frac{1}{4}) = 0.2284733$. ⌟

Proof:

□

Prop. (11.5.1.13). For $0 < |z| \leq 1$,

$$\rho_{0,1}(z) \geq \frac{1}{|z|(\eta^{-1} - \log|z|)},$$

where $\eta = \min\{\rho_{0,1}(z), |z| = 1\} > 0$ by(11.5.1.11). ⌟

Proof: □

Cor. (11.5.1.14). When $z \to 0$, $\rho_{0,1}(z) \sim \frac{1}{|z|\log|\frac{1}{z}|}$. ⌟

Thm. (11.5.1.15) [Landau]. If $f \in \mathcal{O}(\mathbb{D})$ doesn't take the values $0, 1$, then

$$|f'(0)| \leq 2|f(0)|(\eta^{-1} + \Big|\log|f(0)|\Big|)(11.5.1.12).$$

And the equality can be achieved. ⌟

Proof: Cf.[李忠]P41. □

Thm. (11.5.1.16) [Great Picard Theorem]. If an analytic function f has an essential singularity at a point w, then on any punctured nbhd of w, f takes any value infinitely often, except for at most one single exception. ⌟

Proof: We may assume $f : \mathbb{D}\setminus\{0\} \to \mathbb{C}\setminus\{0,1\}$, then by generalized Schwartz lemma(11.5.1.5) and(11.5.1.2),

$$\rho_{0,1}(f(z))|f'(z)| \leq \frac{1}{|z|\log\frac{1}{|z|}}.$$

We want to prove that for $z \in \mathbb{D}(0,e)$, there exists some C s.t.

$$-\log|f(z)| < C\log\frac{1}{|z|}.$$

When $f(z) \geq 1$, this is clearly true, so we may assume $f(z) < 1$. Let $m = \max\{|f(z)| : |z| = \rho\}$, and let $z = re^{i\theta}$. Consider two cases:

If $f(te^{i\theta}) \in \mathbb{D}$ for any $r \leq t \leq e$, then by(11.5.1.13),

$$\frac{|f'(z)|}{|f(z)|}[\eta^{-1} - \log|f(te^{i\theta})|]^{-1} \leq \frac{1}{|z|\log\frac{1}{|z|}}.$$

Integration on $t \in [r, \rho]$ implies that

$$\log[\eta^{-1} - \log|f(z)|] \le \log\log\frac{1}{|z|} - \log\log\frac{1}{\rho} + \log[\eta^{-1} - \log|f(\rho e^{\mathrm{i}\theta})|] \le \log\log\frac{1}{|z|} + \log\log\frac{e^{\eta^{-1}}}{m},$$

which implies that

$$-\log|f(z)| < C\log\frac{1}{|z|}.$$

If $r_0 \in (r, e]$ is the smallest number s.t. $|f(r_0 e^{\mathrm{i}\theta})| = 1$, then integration on t from r to r_0 implies that

$$\log[\eta^{-1} - \log|f(z)|] \le \log\log\frac{1}{|z|} - \log\log\frac{1}{r_0} + \log(\eta^{-1}) \le \log\log\frac{1}{|z|},$$

which also implies that

$$-\log|f(z)| < \eta^{-1}\log\frac{1}{|z|}.$$

Now notice we can do all above for f replaced by $1/f$, so it implies that

$$\log|f(z)| < C'\log\frac{1}{|z|},$$

and then f is meromorphic at $z = 0$. □

Thm. (11.5.1.17) [Schottky]. If $f \in \mathcal{O}(\mathbb{D})$ doesn't take the values $0, 1$, then

$$\log|f(z)| \le [\eta^{-1} + \max\{\log|f(0)|, 0\}]\frac{1+|z|}{1-|z|} - \eta^{-1},$$

and the equality can be achieved. ⌟

Proof: It follows from generalized Schwartz lemma(11.5.1.5) that

$$\rho_{0,1}(f(z))|f'(z)| \le \frac{2}{1-|z|^2}.$$

For $z = re^{\mathrm{i}\theta} \in \mathbb{D}$, if $f(te^{\mathrm{i}\theta}) \in \mathbb{D}$ for any $t \in [0, r]$, then it follows from(11.5.1.13) that

$$\frac{|f'(z)|}{|f(z)|}[\eta^{-1} - \log|f(te^{\mathrm{i}\theta})|]^{-1} \le \frac{2}{1-|z|^2}.$$

Integration on $t \in [0, r]$ implies that

$$\frac{\eta^{-1} - \log|f(z)|}{\eta^{-1} - \log|f(0)|} \le \frac{1+|z|}{1-|z|}.$$

If $r_0 \in (0, r]$ is the largest number s.t. $|f(r_0 e^{\mathrm{i}\theta})| = 1$, then integration on t from r_0 to r implies that

$$\eta(\eta^{-1} - \log|f(z)|) \le \frac{1+|z|}{1-|z|}\frac{1-r_0}{1+r_0} < \frac{1+|z|}{1-|z|}.$$

So in any case we get

$$\eta^{-1} - \log|f(z)| \le [\eta^{-1} + \max\{\log|f(0)|, 0\}]\frac{1+|z|}{1-|z|}.$$

And all the above applies to f replaced by $1/f$, so we get the desired formula.

To show the equality can be achieved, Cf.[李忠]P45. □

2 Harmonic Functions

Def. (11.5.2.1)[Harmonic Functions]. A real-valued function on a region $\Omega \subset \mathbb{C}$ is called **harmonic** iff it is C^1 and has second order derivatives and

$$\Delta u = (\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})u = 4\frac{\partial}{\partial \overline{z}}\frac{\partial}{\partial z} f = 0.$$

This is an elliptic differential operator, so u is automatically smooth, by(11.12.8.4).

The vector space of Harmonic functions on Ω is denoted by $\mathcal{H}(\Omega) \subset \mathbb{C}^\infty(\Omega)$. ⌟

Prop. (11.5.2.2) [Schwarz's Theorem]. Cf.[Ahlfors P169]. ⌟

Def. (11.5.2.3) [Mean-Value Property]. A real valued function u on a region Ω is said to have the **mean-value property** iff

$$u(z_0) = \frac{1}{2\pi}\int_0^{1\pi} u(z_0 + re^{\mathrm{i}\,\theta})d\theta$$

whenever $\mathbb{D}(z_0, r) \subset \Omega$. ⌟

Lemma (11.5.2.4) [Harmonic Mean Value]. If u is a Harmonic function between two concentric circles, then the arithmetic mean of it over circles $|z| = r$ is a linear function of $\log r$:

$$\frac{1}{2\pi}\int_{|z|=r} u\mathrm{d}\theta = \alpha \log r + \beta.$$

In particular, if u is harmonic in the disk, then by continuity, $\alpha = 0$, and the mean value is a constant. ⌟

Proof: Cf.[Ahlfors P165]. □

Prop. (11.5.2.5) [Harmonicity and Mean-Value Property]. A harmonic function satisfies the mean-value property, and conversely, and continuous function satisfying the mean-value property is harmonic. ⌟

Proof: Harmonic function satisfies the mean-value property by(11.5.2.4). Conversely, for any z_0, by Schwarz's theorem(11.5.2.2), there is a harmonic function $v(z)$ that is harmonic in $\mathbb{D}(z_0, \rho)$ and equals $u(z)$ on $\partial B(z_0, \rho)$. Now the maximal and minimal principles apply to $u - v$, thus $u = v$ is harmonic. □

Cor. (11.5.2.6) [Maximum Principle]. If u is a harmonic function, then it attains neither maximum nor minimum at its region of definition. ⌟

Prop. (11.5.2.7) [Real Part of an Analytic Function is Harmonic]. On $\mathbb{C}$, formally,

$$4\frac{\partial}{\partial z}\frac{\partial}{\partial \overline{z}} = 4\frac{\partial}{\partial \overline{z}}\frac{\partial}{\partial z} = \Delta.$$

Thus for any open subset $\Omega \subset \mathbb{C}$, if $f \in \mathcal{O}(\Omega)$, then $\mathrm{Im}\, f, \mathrm{Re}\, f \in \mathcal{H}(\Omega)$. ⌟

Proof: By(11.4.1.4),

$$4\frac{\partial}{\partial z}\frac{\partial}{\partial \overline{z}} = (\frac{\partial}{\partial x} - \mathrm{i}\frac{\partial}{\partial y})(\frac{\partial}{\partial x} + \mathrm{i}\frac{\partial}{\partial y}) = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}.$$

$$4\frac{\partial}{\partial\bar{z}}\frac{\partial}{\partial z}=(\frac{\partial}{\partial x}+\mathrm{i}\,\frac{\partial}{\partial y})(\frac{\partial}{\partial x}-\mathrm{i}\,\frac{\partial}{\partial y})=\frac{\partial^2}{\partial x^2}+\frac{\partial^2}{\partial y^2}.$$

If $f\in\mathcal{O}(\Omega)$, then $f\in C^\infty(\Omega)$ by(11.4.2.7), then by(11.3.3.14) the formal calculation above applies to f, and by(11.4.1.10)

$$\Delta\operatorname{Re}f+\mathrm{i}\,\Delta\operatorname{Im}f=\Delta f=\frac{\partial}{\partial z}\frac{\partial}{\partial\bar{z}}f=0,$$

so $\Delta\operatorname{Re}f=\Delta\operatorname{Im}f=0$, and $\operatorname{Im}f,\operatorname{Re}f\in\mathscr{H}(\Omega)$. □

Cor. (11.5.2.8). If $\Omega\subset\mathbb{C}$ is a region and $z\in\Omega$, $f\in\mathcal{O}(\Omega)$ is non-vanishing, then $\log|f|\in\mathscr{H}(\Omega)$. ⌟

Proof: Being harmonic is local, so we may look locally and assume Ω is a disk. Then by(11.4.2.33), there exists a $g\in\Omega(\Omega)$ s.t.

$$f(z)=\exp(g(z)).$$

Then it follows $\operatorname{Re}(g(z))=\log|f(z)|$, which is harmonic by(11.5.2.7). □

Prop. (11.5.2.9) [Harmonic Functions as the Real Parts of Analytic Functions]. Let $\Omega\subset\mathbb{C}$ be a simply-connected region, $u\in\mathscr{H}(\Omega)$, then there exists $f\in\mathcal{O}(\Omega)$ s.t. $\operatorname{Re}f=u$. And any two such f differ by a purely imaginary constant. ⌟

Proof: Let $g(z)=2\frac{\partial}{\partial z}u$, then $\frac{\partial}{\partial\bar{z}}g=2\frac{\partial}{\partial\bar{z}}\frac{\partial}{\partial z}u=\frac{1}{2}\Delta u=0$, so $g\in\mathcal{O}(\Omega)$. Then by(11.4.2.3), there exists $f\in\mathcal{O}(\Omega)$ s.t. $\frac{\partial}{\partial z}f=g=2\frac{\partial}{\partial z}u$. So

$$2\frac{\partial}{\partial x}u=\frac{\partial}{\partial x}\operatorname{Re}f+\frac{\partial}{\partial y}\operatorname{Im}f=2\frac{\partial}{\partial x}\operatorname{Re}f,\quad 2\frac{\partial}{\partial y}u=\frac{\partial}{\partial y}\operatorname{Re}f-\frac{\partial}{\partial x}\operatorname{Im}f=2\frac{\partial}{\partial y}\operatorname{Re}f.$$

So $u-\operatorname{Re}f$ is a constant function. And we may modify f to make $\operatorname{Re}f=u$. For the last assertion, use the Cauchy-Riemann equations to show that $\frac{\partial}{\partial x}(\operatorname{Im}f-\operatorname{Im}f')=\frac{\partial}{\partial y}(\operatorname{Im}f-\operatorname{Im}f')=0$, so $\operatorname{Im}f-\operatorname{Im}f'$ is a constant function. □

Properties

Prop. (11.5.2.10) [Poisson Formula]. For $u\in\mathscr{H}(\overline{\mathbb{D}(0,R)})$,

$$u(z)=\frac{1}{2\pi}\int_0^{2\pi}\frac{R^2-|z|^2}{|Re^{\mathrm{i}\,\theta}-z|^2}u(Re^{\mathrm{i}\,\theta})d\theta=\operatorname{Re}\Big[\frac{1}{2\pi\,\mathrm{i}}\int_{|\zeta|=R}\frac{\zeta+z}{\zeta-z}u(\zeta)\frac{d\zeta}{\zeta}\Big].$$

for $z\in\mathbb{D}(0,R)$.

In particular, for any $f\in\mathcal{O}(\overline{\mathbb{D}(0,R)})$, there is a constant $C\in\mathbb{R}$ s.t. for any $z\in\mathbb{D}(0,R)$:

$$f(z)=\frac{1}{2\pi\,\mathrm{i}}\int_{|\zeta|=\rho}\frac{\zeta+z}{\zeta-z}\operatorname{Re}(f(\zeta))\frac{d\zeta}{\zeta}+\mathrm{i}\,C.$$

⌟

Proof: This follows from(11.5.2.9) and(11.4.2.12). □

Cor. (11.5.2.11) [Poisson-Jensen Formula]. For $f\in\mathcal{O}(\overline{\mathbb{D}(0,R)})$ with no zeros on the boundary and zeros $a_1,\ldots,a_n$ inside(counting multiplicity), then for $z\in\mathbb{D}(0,R)$ s.t. $f(z)\neq 0$,

$$\log|f(z)|=-\sum_i\log\Big|\frac{R^2-\overline{a}_iz}{R(z-a_i)}\Big|+\frac{1}{2\pi}\int_0^{2\pi}\frac{R^2-|z|^2}{|Re^{\mathrm{i}\,\theta}-z|^2}\log|f(Re^{\mathrm{i}\,\theta})|\mathrm{d}\theta.$$

In particular, if $f(0)\neq 0$, then

$$\log|f(0)| = -\sum_i \log\left|\frac{R}{a_i}\right| + \frac{1}{2\pi}\int_0^{2\pi}\log|f(Re^{\mathrm{i}\,\theta})|\mathrm{d}\theta.$$

⌟

Proof: Firstly, this is true when f is non-vanishing on $\mathbb{D}(0,\rho)$, because in this case $\log|f|$ is harmonic by(11.5.2.8) and we can use mean value theorem(11.5.2.5). In general, consider the function

$$F(z) = f(z)\prod_{i=1}^{n}\frac{R^2-\overline{a}_i z}{R(z-a_i)},$$

then it satisfies $F(z)=f(z)$ for $|z|=R$, and has no zeros on $\mathbb{D}(0,R)$, so

$$\frac{1}{2\pi}\int_0^{2\pi}\log|f(\rho e^{\mathrm{i}\,\theta})|\mathrm{d}\theta = \log|F(0)| = \log|f(0)| + \sum_i \log\left|\frac{R^2-\overline{a}_i z}{R(z-a_i)}\right|.$$

□

Prop. (11.5.2.12) [Hadamard's Three Circle Theorem]. Let $f(z)$ be analytic in the annulus $r_1<|z|<r_2$, and continuous on the boundary, if $M(r)$ denotes the maximum of $|f(z)|$ for $|z|=r$, then:

$$M(r)\leq M(r_1)^{\alpha}M(r_2)^{1-\alpha}$$

where $\alpha=\log(r_2/r):\log(r_2/r_1)$. ⌟

Proof: Apply the maximum principle(11.5.2.6) for

$$g(z) = \log|f(z)| - \log(M(r_1))(\log(r_2/|z|):\log(r_2/r_1)) - \log(M(r_2))(1-\log(r_2/|z|):\log(r_2/r_1)),$$

it is harmonic by(11.5.2.8), then $g(z)\leq 0$ on $|z|=r_1$ and $|z|=r_2$, so $g(z)\leq 0$ on all the annulus. □

Cor. (11.5.2.13). Let $f(z)$ be analytic in the annulus $r_1<|z|<r_2$, then the function

$$s\mapsto \max_{z=e^s}|f(z)|$$

is convex on the interval $[\log(a),\log(b)]$. ⌟

Prop. (11.5.2.14) [Reflection Principle]. ⌟

Proof: □

Prop. (11.5.2.15) [Harnack's Inequality]. For a positive harmonic function u on $B(0,\rho)$,

$$\frac{\rho-|z|}{\rho+|z|}u(0)\leq u(z)\leq\frac{\rho+|z|}{\rho-|z|}u(0).$$

⌟

Proof: By Poisson formula,

$$u(z)=\frac{1}{2\pi}\int\frac{\rho^2-|z|^2}{|\rho e^{\mathrm{i}\theta}-z|^2}u(\rho e^{i\theta})d\theta$$

for $|z|<\rho$, so the conclusion follows from the obvious inequality

$$\frac{\rho-|z|}{\rho+|z|}\leq\frac{\rho^2-|z|^2}{|\rho e^{\mathrm{i}\theta}-z|^2}\leq\frac{\rho+|z|}{\rho-|z|}$$

and Mean-value property(11.5.2.5). □

Cor. (11.5.2.16). If E is a compact subset of a region Ω, there is a constant M, depending on E,Ω that for any positive harmonic function $u(z)$ on Ω, $u(z_2)\leq Mu(z_1)$ for any $z_1,z_2\in E$. ⌟

Proof: This is an easy consequence of Harnack inequality and the compactness of E. □

Cor. (11.5.2.17) [Harnack's Principle]. Consider a sequence of functions $u_n(z)$, each harmonic in a region Ω_n, and there is a region Ω that every point has a nbhd that is contained in all but f.m. Ω_n, and in this nbhd $u_n(z)\leq u_{n+1}(z)$ for n large, then either $u_n(z)$ tends to $+\infty$ in the compact open topology, or they tends to a harmonic function in compact open topology. ⌟

Proof: The uniform continuity follows easily from Harnack's inequality, and for the harmonicity of the limit function $u(z)$ is a consequence of the Poisson formula. □

Bounds on Locations of Zeros

Prop. (11.5.2.18). For $f\in\mathcal{O}(\mathbb{D})$ and $r\in(0,1)$, denote

$$A(r)=\frac{1}{2r}\int_0^{2\pi}\log|f(re^{\mathrm{i}\theta})|\mathrm{d}\theta.$$

Then if f has no zeros on $\partial\mathbb{D}(0,r)$,

$$\frac{\partial}{\partial r}A(r)=\frac{1}{r}\#\{\text{zeros of } f \text{ in } \mathbb{D}(0,r)\}.$$

⌟

Proof: We may divide f by z^k to make $f(0)\neq 0$, then the assertion follows from(11.5.2.11). □

Prop. (11.5.2.19). Let $f\in\mathcal{O}(\overline{\mathbb{D}})$ s.t. $\max_{z\in\overline{\mathbb{D}}}|f|=K|f(0)|$. Then for any $\delta\in(0,1)$,

- $\#\mathrm{Zero}(f)\cap\mathbb{D}(0,1-\delta)\leq\frac{\log K}{\delta}$.
- There exists $C(\delta)\in\mathbb{R}_+$ s.t. for any $s\in\mathbb{D}(0,1-\delta)$,

$$\Big|\frac{f'}{f}(s)+\sum_{\mathrm{Zero}(f)\cap\mathbb{D}(0,1-\delta)}\frac{1}{s-\rho}\Big|\leq C(\delta)\log K.$$

⌟

Proof: 1: By(11.5.2.18) and fundamental theorem of calculus,

$$\#\mathrm{Zero}(f)\cap\mathbb{D}(0,1-\delta)\leq\frac{A(1)-A(1-\delta)}{\delta}\leq\frac{\max_{\partial\mathbb{D}}\log|f|-\log|f(0)|}{\delta}=\frac{\log K}{\delta}.$$

2: Cf.[Larry Guth]P83. □

Dirichlet Problem

3 Miscellaneous

Def. (11.5.3.1) [$L^2(\mathbb{D},\nu_k)$ **Unit Disc**]. Define a density $\nu_k = \frac{4(1-|w|^2)^{k-2}dudv}{|1-w|^{2k}}(k \geq 2)$ on $\mathbb{D}$ and define $L^2(\mathbb{D},\nu_k)$ to be the space of holomorphic functions on $\mathbb{D}$ that is $L^2(\nu_k)$ bounded. Then the space $L^2(\mathbb{D},\nu_k)$ is complete. ⌟

Proof: By(11.4.2.11), the uniform norm is bounded by the local L^1-norm hence also the local L^2-norm. Hence for a compact subset K, the uniform norm is also bounded by $L^2(\nu_k)$-norm. Thus any Cauchy sequence in $L^2(\mathbb{D},\nu_k)$ converges to a holomorphic function by Weierstrass theorem(11.4.5.3). □

Prop. (11.5.3.2). The space $L^2(\mathbb{D},\nu_k)$ has an orthogonal basis consisting of holomorphic functions

$$\{\psi_n = w^n(1-w)^k\}_{n\geq 0}.$$

⌟

Proof: Firstly, ψ_n is convergent: In the polar coordinate, $\nu_k = \frac{4(1-r^2)^{k-2}rdrd\theta}{|1-w|^{2k}}$, so

$$||\psi_n||^2 = 4\int_0^{2\pi}\int_0^1 r^{2n}(1-r^2)^{k-2}\mathrm{d}r\mathrm{d}\theta < \infty.$$

And if $m \neq n$,

$$\int_{\mathbb{D}} \psi_m(w)\overline{\psi_n}(w)dw = 4\int_{\mathbb{D}} w^m(\overline{w})^n(1-r^2)^{k-2}\mathrm{d}r\mathrm{d}\theta = 4\int_0^1 r^{m+n}(1-r^2)^{k-2}\int_0^{2\pi} e^{i(m-n)\theta}\mathrm{d}\theta = 0.$$

□

Def. (11.5.3.3) [**Upper Half Plane** $\mathscr{H}_k$]. On the upper half plane $\mathscr{H}$, we can define a density $\mu_k = y^k\frac{dxdy}{y^2}(k \geq 2)$, and define $L^2(\mathscr{H},\mu_k)$ to be the space of holomorphic functions on $\mathscr{H}$ that is $L^2(\mu_k)$ bounded. Then under the Cayley map $z \mapsto w = \frac{z-\mathrm{i}}{z+\mathrm{i}}$, this density is mapped to the density ν_k of $\mathbb{D}$ and induces an isomorphism of spaces

$$L^2(\mathscr{H},\mu_k) \cong L^2(\mathbb{D},\nu_k).$$

In particular, $L^2(\mathscr{H},\mu_k)$ is complete, and it has an orthogonal basis

$$\{\varphi_n = (\frac{z-\mathrm{i}}{z+\mathrm{i}})^n\frac{(2\,\mathrm{i})^k}{(z+\mathrm{i})^k}\}.$$

by(11.5.3.1) and(11.5.3.2). ⌟

4 Elliptic Functions

Main references are [**?**]Chap7, [Sil99], [Sil16]. [Elliptic Functions according to Eisenstein and Kronecker, Weil].

Trigonometric Functions

Elliptic Functions(Eisenstein)

Def. (11.5.4.1) [Doubly Periodic Function]. Let Λ be a lattice of $\mathbb{C}$, then a meromorphic function f on $\mathbb{C}$ is called **doubly periodic w.r.t.** Λ if it is invariant under Λ. ⌟

Prop. (11.5.4.2). Let f be a periodic function for Λ, not identically zero, and let D be a fundamental parallelogram for Λ that f has no zeros or poles on the boundary of D. Then

- $\sum_{P\in D}\operatorname{ord}_P(f)=0$.
- $\sum_{P\in D}\operatorname{res}_P(f)=0$.
- $\sum_{P\in D}\operatorname{ord}_P(f)\cdot P=0$.

⌟

Proof: f can be realized as meromorphic functions on the Riemann surface $\mathbb{C}/\Lambda$, so $1,2$ are direct consequences of(12.8.9.9) $1,2$. 3 is 2 applied to the meromorphic function $zf'(z)/f(z)$. □

Def. (11.5.4.3) [Order]. The order of an elliptic function f is defined to be the number of poles of f in D. Equivalently, it is the number of zeros of f in D(11.5.4.2). ⌟

Prop. (11.5.4.4). The total number of orders of a non-constant elliptic function≥ 2. ⌟

Proof: If its order is 0, then it is bounded on D and also on $\mathbb{C}$ thus constant by Liouville's theorem. If its order is 1, then it has a simple pole z_0, but then $\operatorname{Res}_{z_0}(f)\neq 0$, contradicting(11.5.4.2). □

Def. (11.5.4.5) [Weierstrass $\wp$-Function]. For a lattice $\Lambda\subset\mathbb{C}$, consider the function

$$\wp(z)=\frac{1}{z^2}+\sum_{\omega\in\Lambda\backslash\{0\}}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)$$

Then it is a doubly periodic meromorphic function that has a double pole at 0, and so does its derivative $\wp'$, having a triple pole at 0. Hence they descend to a rational function on $\mathbb{C}/\Lambda$.

If $\Lambda=\Lambda_\tau$, then the function $\wp(z;\tau)=\wp(z)$ is called the **Weierstrass $\wp$-function**. ⌟

Prop. (11.5.4.6). Let $G_k(\Lambda)$ be given by(20.2.4.5),

$$\wp(z)=\frac{1}{z^2}+\sum_{k\geq 1}(2k+1)G_{2k+2}(\Lambda)z^{2k}.$$

⌟

Proof: This follows from(9.5.2.1). □

Prop. (11.5.4.7) [Fields of Elliptic Functions]. The field of doubly periodic functions for Λ is just $\mathbb{C}(\wp,\wp')$. And $\wp,\wp'$ also satisfies the following equation:

$$\wp'(z)^2=4\wp(z)^3-g_2\wp(z)-g_3$$

where $g_2=60G_4(\Lambda), g_3=140G_6(\Lambda)$(20.2.4.5). ⌟

Proof: For the equational function, just notice we can calculate directly that the difference of the two sides is a holomorphic function in z without constant terms, and they are both doubly periodic, thus is zero.

For the first statement, notice that any function is a sum of an odd function and an even function. $\wp'$ is odd, thus an odd function is $\wp'$ times an even function. Thus it reduces to show that any even doubly periodic function is a rational function of $\wp$.

For any even periodic function f, f has the same order at z_0 and $-z_0$, also if $z_0 \equiv -z0 \mod \Lambda$, the order of f at z_0 must be odd. Now consider $\wp(z) - \wp(z_0)$, then it is a function with two poles at 0, so it has two zeros. If $z_0 \equiv -z_0$, then $\wp(z) - \wp(z_0)$ has a zero of order 2 at z_0, and otherwise it has simple zeros at z_0 and $-z_0$.

So for any even doubly periodic function f, we can use the product $\prod(\wp(z) - \wp(z_0))^{m_i}$ to get a function with the same order of poles and zeros as f, which implies it equals f. □

Prop. (11.5.4.8)[Uniformization Theorem]. For any complex numbers $A, B \in \mathbb{C}$ that $A^3 - 27B^2 \neq 0$, there exists a unique lattice $\Lambda \in \mathbb{C}$ that $g_2(\Lambda) = A, g_3(\Lambda) = B$(11.5.4.7). ⌟

Proof: The j-function(20.2.4.22) is surjective, thus there is a $z \in \mathbb{C}$ s.t.

$$1728\frac{1}{1 - \frac{E_6^2}{E_4^3}} = j(z) = 1728\frac{A^3}{A^3 - 27B^2}$$

And if we assume $A, B \neq 0$, then by(20.2.4.5)(21.7.4.1) and(9.5.1.12), assume this implies

$$(\frac{B}{g_3(\tau)})^2(\frac{g_2(\tau)}{A})^3 = 1.$$

Then we can scale Λ by $\Lambda' = \alpha\Lambda$ s.t. $g_3(\Lambda') = B, \quad g_2(\Lambda) = A$.

The case that $A = 0$ or $B = 0$ is similar.

The uniqueness follows from(15.7.8.11). □

5 Quasi-Conformal Mappings

Modulus

Def. (11.5.5.1)[Conformal Annulus]. A **conformal annulus** is an open subset A of $\mathbb{P}^1(\mathbb{C})$ that can be mapped conformally to an annulus $\mathbb{D}(0, (r, s))$ for $r < s \in \mathbb{R}_{\geq 0}$. And in this case, the **module of** A is defined to be $\frac{1}{2\pi}\log(\frac{s}{r})$. And this is an invariance of A. ⌟

Proof: □

Def. (11.5.5.2) [Uniformly Perfect Subsets]. A compact subset $E \subset \mathbb{P}^1(\mathbb{C})$ is called **uniformly perfect** if $\#E \geq 2$, and the modules of the conformal annuli in $\mathbb{P}^1(\mathbb{C}) \setminus E$ that separate E are bounded. ⌟

Beltrami Equations

Def. (11.5.5.3) [Beltrami Coefficients]. For $f \in C^1(\mathbb{C})$ and $z \in \mathbb{C}$ s.t. $\mathrm{d}f$ is non-singular at z, then the **Beltrami coefficient** of f at z is defined to be the number

$$\mu = \frac{\frac{\partial}{\partial \bar{z}} f}{\frac{\partial}{\partial z} f}.$$

By(11.4.1.5), f preserves orientation iff $|\mu| < 1$ at any point.

If $f^{(-1)}$ is the inverse of f near $f(z)$, then

$$|\mu_{f^{-1}}(f(z))| = |\mu_f(z)|,$$

because

$$\frac{\partial}{\partial z} f^{-1} \frac{\partial}{\partial z} f + \frac{\partial}{\partial \bar{z}} f^{-1} \overline{\frac{\partial}{\partial \bar{z}} f} = 0$$

⌟

Def. (11.5.5.4) [Beltrami Equations]. For $\mu \in C(\mathbb{C})$, the equation $\frac{\partial}{\partial z} f = \mu \frac{\partial}{\partial \bar{z}} f$ is called a **Beltrami equation**. ⌟

Prop. (11.5.5.5). If $f \in \mathbb{C}^1(\mathbb{C})$ is non-singular and φ is conformal, then

$$\mu_{\varphi \circ f}(z) = \mu_f(z),$$

$$\mu_{f \circ \varphi}(z) = \mu_f(\varphi(z)) \frac{\overline{\varphi'(z)}}{\varphi'(z)}.$$

⌟

Proof: These follow from the fact that $\frac{\partial}{\partial \bar{z}} \varphi = 0$. □

Def. (11.5.5.6) [Quasiconformal Maps]. For a region $\Omega \subset \mathbb{C}$ and $k \in [0, 1)$, a k-**quasiconformal map** f on Ω is a function $f^\infty(\Omega)$ s.t. $|\mu| \leq k < 1$ at each point $z \in \Omega$. ⌟

Def. (11.5.5.7) [Quasi-Circles]. A **quasi-circle** is a subset of $\mathbb{P}^1(\mathbb{C})$ that can be mapped via a quasiconformal homeomorphism of the sphere to $\partial \mathbb{D}(0, 1) \in \mathbb{P}^1(\mathbb{C})$. ⌟

6 Multi-Variable case

Basics

Should cover the part from [Complex Analytic and Differential Geometry Demailly], [Principle of Algebraic Geometry Griffith/Harris] and [Complex Geometry Daniel].

Def. (11.5.6.1). A function is called **holomorphic** in several variables iff it is holomorphic for each indeterminate. ⌟

Def. (11.5.6.2). For $a \in \mathbb{C}^n$, the **polydisc** $B(a, \varepsilon) \subset \mathbb{C}^n$ is defined to be the set $\{z \| z_i - a_i| < \varepsilon_i\}$. ⌟

Prop. (11.5.6.3) [Hartog's Extension Theorem]. If K is a compact subset in an open domain Ω of $\mathbb{C}^n (n \geq 2)$ and $\Omega - K$ is connected, then any holomorphic function on $\Omega - K$ extends to a holomorphic function on Ω. ⌟

Proof: □

Prop. (11.5.6.4). Let $\varepsilon = (\delta, \ldots, \delta)$ and f be a holomorphic function on the polydisc $\overline{B_\varepsilon(0)}$. Then if f vanishes of order k at the origin and $|f(z)| \leq C$, then

$$f(z) \leq C(\frac{|z|}{\delta})^k$$

for all $z \in \overline{B_\varepsilon(0)}$. ⌟

Proof: Fix $z \in \overline{B_\varepsilon(0)} \neq = 0$, consider the one-variable function $g_z(w) = w^{-k} f(w \cdot \frac{z}{|z|})$, then g_z is holomorphic and $|g_z(w)| \leq \delta^{-k} C$ for $|w| = \delta$. So maximal principle implies that $g_z(w) \leq \delta^{-k} C$ for all $|\omega| \leq \delta$. Hence $|z|^{-k} |f(z)| = |g_z(|z|)| \leq \delta^{-k} C$. □

11.6 Special Functions

References are [Special Functions].

1 Gamma Function

Def. (11.6.1.1)[Gamma Function]. For a complex number s that $\mathrm{Re}(s) > 0$, the **Gamma function** is defined to be

$$\Gamma(s) = \int_0^\infty e^{-t} t^s \frac{\mathrm{d}t}{t}.$$

which is convergent for any $\mathrm{Re}(s) > 0$ thus an analytic function for $\mathrm{Re}(s) > 0$ by(11.4.2.14). ⌟

Prop. (11.6.1.2). For $\mathrm{Re}(s) > 0$, $\Gamma(s+1) = s\Gamma(s)$. ⌟

Proof: For any $\varepsilon \in \mathbb{R}_+$,

$$\int_\varepsilon^{1/\varepsilon} \frac{\partial}{\partial t}(e^{-t}t^s)\mathrm{d}t = -\int_\varepsilon^{1/\varepsilon} e^{-t}t^s\mathrm{d}t + s\int_\varepsilon^{1/\varepsilon} e^{-t}t^{s-1}\mathrm{d}t.$$

Then letting $\varepsilon \to 0$ gives the desired formula. □

Cor. (11.6.1.3). $\Gamma(s)$ extends to a meromorphic function for all $s \in \mathbb{C}$, with simple poles at $s \in \mathbb{Z}_{\leq 0}$. And for $n \in \mathbb{N}$,

$$\mathrm{res}_{s=-n}\,\Gamma(s) = \frac{(-1)^n}{n!}.$$

⌟

Proof: In fact, for $m \in \mathbb{Z}_+$,

$$F_m(s) = \frac{\Gamma(s+m)}{s(s+1)\ldots(s+m-1)}$$

extends $\Gamma(s)$ meromorphically to $\mathrm{Re}(s) > -m$ with simple poles at $s = 0, -1, \ldots, -m+1$, and

$$\mathrm{res}_{s=-m+1}\,F_m(s) = \frac{\Gamma(1)}{(-1)(-2)\ldots(-m+1)} = \frac{(-1)^{m-1}}{(m-1)!}.$$

□

Prop. (11.6.1.4). For $t \in \mathbb{R}_+$, $\Gamma(t)$ is decreasing for $t \leq 1$, and increasing for $t \geq 1$. ⌟

Proof:

$$\frac{\partial}{\partial t}\Gamma(t) = \int_0^\infty \log t e^{-t}t^s \frac{\mathrm{d}t}{t}.$$

□

Prop. (11.6.1.5).

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}.$$

⌟

Proof: By uniqueness theorem, it suffices to prove for $0<s<1$. Then

$$\begin{aligned}\Gamma(1-s)\Gamma(s) &= \int_0^\infty e^{-t}t^{s-1}\Gamma(1-s)\mathrm{d}t = \int_0^\infty e^{-t}t^{s-1}\Big(t\int_0^\infty e^{-vt}(vt)^{-s}\mathrm{d}v\Big)\mathrm{d}t \\ &= \int_0^\infty\int_0^\infty e^{-t(v+1)}v^{-s}\mathrm{d}v\mathrm{d}t = \int_0^\infty \frac{v^{1-s}}{v(v+1)}\mathrm{d}v \\ (11.4.6.7) &= \frac{\pi}{\sin(\pi s)}\end{aligned}$$

□

Cor. (11.6.1.6). There exists constants c_1,c_2 s.t. for any $s\in\mathbb{C}$,

$$|\frac{1}{\Gamma(s)}|\leq c_1e^{c_2|s|\log|s|}.$$

Thus $1/\Gamma(s)$ has order of growth 1. ⌟

Proof: For $\mathrm{Re}(s)>0$

$$\Gamma(s)=\int_0^1 e^{-t}t^{s-1}\mathrm{d}t+\int_1^\infty e^{-t}t^{s-1}\mathrm{d}t=\sum_{n\in\mathbb{N}}\frac{(-1)^n}{n!(n+s)}+\int_1^\infty e^{-t}t^{s-1}\mathrm{d}t,$$

and this equality holds for all $s\in\mathbb{C}$. Thus by(11.6.1.5),

$$|\frac{1}{\Gamma(s)}|=|\frac{\sin(\pi s)\Gamma(1-s)}{\pi}|\leq\Big|\sum_{n\in\mathbb{N}}\frac{(-1)^n}{n!(n+1-s)}\Big|\frac{\sin(\pi s)}{\pi}|+\Big|\int_1^\infty e^{-t}t^{-s}\mathrm{d}t\Big|.$$

Suppose $k=\lfloor\mathrm{Re}(s)+\frac{1}{2}\rfloor$, then

$$\Big|\sum_{n\in\mathbb{N}}\frac{(-1)^n}{n!(n+1-s)}\frac{\sin(\pi s)}{\pi}|\leq\sum_{n\in\mathbb{N},n\neq k}\Big|\frac{1}{n!(n+1-s)}\frac{\sin(\pi s)}{\pi}\Big|+\Big|\frac{\sin(\pi s)}{(k-1)!(s-k)\pi}\Big|$$

and the first term is bounded by $e^{\pi|s|}$, and the second term is bounded by a constant independent of k, because $\sin(\pi s)$ has a zero at $s=k$.

Also,

$$\Big|\int_1^\infty e^{-t}t^{-s}\mathrm{d}t\Big|\leq\int_1^\infty e^{-t}t^{k+1}\mathrm{d}t=(k+1)!\leq e^{(k+1)\log(k+1)}.$$

So the assertion follows. □

Prop. (11.6.1.7) [Special Values].

$$\Gamma(n+1)=n!,n\in\mathbb{N},\quad\Gamma(\frac{1}{2})=\sqrt{\pi}.$$

⌟

Proof: For the first assertion, use induction: $\Gamma(1)=\int_0^\infty e^{-t}\mathrm{d}t=1$, and the induction process follows from(11.6.1.2). The second assertion follows from(11.6.1.5). □

Thm. (11.6.1.8) [Hadamard Product]. For $s \in \mathbb{C}$,

$$\frac{1}{\Gamma(s)} = e^{\gamma s} s \prod_{n \in \mathbb{Z}_+} [(1 + \frac{s}{n}) e^{-s/n}],$$

where γ is the Euler's constant(11.3.5.2). ┘

Proof: By(11.6.1.6)(11.6.1.3) and(11.4.3.20),

$$\frac{1}{\Gamma(s)} = e^{As+B} s \prod_{n \in \mathbb{Z}_+} [(1 + \frac{s}{n}) e^{-s/n}]$$

for some $A, B \in \mathbb{C}$. Taking $s \to 0$, we get $B = 0$ by(11.6.1.3). And $\Gamma(1) = 1$(11.6.1.7) implies that

$$e^{-A} = \prod_{n \in \mathbb{Z}_+} [(1 + \frac{1}{n}) e^{-1/n}] = \lim_{N \to \infty} e^{\log(N+1) - \sum_{n=1}^{N} 1/n} = e^{-\gamma}(11.3.5.2)$$

□

Cor. (11.6.1.9) [Duplication Formula].

$$\Gamma(2s - 1) = \frac{4^{s-1}}{\sqrt{\pi}} \Gamma(s - \frac{1}{2}) \Gamma(s).$$

┘

Proof: □

Cor. (11.6.1.10) [Euler's Formula].

$$\frac{1}{\Gamma(s)} = \lim_{n \to \infty} \frac{s(s+1)\cdots(s+n)}{n^s n!}$$

┘

Proof: This follows from the definition of the infinite product and the definition of Euler's constant(11.6.1.5). □

Prop. (11.6.1.11) [Mellin Inversion Formula]. By(11.11.2.16) applied to $f(x) = e^{-x}$, for any real $c > 0$,

$$e^{-x} = \frac{1}{2\pi \mathrm{i}} \int_{c - \mathrm{i}\infty}^{c + \mathrm{i}\infty} \Gamma(s) x^{-s} ds, x > 0.$$

┘

Thm. (11.6.1.12) [Stirling's Formula]. $|\Gamma(\sigma + it)| \sim \sqrt{2\pi} |t|^{\sigma - \frac{1}{2}} e^{-\pi|t|/2}$. ┘

Proof: □

Def. (11.6.1.13) [Archimedean L-Factors]. Define

$$L_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}), \quad L_{\mathbb{C}}(s) = 2(2\pi)^{-s} \Gamma(s) = \Gamma_{\mathbb{R}}(s) \Gamma_{\mathbb{R}}(s+1).$$

Notice $L_{\mathbb{R}}(1) = 1, L_{\mathbb{C}}(1) = \pi^{-1}$, by(11.6.1.7). ┘

Estimations

Prop. (11.6.1.14). For $n \in \mathbb{Z}_{\geq 2}$,

$$\binom{2n}{n} \geq 2^n, \quad \binom{2n+1}{n} > 2^{n+1}.$$

⌟

Proof: It is true for $n = 2$, and for $n \geq 3$,

$$\binom{2n+1}{n} \geq \frac{2^{2n+1}-2}{2n} \geq 2^{n+1}, \quad \binom{2n}{n} \geq \frac{2^{2n}-2}{2n-1} \geq 2^n$$

□

2 Bessel Function

Def. (11.6.2.1) [Bessel Function]. The **Bessel function** is defined to be

$$B(r,s) = \int_0^1 (1-y)^{r-1} y^{s-1} dy.$$

⌟

Prop. (11.6.2.2).

$$B(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}.$$

⌟

3 K-Bessel Function

Def. (11.6.3.1). The **K-Bessel function** is defined to be

$$K_s(y) = \frac{1}{2}\int_0^\infty e^{-y(t+\frac{1}{t})/2} t^s \frac{dt}{t}, \quad y > 0.$$

it satisfies $K_{-s}(y) = K_s(y)$. ⌟

Prop. (11.6.3.2). $|K_s(y)| \leq e^{-y/2} K_{\mathrm{Re}\, s}(2)$ when $y > 4$. ⌟

Proof: This is because $e^{-ab} < e^{-a}e^{-b}$ when $a, b > 2$. □

Prop. (11.6.3.3).

$$\frac{\partial}{\partial y} K_s(y) = \frac{1}{2}\int_0^\infty (-(t+\frac{1}{t})/2) e^{-y(t+\frac{1}{t})/2} t^s \frac{dt}{t} = -\frac{1}{2}(K_{s+1}(y) + K_{s-1}(y))$$

⌟

Prop. (11.6.3.4). If $\mathrm{Re}(s) > 1/2$ and $r \in \mathbb{R}$,

$$(\frac{y}{\pi})^s \Gamma(s) \int_{-\infty}^\infty (x^2+y^2)^{-s} e^{2\pi \mathrm{i}\, rx} dx = \begin{cases} \pi^{1/2-s}\Gamma(s-\frac{1}{2}) y^{1-s} & r = 0 \\ 2|r|^{s-1/2}\sqrt{y} K_{s-1/2}(2\pi|r|y) & r \neq 0 \end{cases}$$

⌟

Proof: By(11.6.1.1), the LHS equals

$$\int_{-\infty}^{\infty}\int_0^{\infty} e^{-t}(\frac{ty}{\pi(x^2+y^2)})^s e^{2\pi irx}\frac{dt}{t}dx = \int_0^{\infty}\int_{-\infty}^{\infty} e^{-\pi t(x^2+y^2)/y}t^s e^{2\pi irx}dx\frac{dt}{t}$$

where we interchanged the order of integration because it is absolutely convergent, and made a change of variable. Also notice

$$\int_{-\infty}^{\infty} e^{-t\pi x^2/y}e^{2\pi irx}dx = \sqrt{\frac{y}{t}}e^{-y\pi r^2/t}$$

by Fourier inversion(11.11.2.3), so we get the final answer. □

Prop. (11.6.3.5). If $\mathrm{Re}(s)+k/2>1/2$ and r is real,

$$(\frac{y}{\pi})^s\Gamma(s)\int_{-\infty}^{\infty}\frac{1}{(x+yi)^k(x^2+y^2)^s}e^{-2\pi irx}dx = \begin{cases}\pi^{1/2-s}\Gamma(s-\frac{1}{2})y^{1-s} & r=0\\ 2|r|^{s-1/2}\sqrt{y}K_{s-1/2}(2\pi|r|y) & r\neq 0\end{cases}$$

⌟

Proof: By(11.6.1.1), the LHS equals

$$\int_{-\infty}^{\infty}\int_0^{\infty} e^{-t}(\frac{ty}{\pi(x^2+y^2)})^s e^{2\pi\,\mathrm{i}\,rx}\frac{dt}{t}dx = \int_0^{\infty}\int_{-\infty}^{\infty} e^{-\pi t(x^2+y^2)/y}t^s e^{2\pi\,\mathrm{i}\,rx}dx\frac{dt}{t}$$

where we interchanged the order of integration because it is absolutely convergent, and made a change of variable. Also notice

$$\int_{-\infty}^{\infty} e^{-t\pi x^2/y}e^{2\pi\,\mathrm{i}\,rx}dx = \sqrt{\frac{y}{t}}e^{-y\pi r^2/t}$$

by Fourier inversion(11.11.2.3), so we get the final answer. □

4 Hypergeometric Functions

5 Confluent Hypergeometric Functions

6 Dilogarithm

11.7 General Functional Analysis

Basic references are [Rudin Functional Analysis],[Nonarchimedean Functional Analysis].

This section only contains theorems that are applicable to both Archimedean and non-Archimedean valuations. For theorems specialized to non-Archimedean valuations, See p-adic Analysis, for theorems specialized to Archimedean valuations, See Archimedean Functional Analysis. Many propositions in Functional Analysis can be transplanted in the general case, but I haven't finish yet.

The major problem is that convexity is not definable, so Hahn-Banach fail, causing many to fail.

Notation (11.7.0.1).

- Fix a complete valued field $\mathbb{K}$.
- If char $K \neq 0$, then we fix a sequence of elements $\{a_n\}$ that $\lim |a_n| = \infty$. This will be applied for example in the proof of Banach-Steinhaus theorem, but we will just write n instead of a_n.

⌟

1 Topological Vector Space

Def. (11.7.1.1) [Topological Vector Spaces]. A **topological vector space**(TVS) over $\mathbb{K}$ is a $\mathbb{K}$-vector space that the addition and scalar multiplications are continuous. ⌟

Prop. (11.7.1.2). For subsets K, C of a TVS X that K is compact and C is closed, there is a nbhd V that $(K+V)\cap(C+V)=\varnothing$. ⌟

Proof: For each $x \in K$, there are symmetric nbhd V_x that $(x+V_x+V_x+V_x)\cap C=\varnothing$. Then $(x+V_x+V_x)\cap(C+V_x)=\varnothing$. Because K is compact, there are f.m. x_i that $K\subset\cup(x_i+V_{x_i})$, so let $V=\cap V_{x_i}$, then $(K+V)\cap(C+V)=\varnothing$. □

Cor. (11.7.1.3) [Closed Subbasis]. Every nbhd of 0 in a TVS contains a closure of another nbhd of 0. (Apply the above proposition for $K=\{0\}$). ⌟

Def. (11.7.1.4). A subset containing 0 is called **balanced** iff $kU=U$ for each $k\in K$ s.t. $|k|=1$. ⌟

Prop. (11.7.1.5) [Balanced Subbasis]. Every nbhd U of 0 in a TVS contains a balanced nbhd of 0. By(11.7.1.3), we can even assume $\overline{V}\subset U$. ⌟

Proof: Since scalar multiplication is continuous, there is a $\delta>0$ and a nbhd V that $\alpha V\subset U$, for each $|\alpha|<\delta$. Then let $W=\cup_{|\alpha|<\delta}\alpha V$. □

Def. (11.7.1.6) [F-Spaces and Fréchet spaces]. A space is called an **F-space** if its topology is induced by a complete invariant metric. F-space is of second Baire-category by(4.4.9.2)

A locally convex F-space is called a **Fréchet space**. ⌟

Def. (11.7.1.7) [Norm]. For $X\in \mathcal{V}\mathrm{ect}/K$, a **seminorm** on a vector space X is a real-valued function p that $p(x+y)\le p(x)+p(y)$, and $p(\alpha x)=|\alpha|p(x)$ for $\alpha\in k$. It is called a **norm** if moreover $p(x)=0 \iff x=0$.

A family of seminorms $\{p_i\}$ on X is called **separating** iff for each x, at least one p_i satisfies $p_i(x)\neq 0$. ⌟

Prop. (11.7.1.8). A TVS is metrizable by a translation-invariant metric iff it has a countable basis. ⌟

Proof: One direction is trivial, for the other, Cf.[Rudin P18]. □

Prop. (11.7.1.9). If a subspace Y of a TVS X is a F-space, then it is closed in it. ⌟

Proof: Choose an invariant metric d compatible with its topology, Let U_n be a nbhd of X that $U_n \cap Y = B(0, 1/n)$, and choose a symmetric nbhd V_n of X that $V_n + V_n \subset U_n$, and $V_{n+1} \subset V_n$.

If $y \subset \overline{Y}$, then for any $y_n \subset Y \cap (y + V_n) = E_n$, then $y_n - y_m \subset U_{\min\{m,n\}} \cap Y = B(0, 1/n)$, so it is a Cauchy sequence in Y, hence all E_n has a unique element y_0 in common. Now if we intersect each V_n by a nbhd W of X, the same argument shows that there is a unique element y_W in $Y \cap (y + W \cap V_n)$, and this must by just y_0, but $y - y_W \subset W$, so we must have $y = y_0 \subset Y$. □

Def. (11.7.1.10). A set E in a TVS is called **totally bounded** if for every nbhd V of 0, there is a finite set F that $E \subset F + V$. ⌟

2 Completeness

Thm. (11.7.2.1) [Banach-Steinhaus]. Let $X, Y \in$ TVS and $\Gamma \subset \mathrm{Hom}(X, Y)$. If the set

$$B = \{x \in X | \Gamma(x) \text{ is bounded}\}$$

is a second Baire-category set in X, then $B = X$ and Γ is equicontinuous, (thus maps bounded sets to bounded sets). ⌟

Proof: For an open balanced nbhd W of 0, choose a balanced nbhd U s.t. $\overline{U} + \overline{U} < W$(11.7.1.5), set $E = \cap_{\Lambda \in \Gamma} \Lambda^{-1}(\overline{U})$, then $B \subset \bigcup_{i=1}^{\infty} nE$, so by Baire theorem(4.4.9.2), E has a interior point thus has a nbhd V s.t. $\Gamma(V) \subset \overline{U} + \overline{U} \subset W$. Thus we are done. □

Cor. (11.7.2.2) [Uniform Boundedness Theorem]. If $X, Y \in$ TVS and X is an F-space(11.7.1.6). Suppose $\Gamma \subset \mathrm{Hom}(X, Y)$ satisfies $\Gamma(x)$ is bounded for any $x \in X$, then Γ is equicontinuous. ⌟

Cor. (11.7.2.3). Let $X, Y \in$ TVS and X is an F-space. If $(A_n) \in \mathrm{Hom}(X, Y)^{\mathbb{Z}_+}$ is a sequence of continuous linear mapping, then $\varinjlim A_n = A$ iff $\{||A_n||\}$ is bounded and $\varinjlim A_n x = Ax$ for x in a dense subset of X. ⌟

Proof: One direction is immediate from Banach-Steinhaus and(11.7.1.6), the converse is an easy $\varepsilon/3$-technique. □

Cor. (11.7.2.4) [Strong operator convergence]. Let $X, Y \in$ TVS and X is an F-space. If $(A_n) \in \mathrm{Hom}(X, Y)^{\mathbb{Z}_+}$ is a sequence of continuous linear mapping s.t. $\varinjlim A_n x = Ax$ for any $x \in X$, then $\varinjlim A_n = A$. ⌟

Thm. (11.7.2.5) [Open Mapping theorem]. Let $X, Y \in$ TVS and X is an F-space. Suppose $T \in \mathrm{Hom}(X, Y)$ satisfies $\mathrm{Im}(T)$ is of second Baire-category in Y, then it is a surjective open mapping and Y is an F-space.

In fact, we only need T be defined on a subspace $D(T) \subset X$ and it is a **closed operator** in the sense that its graph is closed. ⌟

Proof: $V_n = T(B(0, \frac{r}{2^n}))$ are all of second category, because $\cup_n n V_n = R(T)$, so $\overline{V_n}$ has an interior by definition. Then also it contains a nbhd of V because $\overline{V_{n+1}} + \overline{V_{n+1}} \subset \overline{V_n}$.

Now we show $\overline{V_{n+1}} \subset V_n$, which will imply that T is open. thus for a $y \in \overline{V_n}$ since $\overline{T(V_{n+1})}$ contains a nbhd of 0, we can consecutively choose $x_i \in B(0, \frac{r}{2^{n+i}})$ s.t. $y - \sum_{i=1}^{n} T(x_i) \in \overline{T(B(0, \frac{1}{2^{n+i+1}}))}$. So by completeness of X and closedness, $\sum x_i$ converges to some $x \in D(T)$, and $Tx = y \in V_n$.

And an open linear mapping must be surjective. hence $Y \cong X/N(T)$, so Y is also an F-space. □

Cor. (11.7.2.6) [Banach Theorem]. If a continuous map T between F-spaces is a bijection, then it has a continuous inverse. ⌟

Cor. (11.7.2.7). If a F-space is complete w.r.t two different topologies and one is stronger than the other, then they are equivalent. ⌟

Cor. (11.7.2.8). For every operator between F-spaces that has closed image, we have $X/N(T) \cong R(T)$. ⌟

Cor. (11.7.2.9) [Closed Graph Theorem]. If $T : X \to Y$ is a closed linear mapping between two F-spaces, i.e. the graph of it is closed, then it is continuous.

Notice the graph being closed is equivalent to if $x_i \to x$ and $Tx_i \to y$, then $y = Tx$. This is very useful when proving some map is continuous. ⌟

Proof: Because the metric induced by the graph is stronger than the original one, we can use Banach Theorem. □

Cor. (11.7.2.10). If A, B, C are F-spaces, and $f : A \to B, g : B \to C$, if gf, g is continuous and g is injective, then F is continuous. ⌟

Proof: Use closed graph theorem, if $x_i \to x, f(x_i) \to z$, then $gf(x_i) \to g(z)$, so $gf(x) = g(z)$, so $f(x) = z$. □

Cor. (11.7.2.11) [Finite Codimensional Image]. If the image of a continuous linear mapping T between F-spaces has finite codimensional image, then the image is closed and complemented. ⌟

Proof: It has finite codimension, so we can construct $K^n \oplus X/N(T) \to Y$, by Banach theorem(11.7.2.6) it is a homeomorphism, and the image of $X/N(T)$ corresponds to the image, so the image is closed. □

Prop. (11.7.2.12) [Separate Continuous]. If a bilinear map $B : X \times Y \to Z$ where X is a F-space is separately closed, then $B(x_n, y_n)$ converges to $B(x_0, y_0)$. ⌟

Proof: Use Banach-Steinhaus to prove $B_{y_n}(x)$ is equicontinuous, then use $B(x_n - x_0, y_n) + B(x_0, y_n - y_0)$. ? □

3 Dual Space

Prop. (11.7.3.1) [Operator Space]. If X, Y are normed spaces then $L(X, Y)$ is also a normed space with the metric $||\Lambda|| = \sup\{||\Lambda x|| |x| \le 1\}$. And if Y is Banach, then $L(X, Y)$ is also Banach. The proof is easy.

In particular, X^* is a Banach space. ⌟

Prop. (11.7.3.2). For a bounded operator T,

$$\overline{R(T)} = N(T^*)^{\perp}, \text{ Thus } \overline{R(T^*)} = N(T)^{\perp}$$

In particular, using Hahn Banach, $R(T)$ is dense in Y iff T^* is injective, T is injective iff T^* is weak*-dense in X^*. ⌟

Prop. (11.7.3.3). Let $\Lambda_1, \ldots, \Lambda_n, \Lambda$ are linear functionals on a vector space X, let $N = \cap \ker f_i$, the following are equivalent:

1. $\Lambda = \sum \alpha_i \Lambda_i$.
2. $|\Lambda x| \leq \gamma |\Lambda_i x|$.
3. $\ker \Lambda \subset N$.

⌟

Proof: Only need to show $3 \to 1$: define $\pi : X \to k^n : x \mapsto (\Lambda_1 x, \ldots, \Lambda_n x)$, then by hypothesis $f(\pi_i(x)) = \Lambda(x)$ defined a linear functional on $\pi(X)$. This can be extended to a functional on $k^n : F(u_1, \ldots, u_n) = \sum \alpha_i u_i$, so Λ is a linear combination of Λ_i. □

Weak Convergence

Def. (11.7.3.4) [Operator Topologies]. There are three topologies on $L(X)$ for a normed space X:

- norm topology: $||T_i - T|| \to 0$.
- strong topology: $\forall x \in X, ||(T_i - T)x|| \to 0$.
- weak topology: $\forall x \in X, f \in X^*$, $\lim f(T_n x) = f(Tx)$.

⌟

Prop. (11.7.3.5) [Weak Convergence and Boundedness]. In a normed space X, if $x_n \to x$ weakly iff $\{x_n\}$ is bounded and $\lim f(x_n) = f(x)$ for f in a dense subset a dense subset $M \subset X^*$. ⌟

Proof: This follows from(11.7.2.3), as X^* is a Banach space, by(11.7.3.1). □

4 Banach Spaces

Def. (11.7.4.1) [Normed(Valued) K-Spaces]. A **normed(valued) K-space** is a TVS over K with a norm that satisfies $||kv|| = |k|.||v||$ for $k \in K$. ⌟

Def. (11.7.4.2) [Banach Spaces]. A complete normed(valued) K-vector space(11.7.4.1) is called a **Banach space**.

A K-algebra with a complete K-algebra norm is called a **Banach algebra**. ⌟

Prop. (11.7.4.3). The dual space of a Banach space is a Banach space. (Immediate from(11.7.3.1)). ⌟

Prop. (11.7.4.4). If A is a Banach space as well as a topological group, then there is a norm on A which induce the same topology and makes A into a Banach algebra. ⌟

Proof: embed A into $L(A)$ by left multiplication, which is injective, and $||x|| = ||xe|| = ||M_x e|| \leq ||M_x||||e||$, so its inverse is continuous. Now if we show the image $\tilde{A}$ is closed in $L(A)$, then the open mapping theorem will show that $A \cong \tilde{A}$, and $\tilde{A}$ is clearly a Banach algebra.

To show it is closed, if $T = \lim T_i$, notice $T_i(y) = T_i(e)y$, so take a limit, $T(y) = T(e)y = M_{T(e)}y$. □

Cor. (11.7.4.5). Any f.d. Banach algebra A is isomorphic to $\mathrm{Mat}(n; K)$ for some $n \in \mathbb{N}$. In particular, if $xy = e$, then $yx = e$. ⌟

Proof: Embed A into $L(A)$. □

Remark (11.7.4.6) [Inequivalent Banach Norms]. There exist two complete norm on a vector space that are inequivalent. For this, just choose a Banach space X, and notice if we can choose a discontinuous bijection $X \to X$, then the induced metric is also complete, and it cannot by equivalent by Banach theorem(11.7.2.6). For this, choose a infinite dimensional Banach space over $\mathbb{C}$, and choose a $\mathbb{C}$-basis x_i for it, and choose a sequence x_n and maps x_n to nx_n, the rest are invariant, then this is not continuous. ⌟

Hilbert Space

Def. (11.7.4.7). there are different topologies in the space of operators on a Hilbert space $\mathcal{H}$.
Norm operator topology: defined by the norm $||T||$.
Strong operator topology: defined by the separating seminorms $T \mapsto ||Tu||, u \in \mathcal{H}$.
Weak operator topology: defined by the separating seminorms $T \mapsto (Tu, v), u, v \in \mathcal{H}$. ⌟

Prop. (11.7.4.8). The strong and weak operator topology coincides on the unitary operators on $\mathcal{H}$. The sets of unitary operators that is continuous in this two topology is denoted by $U(\mathcal{H})$. ⌟

Proof: If T_n converges to T in the weak operator topology, then

$$||(T_n - T)u||^2 = ||Tu||^2 + ||T_n u||^2 - 2\,\mathrm{Re}(T_n u, Tu).$$

The right hand side is clearly bounded by the weak seminorms, so the two topologies coincide. □

Prop. (11.7.4.9) [Hilbert Basis]. If H is a Hilbert space and $S = \{e_\alpha\}$ is an orthonormal basis in H, then the following are equivalent:

1. For any x, $x = \sum(x, e_\alpha)e_\alpha$,(notice the sum are in fact infinite sum).
2. There is a no nonzero element x that is orthogonal to all e_α.
3. **Parseval equality** holds: $||x||^2 = \sum|(x, e_\alpha)|^2$.

If these are true, then S is called a **Hilbert basis** of H, a Hilbert basis always exists, by Zorn's lemma. ⌟

Proof: $1 \to 2$: if $(x, e_\alpha) = 0$ for all e_α, then by 1, $x = \sum(x, e_\alpha)e_\alpha = 0$.
$2 \to 3$: Notice $y = x - \sum(x, e_\alpha)e_\alpha$ is orthogonal to all e_α, and

$$||y|| = ||x||^2 - \sum|(x, e_\alpha)|^2,$$

so Parseval equality holds.
$3 \to 1$: $||x - \sum(x, e_\alpha)e_\alpha|| = 0$. □

Prop. (11.7.4.10). Any symmetric operator on a Hilbert space is continuous. ⌟

Proof: Because $x_n \to 0$ implies $Tx_n \to 0$ weakly, so we can use closed graph theorem(11.7.2.9).**?**
□

Ultranormed Banach Spaces

The ultranormed Banach spaces are defined in(14.2.4.5).

Nuclear Maps and Spaces

11.8 Archimedean Functional Analysis

References are [Rud91]. [Rudin Functional Analysis Chap11,13] needs to be revisited.

This section contains functional analysis in characteristic 0. By Ostrowski theorem(11.2.3.18), the base field is just $\mathbb{R}$ or $\mathbb{C}$.

1 Topological Vector Space

Def. (11.8.1.1) [Seminorms]. A **sublinear functional** is a function p that $p(x+y) \leq p(x)+p(y)$ and $p(\lambda x) = \lambda p(x)$ for $\lambda > 0$.

A **seminorm** is a non-negative function p that $p(x+y) \leq p(x)+p(y)$ and $p(\alpha x) = |\alpha| p(x)$ for all complex α. ⌟

Def. (11.8.1.2). A **absorbing set** is a convex set A that $\cup_{k>0} kA = X$. A convex nbhd of 0 is clearly absorbing. ⌟

Def. (11.8.1.3) [Minkowski Functional]. For an absorbing set A, the **Minkowski functional** μ_A is defined to be $\mu_A(x) = \inf\{t > 0, x/t \in A\}$. It satisfies:

- $\mu_A(x+y) \leq \mu_A(x) + \mu_A(y)$.
- $\mu_A(kx) = k\mu_A(x)$ if $k > 0$.
- μ_A is a seminorm if A is balanced.
- If $B = \{x|\mu(x) < 1\}, C = \{x|\mu(x) \leq 1\}$, then $B \subset A \subset C$ and $\mu_A = \mu_B = \mu_C$.

⌟

Proof: Cf.[Rudin P27]. □

Cor. (11.8.1.4) [Seminorm and Absorbing set]. A seminorm on X is exactly the Minkowski functional of a balanced absorbing set W, but the set may not be unique. and it is uniformly continuous iff 0 is an interior point. ⌟

Proof: If p is a seminorm, then $\{x|p(x) < 1\}$ is convex, balanced and absorbing by definition(11.7.1.7). The converse is by(11.8.1.3). The last assertion is easy. □

Prop. (11.8.1.5) [Minkowski Functional and Separating Seminorms]. If $\mathfrak{B}$ is a convex local base in a TVS X, then the Minkowski functionals of elements of $\mathfrak{B}$ forms a separating family of seminorms.

Conversely, a separation family $\mathfrak{P}$ of seminorms on a vector space defines a convex balanced local base for a topology τ that is locally convex. And in this topology, a sequence converges iff $p(x_i - x) \to 0$ for $p \in \mathfrak{P}$, a set is bounded if each p is bounded on it. ⌟

Proof: For any $V \in \mathfrak{B}$, $V = \{x \in X|\mu_V(x) < 1\}$, because V is open and convex. (11.8.1.3) shows each μ_V is a seminorm, and it is continuous because it is bounded on V. And they are separating because $\mathfrak{B}$ is a local base.

Defined $V(p,n) = \{x \in X|p(x) < 1/n\}$, and let these be a local subbasis at 0, and make it a topology by translation. This is checked to be a locally convex TVS. For the last assertion, if E is bounded, then $E \subset kV(p,1)$ for k large, so p is bounded on E, and conversely, for each nbhd U, there are p_i and M_i and $\cap V(p_i, M_i) \subset U$, so $E \subset kU$ for n large. □

Prop. (11.8.1.6). If $\mathfrak{P}$ is a family of countable separating family of semi-norms on X, then the topology defined in(11.8.1.5) is in fact metrizable, by a metric $d(x,y) = \sum \frac{1}{2^k}\frac{p_i(x-y)}{1+p_i(x-y)}$. ⌟

Finite Dimensional Subspace

Prop. (11.8.1.7)[Finite Dimensional and Locally Compact]. There is only one topological vector space structure on a finite dimensional $\mathbb{C}$-vector space and it is complete. A TVS is locally compact iff it is f.d. ⌟

Proof: Cf.[Rudin P17].

For the second assertion, if is locally compact, then 0 has a nbhd V that is precompact, so bounded, hence $2^{-n}V$ forms a local basis. the compactness of $\overline{V}$ shows there are f.m. x_i that $\overline{V} \subset \cup(x_i + \frac{1}{2}V)$. Let Y be the subspace spanned by x_i, then it is of f.d, thus closed. Now $V \subset Y + \frac{1}{2}V$, so $\frac{1}{2}V \subset Y + \frac{1}{4}V$, hence continuing this way, $V \subset \cap(Y + 2^{-n}V)$, so $V \subset \overline{Y} = Y$. But then $Y = X$. □

Cor. (11.8.1.8)[Finite Subspace Closed]. A f.d subspace in a TVS over $\mathbb{C}$ is closed, because it must be a F-space, hence it is closed by(11.7.1.9). ⌟

Prop. (11.8.1.9) [Finite Subspace in Banach Space]. For a finite dimensional space V in an Archimedean Banach space, there is a continuous projection onto it. In particular, any finite dimensional space in an Archimedean Banach space is complemented.

Also finite codimensional subspace in any Banach space is complemented by(11.7.2.11). ⌟

Proof: Choose a basis e_i for V, consider the dual basis f_i. Because a finite dimensional space only has one topology(11.8.1.7), these f_i are bounded on V. Extend them to bounded functional on X, then consider $p(x) = \sum f_i(x)e_i$, then this is a continuous projection onto V. □

2 Various Spaces and Duality

For a bounded connected open set Ω,

Prop. (11.8.2.1)[Various Spaces and Duality].

- **Sobolev Space** $W^{m,p}(\Omega)$ is the completion of a subspace of $C^\infty(\Omega)$ with the norm**?**

$$||u||_{m,p} = (\sum_{|\alpha|\leq m}\int_\Omega |\partial^\alpha u(x)|^p \mathrm{d}x)^{1/p}.$$

  for $m > 0$. And we denote $W^{m,2}(\Omega)$ by $H^m(\Omega)$. It is also a subspace of $L^p(\Omega)$ that satisfies this, without completion(11.11.4.1).
- $C_0^\infty(\Omega)$ is the subspace of $C^\infty(\Omega)$ that have compact support in Ω. Its completion $W_0^{m,p}(\Omega)$ is a closed subspace of $W^{m,p}(\Omega)$. And we denote $W_0^{m,2}(\Omega)$ by $H_0^m(\Omega)$ and the dual space of $H_0^m(\Omega)$ by $H^{-m}(\Omega)$.
- For a locally convex space X, $C(X)$ in the topology of compact convergence is a Fréchet space(11.7.1.6).
- $\mathcal{O}(\Omega) \subset C(\Omega)$ the space of holomorphic functions in Ω is a closed subspace of $C(\Omega)$ by(11.4.2.15), thus it is a Fréchet space. By Hausdorff theorem(4.4.8.7), Montel's theorem says exactly that $\mathcal{O}(\Omega)$ has the Heine-Borel property(11.7.1.6).
- $\mathcal{O}^2(D)$ the space of holomorphic functions on $\mathbb{D}$ that is also L^2. It has the L^2 norm.
- $C^\infty(\Omega)$ in the topology defined by seminorms $p_N(f) = \max\{|D^\alpha f(x)| : x \in K_N, |\alpha| \leq N\}$, is a Fréchet space thus locally convex and it has the Heine-Borel property by Arzela-Ascoli.

- For $K \subset \Omega$ closed, $D(K)$ is the closed subspace of smooth functions on Ω with support in K, thus a Fréchet space with Heine-Borel property.
- $D(\Omega)$ is the space of smooth functions with support in Ω. It has the topology generated by translation of basis consisting of convex balanced sets W that $W \cap D(K)$ is open for every compact K. This makes $D(\Omega)$ into a locally convex TVS, Cf.[Rudin P152]. It has Heine-Borel property(11.11.1.1).
- (Schwartz Functions) The space of **Schwartz functions** $\mathcal{S}(\mathbb{R}^n)$ is defined as smooth functions on $\mathbb{R}^n$ s.t.

$$\sup_{|\alpha|\leq N, x\in\mathbb{R}^n} (1+|x|^2)^N |(D_\alpha f)(x)| < \infty$$

for any $N > 0$. And it is a Fréchet space define by these seminorms.

⌟

Dual Spaces

Prop. (11.8.2.2).
- For a σ-finite measure space (X, Ω, μ) and $1 \leq p < \infty$, by(11.3.6.3),

$$L^p(X, \Omega, \mu)^* = L^q(X, \Omega, \mu).$$

- $C[0, 1]^* = BV[0, 1]$ and $C[X]^* = \mathrm{Meas}(X)$, the space of complex measure on compact X with the norm of total variance, by Riesz representation theorem(11.10.1.10).

⌟

3 Convexity

Prop. (11.8.3.1). Every convex nbhd of 0 contains a balanced convex nbhd of 0. By(11.7.1.3), we can even assume $\overline{V} \subset U$. ⌟

Proof: If U is convex, choose W as in(11.7.1.5), then $W \subset A = \cap_{|\alpha|=1} \alpha U$ because it is balanced. Then $W \subset A^\circ$ and A° is open and balanced, satisfying the requirement. □

Prop. (11.8.3.2). For a compact convex set K in a TVS X, if a set Γ of continuous linear mapping is bounded for every $x \in K$, then Γ is equicontinuous on K. ⌟

Proof: The proof is similar to that of Banach-Steinhaus(11.7.2.1). For K compact convex, the same argument shows that there is a nbhd V that $K \cap (x_0 + V) \subset nE$, fix $p > 1$ that $K \subset x_0 + pV$, then for any $x \in K$, consider $z = (1-p^{-1})x_0 + p^{-1}x$, then $z \in K$ as K is convex and $z - x_0 = p^{-1}(x - x_0) \in V$, so $z \in nE$, and since $x = pz - (p-1)x_0$, $\Lambda x \in pnW$ for each $\Lambda \in \Gamma$, so Γ is equicontinuous. □

Hahn-Banach

Prop. (11.8.3.3) [Real Hahn]. For a sublinear functional p on a real linear space X and a subspace X_0, if a functional f satisfies $f(x) \leq p(x)$ on X_0, then it can be extended to a functional Λ on X that $|\Lambda(x)| \leq |p(x)|$. ⌟

Proof: Use Zorn's lemma, if the maximum extension is not on the whole space but on M, choose $x_1 \in X - M$, we want to define $f(x_1)$. Now let $M_1 = \{x + tx_1 | x \in M\}$. Since for $x, y \in M$, $f(x) + f(y) = f(x + y) \leq p(x + y) \leq p(x - y) + p(x_1 + y)$, so

$$f(x) - p(x - x_1) \leq p(y + x_1) - f(y)$$

for $x, y \in M$. Let the maximum of the left side be α, and define $f(x_1) = \alpha$, then it is clear $f(z) \le p(z)$ still. □

Prop. (11.8.3.4) [Complex Hahn]. For a seminorm p (i.e. it can attain 0) on a complex linear space X and a subspace X_0, if a functional f satisfies $|f(x)| \le p(x)$ on X_0, then it can be extended to a functional on X with the same condition. ⌟

Proof: Let $g(x) = \mathrm{Re}\, f(x)$ and extend it by Hahn and set $f(x) = g(x) - ig(ix)$, then f is complex linear, and for any x, for some $|\alpha| = 1$, $|f(x)| = f(\alpha x) = g(\alpha x) \le p(\alpha x) = p(x)$. □

Cor. (11.8.3.5) [Hahn]. In a normed space X, a bounded linear functional on a subspace X_0 can be extended to a bounded functional on X with the same norm. ⌟

Cor. (11.8.3.6) [Extending Functional Preserving Norm]. If X is a normed space and N is a closed subspace, if x_0 satisfies $d = d(x_0, M) > 0$, then here is a continuous functional f that $f(x) = 0$ and $f(x_0) = d$ and $||f|| = 1$. ⌟

Proof: Define $f(m + \alpha x) = |\alpha| d$ on $\mathrm{span}\{M, x\}$, then $f(m + \alpha x) = |\alpha| d = |\alpha| d(x_0, M) \le |\alpha| ||\frac{x'}{\alpha} + x_0|| = ||x' + \alpha x|| = ||x||$. So $||f|| \le 1$, so we can use Hahan-Banach to extend it to a functional on X. □

Prop. (11.8.3.7) [Geometric Hahn].

- If E_1 and E_2 are two convex set that $E_1 \cap E_2 = \emptyset$ and E_1 has interior point, then there is a continuous linear functional that separate them, i.e $\mathrm{Re}\, f(E_1) < \mathrm{Re}\, f(E_2)$. (The interior point is here to assure f is continuous).
- In a locally convex TVS, if E_1 is convex compact and E_2 is convex closed, then there is a real functional that separate them, i.e. $\mathrm{Re}\, f(E_1) < \gamma_1 < \gamma_2 < \mathrm{Re}\, f(E_2)$. Thus for a set E and a point x, $x \in \overline{\mathrm{span} E} \iff$ for all f that $f(E) = 0$, $f(x) = 0$.

⌟

Proof: The complex case follows from the real case, so assume it is real. Consider $a_0 \in E_1, b_0 \in E_2$, let $x_0 = a_0 - b_0$ and let $C = E_1 - E_2 + x_0$, then C is a convex nbhd of 0. Let p be the Minkowski functional of C, then p is sublinear by(11.8.1.3) and $p(x_0) \ge 1$. Let $f(tx_0) = t$ on the subspace M generated by x, then it extends to a functional Λ that≤ 1 on C, thus it is bounded by 1 on $C \cap (-C)$, hence continuous. For any $a \in E_1, b \in E_2$, because $\lambda(x_0) = 1$ and $a - b + x_0 \in C$ open, $\Lambda a < \Lambda b$.

For the second, There is a convex nbhd V of 0 that $E_1 + V \cap B = \varphi$, so the above argument applied with $E_1 + V$ and B shows that there is a f that separate them. And $f(E_1 + V)$ is open and $f(E_1)$ is compact, so the conclusion follows. □

Cor. (11.8.3.8) [Banach-Saks]. The weak closure of a convex set in a locally convex metric space equals the original closure.

Thus if a sequence $\{x_n\}$ weakly converges to x in a metrizable locally convex space, then a convex combination of $\{x_n\}$ strongly converge to x, i.e. $x \in \overline{\mathrm{co}}(\{x_n\})$, because metric space is first countable. ⌟

Proof: A weak closed set is closed, and to show the closure is weakly closed, use(11.8.3.7). □

Prop. (11.8.3.9). If A_i are compact convex sets in a TVS X, then $co(A_1 \cup \ldots \cup A_n)$ is compact. ⌟

Proof: Firstly, the image K of $S \times A_1 \times \ldots \times A_n$, $(s_1, \ldots, s_n) \times (a_1, \ldots, a_n) \mapsto \sum s_i a_i$ is closed, where $S = \{0 \le x_i, \sum x_i = 1\}$. And we show K is just the convex closure: it contains all A_i, and it is convex because each A_i is. □

Prop. (11.8.3.10). In F-space, a closed subset is compact iff it is totally bounded by(4.4.8.7). ⌟

Prop. (11.8.3.11). In a locally convex space, if E is totally bounded, then $\mathrm{co}(E)$ is totally bounded. Thus in a Fréchet space, if K is compact, then $\overline{co}(K)$ is compact. ⌟

Proof: For a nbhd U of 0, choose a convex nbhd V that $V+V\subset U$, then $E\subset F+V$ for some finite set F, hence $co(E)\subset co(F)+V$. But $co(F)$ is compact by(11.8.3.9). So $co(F)\subset F_1+V$ for some finite set F_1, then $co(E)\subset F_1+U$.

If K is compact, then it is totally bounded, and then $co(K)$ is totally bounded and $\overline{co(K)}$ is totally bounded by(4.4.8.5), so it is compact by(11.8.3.10). □

Prop. (11.8.3.12)[Weakly Bounded and Locally Convex]. In a locally convex space, bounded $\iff$ weakly bounded. ⌟

Proof: One direction is trivial, for the other, suppose E is weakly bounded and U is a closed nbhd of 0. Because X is locally convex, there is a convex, balanced nbhd of 0 that $\overline{V}\subset U$(11.8.3.1). Now $\overline{V}=V^{**}$ the polar(11.8.4.1) by(11.8.3.8).

Now V^* is weak*-compact and $|\Lambda(x)|\leq\gamma(\Lambda)$ for each $\Lambda\in X^*$ for some $\gamma(\Lambda)$ because E is weakly bounded. So we can use(11.8.3.2) to show that $|\Lambda x|\leq\gamma$ for some γ and all $\Lambda\in V^*$. So we have $\gamma^{-1}E\subset\overline{V}\subset U$. This proves that E is bounded. □

Prop. (11.8.3.13) [Markov-Kakutani Fixed Point Theorem]. For a commuting family $\mathcal{F}$ of continuous affine maps from K to K where K is a compact convex set in a TVS, then there is a fixed point in K for all maps in $\mathcal{F}$. ⌟

Proof: Consider the semigroup $\mathcal{F}^*$ generated by these maps together with their average, it is also commutative because they are all affine. For any $f,g\in\mathcal{F}^*$, $f(K)\cap g(K)\supset f\circ g(K)$, so by finite intersection property, there is a point in $p\in K$ in all $f(K)$.

For this p, consider $p=\frac{1}{n}(I+T+t^2+\ldots+T^{n-1})(x)$, then $p-Tp=\frac{1}{n}(x-T^nx)\in\frac{1}{n}(K-K)$. as K is bounded and n is arbitrary, this means that $p=Tp$ for all T. □

Cor. (11.8.3.14)[Invariant Hahn]. For a commuting family Γ of operators on a normed space and Y an invariant space, then for any Γ-invariant continuous functional f on Y, it has a Γ-invariant Hahn extension. ⌟

Proof: We may assume $||f||=1$. Let K be all extensions of f that has norm≤ 1. K is obviously convex, and it is weak*-compact by Banach-Alaoglu. The adjoint action of T is checked to be continuous in the weak*-topology, so by(11.8.3.13), there is some $F\in K$ that is invariant under Γ. □

Krein-Milman theorem

Thm. (11.8.3.15) [Krein-Milman]. For a compact convex set K in a TVS X that is weakly-Hausdorff(X^* separate points), $K=\overline{\mathrm{co}}(\mathrm{Extreme}(K))$.

If K is a compact set in a locally convex space, then $K\subset\overline{\mathrm{co}}(E(K))=\overline{\mathrm{co}}(K)$. ⌟

Proof: First show that every compact extreme set S of K contains an extreme point. Notice arbitrary intersection of compact extreme sets of K is compact extreme, because compact is closed, because X is Hausdorff. And for any functional $\Lambda\in X^*$, the maximal value point in K is compact extreme. Now we use Zorn's lemma to find a minimal compact extreme set in S, then it must be a point because X^* separate points.

Now use the weak topology Hahn(11.8.4.2), if $\overline{co}(E(K)) \subset K$ is not K, then it is compact, then we can find a functional that separate $\overline{co}(E(K))$ and some point of K. This is a contradiction because the extreme value point for any functional on K is an extreme set.

In the locally convex case, the convexity of K is not needed, and we can show using geometric Hahn(11.8.3.7) instead that, $K \subset \overline{co}(K)$. □

Prop. (11.8.3.16) [Milman's Theorem]. If K is a compact set in a locally convex space X and if $\overline{\mathrm{co}}(K)$ is also compact(e.g in a Fréchet space(11.8.3.11)), then every extreme point of $\overline{\mathrm{co}}(K)$ lies in K. ⌟

Proof: □

Def. (11.8.3.17). For a compact Hausdorff space S and an algebra $A \subset C(S)$, a subset E is called A**-antisymmetric** iff every $f \in A$ that is real on E is constant on E. There are in fact maximal A-antisymmetric subsets of S. ⌟

Prop. (11.8.3.18) [Bishop Theorem]. If A is a closed subalgebra of $C(S)$. If $g \in C(S)$ satisfies $g|_E \in A|_E$ for every maximal A-antisymmetric set E, then $g \in A$. This theorem is a generalization of Stone-Weierstrass approximation. ⌟

Proof: The annihilator $A^\perp$ of A consists of all regular complex Borel measure μ on S that $\int f d\mu = 0$ for all $f \in A$ by Riesz representation(11.10.1.10). ?Cf.[Rudin P122]. □

Prop. (11.8.3.19)[Schauder Fixed Point Theorem]. If C is a closed convex subset in a metrizable TVS and continuous $T : C \to C$ has sequentially compact image (e.g. C is compact and X is locally convex hence X^* separate points), then T has a fixed point. ⌟

Proof: As $T(C)$ is sequentially compact, for each n, there is a $1/n$-net $N_n = \{y_i\} \subset T(C)$, let $E_n = \mathrm{span}\{N_n\}$.

Define a map $T(C) \to co(N_n) : I_n(y) = \sum y_i\lambda_i(y)$, where $\lambda_i(y) = \frac{m_i(y)}{\sum m_i(y)}$, and $m_i(y) = 1-n||y-y_i||$ if $y \in B(y_i, 1/n)$, and 0 otherwise.

Now $||I_n(y) - y|| = ||\sum(y_i - y)\lambda_i(y)|| \leq \sum ||y_i - y||\lambda_i(y) \leq \frac{1}{n}$ for each $y \in T(C)$. As C is convex, $co(N_n) \subset C$, if we let $T_n = I_n \circ T$, then T_n has a fixed pt x_n in $co(N_n)$ by Brower fixed pt theorem(4.14.4.2).

As $T(C)$ is sequentially compact and C is closed, there is a subsequence Tx_{n_k} that converges to $x \in C$. And then

$$||x_{n_k} - x|| = ||I_nTx_{n_k} - x|| \leq ||I_nTx_{n_k} - Tx_{n_k}|| + ||Tx_{n_k} - x|| < \frac{1}{n} + ||Tx_{n_k} - x||$$

so $x_{n_k} \to x$, and then by continuity, $Tx = x$. □

Vector-valued Integrations

Def. (11.8.3.20) [Vector-Valued Integration]. Given a measure space (Q, μ) and X is an Archimedean TVS on which X^* separate points. If f is a function from M to X that $\Lambda \circ f$ are integrable w.r.t μ for any $\Lambda \in X^*$. The **integration** $\int_M f d\mu$ of f w.r.t Q is an element y that

$$\Lambda y = \int_Q (\Lambda f) d\mu$$

for any $\Lambda \in X^*$. ⌟

Prop. (11.8.3.21). If X is an Archimedean TVS on which X^* separate points, (Q, μ) is a Radon measure on a locally compact Hausdorff space that μ is compactly supported, and f is continuous that $\overline{co}(f(Q))$ is compact(e.g. when X is Fréchet(11.8.3.11)), then the integral $y = \int_Q f d\mu$ exists, and belongs to the closed linear span of the range of H. Moreover if μ is positive and $\mu(Q) = 1$, then $y \in \overline{co}(f(Q))$. ⌟

Proof: Cf.[Rudin P78]. □

Cor. (11.8.3.22). If Q is Hausdorff, $d\mu$ is compactly supported, X is Archimedean Banach and $f : Q \to X$ is continuous, then

$$||\int_Q f d\mu|| \leq \int_Q ||f|| d\mu$$

⌟

Proof: Let $y = \int_Q f d\mu$. By(11.8.3.6), there is a $||\Lambda|| \leq 1$ that $\Lambda y = ||y||$, so

$$\Lambda y = ||y|| = \int_Q \Lambda f d\mu = |\int_Q \Lambda f d\mu| \leq \int_Q |\Lambda f| d\mu \leq \int_Q ||f|| d\mu$$

□

Prop. (11.8.3.23). If X is an Archimedean TVS on which X^* separate points, Q is a compact subset of X, and $\overline{co}(Q)$ is compact, then $y \in \overline{co}(Q)$ iff there is a regular Borel measure μ on Q that $y = \int_Q x d\mu(x)$. ⌟

Proof: Cf.[Rudin P79]. □

Prop. (11.8.3.24)[Continuous Action Extends to Measure]. For a fixed map $f : Q \to X$, assume X is a Fréchet space, then the integration functor in(11.8.3.21) induces a continuous map

$$Meas_c(Q) \to X : \mu \mapsto \int_\mu f$$

that maps δ_x to $f(x)$. ⌟

Proof: It suffices to verify continuity: for any seminorm ρ, by convexity,

$$\rho(\int_\mu f) \leq (\mu, \rho(f)),$$

thus for $\mu \in U$ satisfying $(\mu, \rho(f)) < 1$, $\rho(\int_\mu f) < 1$. This proves continuity. □

Prop. (11.8.3.25)[Vector Valued Integration Stronger]. If V is a Banach space and μ is a Radon measure on a locally compact Hausdorff space X. If $g \in L^1(\mu)$ and $H : X \to V$ is bounded and continuous, then $\int gH d\mu$ exists and belongs to the closed linear span of the range of H, and

$$||\int gH d\mu|| \leq \sup_{x \in X} ||H(x)|| \int |g(x)| \mu(x)$$

⌟

Proof: Clearly $\varphi(gH) \in L^1(\mu)$ for all $\varphi \in V^*$. And μ is Radon, so there is a sequence $\{g_n\} \in C_c(X)$ that converges to g in L^1, so $\int g_n H d\mu$ is integrable by(11.8.3.21), and

$$\int ||g_n(x)H(x) - g_m(x)H(x)dx||d\mu(x) \leq \int |g_n(x) - g_m(x)|d\mu(x) \to 0$$

thus this is a Cauchy sequence, converging to some y. Now for any $\varphi \in V^*$,

$$\varphi(y) = \lim \varphi(\int g_n H d\mu(x)) = \lim \int \varphi \circ (g_n H)d\mu = \int \varphi \circ (gH)d\mu$$

The last equality uses boundedness again.

Moreover, each $\int g_n H d\mu$ belongs to the closed range of H by(11.8.3.21), hence so does $\int gHd\mu$. And last assertion is also from(11.8.3.21). □

Holomorphic Functions

Def. (11.8.3.26) [Holomorphic Functions]. Let Ω be an open set in $\mathbb{C}$, and X be a TVS over $\mathbb{C}$, then A function $f : \Omega \to X$ is called:

- **weakly holomorphic** if Λf is holomorphic for any $\Lambda \in X^*$.
- **strongly holomorphic** if $\lim_{w\to z} \frac{f(w)-f(z)}{w-z}$ exists for every $z \in \Omega$.

A strongly holomorphic function is clearly weakly holomorphic, and the converse is true when X is Fréchet space, by the following proposition(11.8.3.27). ⌟

Prop. (11.8.3.27)[Weak and Strong Holomorphic]. Let Ω be an open set in $\mathbb{C}$, and X be a Fréchet space over $\mathbb{C}$, then f is strongly continuous, and the Cauchy integral formula(11.4.2.6) holds for f, and f is strongly holomorphic. ⌟

Proof: We may assume $0 \in \Omega$, then Let $B(0, 2r) \subset \Omega$ and Γ the boundary of $B(0, 2r)$, since Λf is holomorphic,

$$\frac{(\Lambda f)(z) - (\Lambda f)(0)}{z} = \frac{1}{2\pi i}\int_\Gamma \frac{(\Lambda f)(\zeta)}{(\zeta - z)\zeta}d\zeta \quad 0 < |z| < 2r.$$

Therefore $\{\frac{f(z)-f(0)}{z}|0 < |z| \leq r\}$ is weakly bounded, so it is also bounded by(11.8.3.12), so f is strongly continuous.

The integral exists by(11.8.3.21), so f satisfies Cauchy integral formula because it satisfies this when acting with any functional Λ, and X^* separate points.

For the last assertion, Cf.[Rudin P84]. □

Prop. (11.8.3.28) [Liouville's Theorem]. If X is a TVS over $\mathbb{C}$ on which X^* separate points and $f : \mathbb{C} \to X$ is weakly holomorphic and $f(\mathbb{C})$ is weakly bounded, then f is constant. ⌟

Proof: Immediate from Liouville's theorem(11.4.2.10). □

4 Duality Theory

Prop. (11.8.4.1)[Banach-Alaoglu]. For a nbhd V of 0 in a TVS X, the set

$$K = \{f|\ |fx| \leq 1,\ \forall x \in V\}$$

is weak*-compact in X^*, which is called the **polar** V^* of V. ⌟

Proof: Consider the Minkowski function γ of V, then for each $\Lambda \in K$, $|\Lambda x| \leq \gamma(x)$. If we consider the space $P = \prod_{x \in X}[-\gamma(x), \gamma(x)]$, then P is compact by Tychonoff(4.4.2.5).

The point is that the weak*-topology coincides with the pointwise convergence topology on K, because they have the same generating subbasis. If we show K is a closed subspace of P, this will finish the proof that K is weak*-compact. For this, consider any f_0 in its closure, then for each $x, y \in X$, $\alpha, \beta \in K$, there is a $f \in K$ that is close to f_0 at x, y and $\alpha x + \beta y$. So f_0 is linear. Similarly we can show $|f_0(x)| \leq 1$ for $x \in V$, so $f_0 \in K$. □

Prop. (11.8.4.2). If X is a TVS that X^* separate points(e.g. locally convex), then the weak topology X_w is a locally convex space, and $(X_w)^* = X^*$. ⌟

Proof: If Λ is a functional that is continuous in X_w-topology, then $|\lambda x| < 1$ for some set defined by elements in X^*, so by(11.7.3.3), $\Lambda = \sum \alpha_i \Lambda_i$ which is continuous w.r.t the original topology. □

Prop. (11.8.4.3) [Hahn Weak Topology case]. If X is a TVS that X^* separate points, then if A, B are disjoint nonempty, compact convex sets in X, then there is a $\Lambda \in X^*$ that separate A and B, i.e. $\operatorname{Re} f(E_1) < \gamma_1 < \gamma_2 < \operatorname{Re} f(E_2)$. ⌟

Proof: Let X_w be X with the weak topology, then the sets A and B are compact in X_w as it's weaker. And they are also closed because X_w is Hausdorff. X_w is convex, so we can use geometric Hahn(11.8.3.7). Now $(X_w)^* = X^*$, so the chosen functional is also continuous in the original topology. □

Prop. (11.8.4.4) [Dual Banach Space]. For a normed space X, $x \in X$ can be seen as functional on X^*, of norm exactly $||x||$. And the closed ball B^* of the dual space X^* is weak*-compact. ⌟

Proof: The first assertion is because of(11.8.3.6), the last assertion is because of Banach-Alaoglu(11.8.4.1). □

Prop. (11.8.4.5) [Adjoint Norm]. For X, Y normed, the adjoint of $T : X \to Y$ satisfies $||T^*|| = ||T||$. ⌟

Proof: Use(11.8.4.4), $||T|| = \sup\{|\langle Tx, y^*\rangle| ||x|| \leq 1, ||y^*|| \leq 1\} = ||T^*||$. □

Prop. (11.8.4.6) [Closed Range Theorem]. Let T be continuous mapping between Banach spaces X and Y, let U, V be open balls of X, Y particularly. then the following are equivalent:

1. $||T^*y^*|| \geq \delta ||y^*||$ for some δ.
2. $\delta V \subset \overline{T(U)}$.
3. $\delta V \subset T(U)$, i.e. T^{-1} is continuous.
4. $T(X) = Y$.
5. T^* is one-to-one and $R(T^*)$ is closed in X.

⌟

Proof: $1 \to 2$: If $||T^*y^*|| \geq \delta ||y^*||$, first prove $\delta V \subset \overline{T(U)}$. If $y_0 \notin \overline{T(U)}$, since $\overline{T(U)}$ is convex closed and balanced, geometric Hahn shows that there is a y^* that $|y^*(y)| \leq 1$ for every $y \in T(U)$, and $|y^*(y_0)| > 1$. Then if follows $||T^*y^*|| \leq 1$. So

$$\delta < \delta |y^*(y_0)| \leq \delta ||y_0|| ||y^*|| \leq ||y_0|| ||T^*y^*|| \leq ||y_0||$$

This shows $\delta V \subset \overline{T(U)}$.

$2 \to 3$: may assume $\delta = 1$. Then $\overline{V} \subset \overline{T(U)}$. Then for every $y \in Y$ and every $\varepsilon > 0$, there is a x that $||x|| \le ||y||$ and $||y - Tx|| < \varepsilon$. For any $y_1 \in V$, pick $\varepsilon_n > 0$ that $\sum \varepsilon_n < 1 - ||y_1||$, then choose $||x_n|| \le ||y_n||$ that $||y_n - Tx_n|| < \varepsilon_n$, and let $y_{n+1} = y_n - Tx_n$. Then is verified that $x = \sum x_n \in U$ and Tx.

$3 \to 1$: $||T^*y^*|| = \sup\{|\langle x, T^*y^*\rangle||x \in U\} \ge \sup\{|\langle y, y^*\rangle||y \in V\} = \delta||y^*||$.

$3 \iff 4$: By Open mapping theorem.

$4 \to 5$: T^* is injective by(11.7.3.2). By open mapping theorem, T^* is a multiple of a dilation, so $R(T^*)$ is closed by(4.4.8.10).

$5 \to 4$: $R(T)$ is dense in Y by(11.7.3.2), and it is closed by the proposition(11.8.4.7) below. □

Prop. (11.8.4.7) [Closed Range Theorem]. If X, Y are Banach spaces and $T \in L(X, Y)$, the following are equivalent:

1. $R(T)$ is closed in Y.
2. $R(T^*)$ is weak*-closed in X^*.
3. $R(T^*)$ is closed in X.

⌟

Proof: $1 \to 2$: As $N(T)^\perp$ is the weak*-closure of $R(T^*)$, it suffices to prove $N(T)^\perp \subset R(T^*)$. As $R(T)$ is complete, the open mapping theorem applies to $X \to R(T)$, showing that each $y \in R(T)$ corresponds to an element $x \in X$ that $Tx = y$ and $||x|| \le K||y||$.

For $x^* \in N(T)^*$, define a functional Λ on $R(T)$ by $\Lambda Tx = \langle x, x^*\rangle$, this is well-defined, and $|\Lambda y| = \Lambda Tx| \le K||y||||x^*||$. So it is continuous and by Hahan=Banach some continuous functional $y^* \in Y^*$ extends Λ. Then $\langle Tx, y^*\rangle = \Lambda Tx = \langle x, x^*\rangle$, so $x^* = T^*y^*$ is in the image of T^*, so we are done.

$3 \to 1$: let $Z = \overline{R(T)}$. RT is dense in Z, so(11.7.3.2) shows $T^* : Z^* \to X^*$ is injective. And for each $z^* \in Z*$, there is an extension y^* by Hahn-Banach, and then $\langle x, T^*y^*\rangle = \langle Tx, y^*\rangle = \langle Tx, z^*\rangle = \langle x, T^*z^*\rangle$, so $T^*(Y^*) = T^*(Z^*)$, which is closed by hypothesis.

Now use open mapping theorem for $Z^* \to R(T^*)$, then there is a c that $c||z^*|| \le ||T^*z^*||$. So $T : X \to Z$ is surjective, by(11.8.4.6). So $R(T) = Z$ is closed. □

Prop. (11.8.4.8). In a normed space, iff $x_n \to x$ weakly, then $\underline{\lim}||x_n|| \ge ||x||$. ⌟

Proof: Choose a functional that $||f|| = 1$ and $|f(x)| = 1$ by(11.8.3.6), then use the definition of weak convergence. □

Prop. (11.8.4.9) [Eberlein-Smulian]. For a set A in a Banach space X, A is weak*-sequentially compact iff its weak precompact. ⌟

Proof: **?**

We prove here that the case that the closed unit ball of a reflexive Banach space is weakly*-self sequentially compact.

To prove this, first we show that a bounded sequence has a subsequence that is weak*-convergent in X. Let $X_0 = \overline{\text{span}\{x_n\}}$, then X_0 is reflexive by(11.8.4.13), and it is separable, so X_0^* is separable by(11.8.4.11). Then the result follows from(11.8.4.14).

Finally, the weak limit x is in the closed unit ball, by(11.8.4.8). □

Reflexive and Separable

Def. (11.8.4.10)[Reflective Banach Space]. If X is a Banach space, there is an isometric immersion of X onto a closed subspace of X^{**}(closed because X is complete). X is called **reflexive** iff $X \cong X^{**}$. ⌟

Prop. (11.8.4.11) [Separability Banach]. For a normed space X, if X^* is separable, then X is separable. ⌟

Proof: Choose a countable dense set in X^*, then their projection to the unit sphere S^* $\{g_n\}$ are dense in S^*(easily checked), and choose for each of them a x_n that $||x_n|| = 1$ and $g_n(x_n) > \frac{1}{2}$.

Now I claim x_n are dense in X, i.e. $X_0 = \overline{\text{span}\{x_n\}} = X$. If this is not the case, then there is a $||x|| = 1$ not in X_0, so by(11.8.3.6), there is a f that $f(X_0) = 0$ and $||f|| = 1$ and $f(x) = 1$. Then $||g_n - f|| = \sup_{||x||=1}\{|g_n(x) - f(x)|\} \geq |g_n(x_n) - f(x_n)| = |g_n(x_n)| \geq 1/2$, contradicting the fact g_n is dense in S^*. □

Prop. (11.8.4.12) [Duality Exact]. If X is a closed subspace of a normed space Y, and Y/X is the quotient field, then $(Y/X)^*$ is a closed subspace of Y^*, and X^* is the quotient. ⌟

Proof: $(Y/X)^* \to Y^*$ is clearly injective, and the X^* are all functionals on Y modulo the functionals that vanish on X. □

Cor. (11.8.4.13) [Pettis]. Closed subspace and quotient space of a reflexive normed space is reflexive. ⌟

Proof: Use the fact that $0 \to X \to Y \to Z \to 0$ induces an exact sequence $0 \to X^{**} \to Y^{**} \to Z^{**} \to 0$, and there is a map $X \to X^{**}$, so we can use snake lemma(as modules). □

Prop. (11.8.4.14) [Separable Ball Weak*-Sequentially Compact]. If a normed space X is separable, then the closed unit ball of X^* is weak*-sequentially compact. ⌟

Proof: Let x_n be a countable dense subset of X, then by diagonal method, for each bounded sequence of $f_n \in X^*$, there is a subsequence f_{n_k} that $f_{n_k}(x_m)$ converges for each x_m. Then by(11.7.2.3), f_{n_k} converges to some $f \in X^*$. So the theorem is finished. □

Prop. (11.8.4.15) [Reflexive Ball Weak*-Sequentially Compact]. In a reflexive Banach space X, then a set in X is bounded iff it is weak*-sequentially compact. ⌟

Proof: If it is reflexive, then the unit ball is weak*-compact by Alaoglu, so it is weak*-sequentially compact by Eberlein(11.8.4.9). Conversely, if it is weak*-sequentially compact, then its closure is weak*-compact, thus bounded. □

Prop. (11.8.4.16). A closed convex set of a reflexive Banach space attains minimal norm. ⌟

Proof: By Hahn, a closed convex set is weakly closed. let $d = \inf\{||x||\}$, then if $d \leq ||x_n|| < d+q/n$, then $\{x_n\}$ is bounded, so by(11.8.4.15) it is weak-sequencially compact(11.8.4.9), thus some $x_n \to x$ weakly. and use(11.8.4.8), x must attains minimal norm d. □

5 Compact Operators & Fredholm Operators

Def. (11.8.5.1) [Compact Operators]. A **compact operator** is an operator between Banach spaces that maps bounded set to sequentially compact(equivalently precompact or totally bounded(4.4.8.7)) set. It is necessarily continuous because the norm function is continuous thus $||Tx||$ is bounded on the unit ball. The set of compact operators between X, Y is denoted by $\mathfrak{C}(X, Y)$. ⌟

Prop. (11.8.5.2) [Examples of Compact Operators].

- Let X be a compact measure space and $Lu(x) = \int_X K(x,y)u(y)\mathrm{d}y$ for $K \in C(X \times X)$. This is a compact operator on $C(X)$ by Arzela-Ascoli.
- Let Ω be a σ-finite measure space and let $\mathcal{L}u(x) = \int_\Omega K(x,y)u(y)\mathrm{d}y$ for $K(x,y) \in L^2(\Omega \times \Omega)$. This is a compact operator on $L^2(\Omega)$, as it is Hilbert-Schmidt(11.9.5.5)(11.9.5.3).

⌟

Prop. (11.8.5.3) [Properties of Compact Operators].

1. For a continuous operator, it has f.d. image iff it is compact and the image is closed.
2. The space of compact operator is a closed subspace of $L(X, Y)$. Thus the limit of f.d. operators is compact.
3. If one of A or B is compact and the other is continuous, then AB is compact, because continuous maps bounded to bounded and compact to compact.

⌟

Proof:

1. A finite dimensional space is closed by(11.8.1.8), and a finite dimensional space is Heine-Borel(4.4.5.2), so it maps closed ball to precompact set, as it is continuous. Conversely, if it is compact and the image is closed, then it is an open map to its image, by open mapping theorem, and the image is locally compact because T is compact, so it has finite dimension(11.8.1.7).
2. $S+T$ is continuous because sum of precompact set is precompact. To show it is closed subspace, Use totally bounded definition, for T is the closure, let $||S-T|| < r$, then if $S(x_i)$ is a r-net for $S(B(0,1))$, then $T(x_i)$ is a $3r$-net for $T(B(0,1))$.
3. Because continuous function preserves both boundedness and (pre)compactness.

□

Prop. (11.8.5.4) [Compact Operators and Totally Convergence]. Let $x_n \to x$ weakly, if T is compact, then $Tx_n \to T_n x$ strongly. The converse is true when X is reflexive. In particular, this applies to Hilbert space. ⌟

Proof: Assume the contrary, if Tx_n doesn't converge to Tx, there is a subsequence x_{n_k} that $||Tx_{n_k} - Tx|| \geq \varepsilon_0$. Now $\{x_n\}$ is bounded by(11.7.3.5), so by T compact, there is a subsubsequence $Tx_{n_k} \to z$ strongly. But because $x_{n_i} \to x$ weakly, $Tx_{n_i} \to Tx$ weakly because T is continuous, and thus $z = Tx$.

The converse is by Eberlein(11.8.4.9), because the bounded x_n has a weak convergent subsequence, and it is mapped to convergent sequence by T. □

Prop. (11.8.5.5). T is compact $\iff$ T^* is compact. ⌟

Proof: We need only to show that $T^* y_n^*$ has a uniformly convergent subsequence on the unit sphere, but for this it suffice to prove y_n^* is sequentially compact in $C(\overline{T(B(0,1))})$. And we use Arzela-Ascoli because $\overline{T(B(0,1))}$ is compact. For the other half, use the double dual space. □

Lemma (11.8.5.6). If there is a chain of closed subspaces $M_1 \subset M_2 \subset \ldots$ that $T(M_n) = M_n$ and $(T - \lambda_n I)M_n \subset M_{n-1}$ for some $\lambda_n \in \sigma(A) - B(0,r)$, then T is not compact. ⌟

Proof: There are $y_n \in M_n$ that $||y_n|| \leq 1$ and $||y_n - x_n|| \geq 1/2$ for $x \in M_{n-1}$, so if $m < n$, $||Ty_m - Ty_n|| = ||\lambda y_n - (Ty_m - (T-\lambda_n)y_n)|| \geq \frac{|\lambda_n|}{2} \geq \frac{r}{2}$, so Ty_n has no convergent subsequence. □

Lemma (11.8.5.7). If A is compact and $T = 1 - A$, then if T is not injective, then it is not surjective. And for any $r > 0$, $\sigma_p(A) - B(0,r)$ is a finite set. ⌟

Proof: We use(11.8.5.6). If $R(T) = X$, then let $M_n = N(T^n)$, then $M_0 \neq 0$ because there is a $Tx_0 = 0$, and $M_n \subset M_{n+1}$ because there is a $T^n x_{n+1} = x_0$, so $x_{n+1} \in M_{n+1} - M_n$.

If $\sigma_p(A) - B(0,r)$ is infinite, then choose M_n to be generated by n eigenvectors, then it is clear that a chain like above will be found. □

Lemma (11.8.5.8). If A is compact and $T = 1 - A$, then $R(T)$ is closed. ⌟

Proof: it suffices to show $T^{-1} : R(T) \to X/N(T)$ is continuous, if this is not the case, then there is a sequence $||x_n|| = 1$ but $Tx_n \to 0$. But A is compact, so there is a subsequence that $Ax_{n_k} \to z$, so $x_{n_k} \to z$. So $Tz = 0$ so $z = 0$, but then $x_{n_k} \to 0$, contradiction. □

Prop. (11.8.5.9) [Riesz-Fredholm]. For a compact operator $A \in L(X)$, let $T = I - A$. Then:

1. $0 \in \sigma(A)$ if X is not f.d.
2. T is Fredholm of index 0(11.8.5.17). Equivalently, $\sigma(A)\backslash\{0\} = \sigma_p(A)\backslash\{0\}$(because either T not injective or T is surjective).
3. $\sigma(A)$ has at most one convergent point 0 (it must attain 0 if X is a infinite-dimensional). Hence it has at most countable spectrum.

⌟

Proof: 1: If 0 is a regular value, then T is invertible, thus $T^{-1}T = \mathrm{id}$ is compact, thus X has f.d.(11.8.1.7).

2 : Firstly $\dim N(T) < \infty$. This is because $T|_{N(T)} = \mathrm{id}_{N(T)}$, so it is compact iff it is f.d.(11.8.5.3). by [Rudin P108]**?**.

3: By(11.8.5.7). □

Prop. (11.8.5.10) [Lomonosov's Invariant Subspace Theorem]. If X is an infinite dimensional complex Banach space, and $T \neq 0$ is a compact operator in $L(X)$, then there is a proper closed subspace M of X that is invariant under S for any S that commutes with T.

In particular, if S commutes with some compact operator T, then S has an invariant closed subspace. ⌟

Proof: If Γ is the subspace of all operators that commutes with T, then it is a subalgebra of $L(X)$, and for each $y \in X$, let $\Gamma(y) = \{Sy | S \in \Gamma\}$, then $S(\Gamma(y)) \subset \Gamma(y)$, then so does the closure of $\Gamma(y)$. So if the proposition is false, then $\Gamma(y)$ is dense in X for each y.

Pick x_0 that $Tx_0 \neq 0$, then there is an open ball B of x_0 that $||Tx|| \geq \frac{1}{2}||Tx_0||$ and $||x|| \geq \frac{1}{2}||x_0||$ for $x \in B$. Now our assumption shows that for every $y \neq 0$, there is a nbhd W of it that maps into B by some $S \in \Gamma$(notice Γ is a subspace).

Now $K = \overline{T(B)}$ is compact because T is compact, so there are f.m. open sets W_i whose union cover K, and $S_i(W_i) \in B$, where $S_i \in \Gamma$. Now let $\mu = \max\{||S_i||\}$. Consider $Tx_0 \in K$, so there is a $S_{i_1}Tx_0 \in B$, then $TS_{i_1}Tx_0 \in K$, so there is a $S_{i_2}TS_{i_1}Tx_0 \in B$. Continuing this way, we get

$$\frac{1}{2}||x_0|| \leq ||x_N|| \leq \mu^N ||T^N|| ||x0||,$$

so by Gelfand theorem(11.9.1.8), $\rho(T) > 0$, so there is a eigenvalue λ of T(by(11.8.5.9)) that $N(T-\lambda I)$ is finite dimensional, so not equal to X, and it is clearly invariant under Γ. □

Prop. (11.8.5.11) [Jordan Decomposition for Compact Operators]. For a compact operator A and all the non-zero eigenvalues λ_i, we can find a subspace

$$\bigoplus_{i=1}^{\infty} N((\lambda_i - A)^{p_i}), \quad \lambda_i \neq 0$$

on which A has a Jordan form. ⌟

Proof: Let $T = 1 - A$, By(3.2.4.5), we only have to prove there are some m, n that There is a p that $N(T^p) = N(T^{p+1})$ and a q that $R(T^q) = R(T^{q+1})$, because then we have a decomposition $X = N((T-\lambda I)^p) \oplus R((T-\lambda I)^p)$, and all these $N((T-\lambda I)^p)$ are pairwisely disjoint.

Now $q < \infty$, because if $R(T) \supset R(T^2) \supset \ldots$, because T^k is of the form $1+$ compact operator, $R(T^k)$ are all closed by(11.8.5.8), so by(11.8.5.6), this is impossible.

For p, use Riesz-Fredholm(11.8.5.9),

$$\dim N(T^q) = \mathrm{codim} R(T^q) = \mathrm{codim} R(T^{q+1}) = \dim N(T^{q+1}) < \infty$$

So $p \leq q < \infty$. □

Prop. (11.8.5.12). If X, Y are Banach spaces and $T, K \in L(X, Y)$, K is compact and $R(A) \subset R(K)$, then A is compact. ⌟

Proof: Use(11.7.2.10), then we can lift the function to a map $\widetilde{T} : X \to X/N(K)$, which is also continuous, so $T = \widetilde{K} \to \widetilde{T}$ is also compact. □

Schauder Basis

Def. (11.8.5.13) [Schauder Basis]. Let X be a Banach space, a sequence e_n is called a **Schauder basis** iff for any $x \in X$, there is a unique sequence $C_n(x)$ that $x = \lim \sum_{n=1}^{N} C_n(x) e_n$. Notice in this case X is automatically separable. ⌟

Prop. (11.8.5.14). If X has a Schauder basis, then $C_n(x)$ are continuous functional on X. ⌟

Proof: Consider the module $||x||_1 = \sup ||S_N x||$, Firstly, it is complete, because $||x|| = \lim ||S_N x|| \leq ||x||_1$, so if there is a Cauchy sequence $\{x_i\}$ in $|\cdot|_1$, then it is a Cauchy sequence in $|\cdot|$, then it converges to some x. Now $C_N(x) = S_N(x_i) - S_{N-1}(x_i)$ are all Cauchy sequence, uniform in N, so they converges to some sequence c_N.

It is left to verify that $s_N = \sum_{i=1}^{N} c_n e_n$ converges to x, because then it is easy to verify that $\lim ||x_i - x||_1 = 0$. For this, choose N_1 large that $||x_n - x|| \leq \varepsilon$ for $n \geq N_1$, and choose N_2 large that $||S_k(x_n) - s_k|| \leq \varepsilon$ for all k and $n \geq N_2$. Then for $x_{N_1+N_2}$, there is a N_3 that $||S_n x_{N_1+N_2} - x_{N_1+N_2}|| \leq \varepsilon$, so $||x - s_k|| \leq ||x - x_{N_1+N_2}|| + ||S_k x_{N_1+N_2} - x_{N_1+N_2}|| + ||S_k(x_{N_1+N_2}) - s_k|| \leq 3\varepsilon$ for k large.

Now by Banach(11.7.2.7), $||x||_1 \leq M||x||$ for some M, so $|C_n(x)e_n| \leq 2M||x||$ and C_n is continuous. □

Prop. (11.8.5.15). If X has a Schauder basis, then any compact operator is a limit of operators of f.d. range. ⌟

Proof: Let $S_N(x)=\sum_{n=1}^N C_n(x)e_n$, it is continuous by(11.8.5.14). And it converges, so $||S_N||\leq M$, by Banach-Steinhaus(11.7.2.1).

For any compact operator, we want to find f.d. range operator T_i that $T_i\to T$. For this, given any $\varepsilon>0$, because $\overline{T(B(0,1))}$ is compact, there are operators that is a ε/M^2-net y_i, then choose N large enough that $|S_Ny_i-y_i|\leq\varepsilon/M^2$, then for any x, there is a y_i that $|Tx_i-y_i|<\varepsilon/M^2$, so $|S_NTx_i-S_Ny_i|<\varepsilon/M$, and then $|S_NTx-Tx_i|<\varepsilon$, and notice S_NT has f.d. range. □

Prop. (11.8.5.16) [Compact Operator as Limits of F.D. Operators]. Any compact operator on a Hilbert space is a limit of f.d. operators. ⌟

Proof: Cf.[Trace Classes and Hilbert-Schmidt Operators, Thm10]. □

Fredholm Operator

Def. (11.8.5.17) [Fredholm Operator]. A bounded operator between Banach space is called a **Fredholm operator** if $\dim N(T)<\infty$ and $\mathrm{codim}R(T)<\infty$. It necessarily has closed image by(11.7.2.11), so $R(T)=N(T^*)^\perp$(11.7.3.2).

The **index** of a Fredholm operator is defined as $\mathrm{ind}(T)=\dim N(T)-\mathrm{codim}R(T)$, thus for a compact operator A, $I-A$ has index 0, by(11.8.5.9). ⌟

Prop. (11.8.5.18). For a Fredholm operator between Banach space, we have

$$X=N(T)\oplus R(T)\quad Y=Y/R(T)\oplus R(T)$$

and $X/N(T)\cong R(T)$. ⌟

Proof: Because $R(T)$ and $N(T)$ are finite/cofinite hence closed and complemented by(11.8.1.9). If $X=N(T)\oplus M_1$ and $Y=R(T)\oplus M_2$, then $M_1\cong X/N(T)$, $X/N(T)\cong R(T)$ and $M_2\cong Y/R(T)$ by Banach theorem. □

Prop. (11.8.5.19) [Characterizating Fredholm Operator]. T is Fredholm from X to Y iff there exist a bounded S_1,S_2 from Y to X that $S_1T=I-A_1,TS_2=I-A_2$, where A_1,A_2 is compact. If this is the case, S_1 and S_2 can be chosen the same as S, then S is called the **regulator** of T, and S is Fredholm as well.

So the Fredholm operator is the set of operators invertible 'modulo compact ones'. ⌟

Proof: By(11.8.5.18) $T:X/N(T)\cong R(T)$, and there is a projection of $\pi:Y$ onto $R(T)$. Thus we composed them to get a $S=T^{-1}\circ\pi:Y\to X$. And ST and TS are both 1 minus a projection with f.d. image, hence compact(11.8.5.3).

For the converse, $R(T)\supset R(1-A_2)$ is of finite codimention because $1-A_2$ is Fredholm, and $N(T)\subset N(1-A_1)$ is of finite dimension because $1-A_1$ is Fredholm. □

Cor. (11.8.5.20). The set of Fredholm operators is closed under composition. Index is a locally constant function on it, and $\mathrm{ind}(T_1T_2)=\mathrm{ind}(T_1)+\mathrm{Ind}(T_2)$. ⌟

Proof: There is a long exact sequence(use(4.8.7.4) in the category of vector spaces)

$$0\to\ker T_2\to\ker T_1T_2\to\ker T_2\to\mathrm{Coker}\,T_2\to\mathrm{Coker}\,T_1T_2\to\mathrm{Coker}\,T_1\to 0.$$

which shows the composition and index is additive.

For the openness and locally constancy, use(11.8.5.19), when adding a small R, $S(T+R) = 1-A_1+SR$, and if when $||R|| < ||S||^{-1}$, $E_1 = (I+RS)^{-1}$ is bounded, so $E_1S(T+R) = I-E_1A_1$, and similarly does $(T+R)SE_2$, so $T+R$ is Fredholm. And $\operatorname{ind} E_1+\operatorname{ind} S+\operatorname{ind}(T+R) = \operatorname{ind}(1-E_1A_1) = 0$, and $\operatorname{ind} E_1 = 0$ because it is invertible, and $\operatorname{ind} S + \operatorname{ind} T = \operatorname{ind}(1-A_1) = 0$, so $\operatorname{ind} T = \operatorname{ind}(T+R)$. □

Cor. (11.8.5.21). If T is Fredholm and A is compact, then $T+A$ is Fredholm, and $\operatorname{ind}(T+A) = \operatorname{ind} T$, so ind is in fact defined on the quotient of $L(X,Y)$ by compact operators. ⌟

Proof: It is Fredholm by(11.8.5.19), and we notice $S(T+A)$ and ST are both 1 minus compact operators, thus(11.8.5.20) and(11.8.5.9) gives the result. □

Cor. (11.8.5.22). If T is Fredholm, then T^* is Fredholm, and $\operatorname{ind}(T^*) = -\operatorname{ind}(T)$. ⌟

Proof: The first follows from(11.8.5.19) and(11.8.5.5). For the second, use the fact $R(T)$ and $N(T)$ are all closed. □

6 Unbounded Operators

11.9 Archimedean Banach Algebra

References are [Rud91].

Notation (11.9.0.1).
- Use notations defined in Archimedean Functional Analysis.
- Every Banach space in this section is assumed to be defined over $\mathbb{C}$.

⌟

1 Banach Algebras

Def. (11.9.1.1) [Spectrums]. Suppose X is Banach space and $A \in L(X)$. Then $\lambda \in \mathbb{C}$ is called a:
- **point spectrum** if $\lambda I - A$ is not injective;
- **continuous spectrum** if it is not a point spectrum and $R(\lambda I - A) \neq X$ but $\overline{R(\lambda I - A)} = X$.
- **residue point** if it is not a point spectrum and $\overline{R(\lambda I - A)} \neq X$.
- **regular point** if $\lambda I - A$ is injective and $R(\lambda I - A) = X$, in which case $(\lambda I - X)^{-1}$ is continuous, by Banach.

denote $\sigma(A) = K \setminus \{\text{regular points of } A\}$ the **spectrum** of A, and $\rho(A) = \sup\{|\lambda||\lambda \in \sigma A\}$ is called the **spectral radius** of A. ⌟

Prop. (11.9.1.2). If A is a Banach algebra and x is invertible in A, and $h \in A$ satisfies $||h|| < \frac{1}{2}||x^{-1}||^{-1}$, then $x + h$ is also invertible and

$$||(x + h)^{-1} - x^{-1} + x^{-1}hx^{-1}|| \leq 2||x^{-1}||^3||h||^2$$

⌟

Proof: $x + h = x(e + x^{-1}h)$ and $||x^{-1}h|| < \frac{1}{2}$, so $x + h$ is invertible by(11.9.1.14), and $||(x + h)^{-1} - x^{-1} + x^{-1}hx^{-1}|| = ||[(e + x^{-1}h)^{-1} - e + x^{-1}h]x^{-1}|| \leq 2||x^{-1}||^3||h||^2$ also by(11.9.1.14). □

Cor. (11.9.1.3). If A is a Banach algebra, then the invertible elements $G(A)$ is an open subset of A, and the mapping $x \mapsto x^{-1}$ is a homeomorphism of $G(A)$ onto $G(A)$. ⌟

Prop. (11.9.1.4). For $T \in L(X)$ where X is Banach space, $\mathbb{C}\backslash\sigma(T)$ is an open set and $\lambda \to (\lambda I - T)^{-1}$ is a holomorphic function on $\mathbb{C}\backslash\sigma(T)$.

In particular, $\underline{\sigma(T) \text{ is not empty}}$. ⌟

Proof: The first assertion is by(11.9.1.3), for the second, let $f(\lambda) = (\lambda e - x)^{-1}$ is defined on $\Omega = \mathbb{C} - \sigma(x)$ and(11.9.1.2) shows

$$||f(\mu) - f(\lambda) + (\mu - \lambda)f^2(\lambda)|| \leq 2||f(\lambda)||^3|\mu - \lambda|^2$$

so $\lim_{\mu\to\lambda} \frac{f(\mu)-f(\lambda)}{\mu-\lambda} = -f^2(\lambda)$, which means that f is strongly holomorphic in Ω.

Now if $|\lambda| > ||x||$, then $|f(\lambda)| = |\lambda^{-1}e + \lambda^{-2}x + \ldots| \leq \frac{1}{|\lambda|-||x||}$, so $\sigma(x)$ cannot be empty by Liouville theorem(11.8.3.28). □

Cor. (11.9.1.5) [Gelfand-Mazur]. If A is a Banach algebra over $\mathbb{C}$ and $A^\times = A^*$, then $A = \mathbb{C}$ ⌟

Proof: Any nonzero element x has a nonempty spectrum, so there is a $\lambda(x)$ that $x-\lambda(x)e$ is not invertible, so it must be 0. That is, the mapping $\mathbb{C}\to A:\lambda\mapsto\lambda e$ is bijective, so is is isomorphism by Banach. □

Prop. (11.9.1.6). Notice $(I-T)$ is invertible for $||T||<1$ and the inverse can be calculated by definition.

In particular, for a Banach algebra A and any $x\in A$, when $\lambda>||x||$, $e-\lambda^{-1}x$ is invertible, so the spectrum of x is bounded. Now that its complement is open as the inverse image of $G(A)$ by $\lambda\mapsto\lambda e-x$, so the spectrum of x is compact. ⌟

Cor. (11.9.1.7) [Spectrum is Continuous]. The spectrum of an element of a Banach algebra is continuous, i.e. if $\sigma(x)\subset\Omega$ for some open subset $\Omega\subset\mathbb{C}$, then there is a $\delta>0$ that $\sigma(x+y)\subset\Omega$ for $||y||<\delta$. ⌟

Proof: As $||(\lambda e-x)^{-1}||$ is a continuous function of λ in the complement of σ, and since the norm tends to 0 as $\lambda\to\infty$, there is a M that $||(\lambda e-x)^{-1}||<M$ for all $\lambda\notin\Omega$. Now if $||y||<1/M$ and $\lambda\notin\Omega$, then $\lambda e-(x+y)=(\lambda e-x)[e-(\lambda e-x)^{-1}y]$ is invertible. □

Prop. (11.9.1.8) [Gelfand]. The spectrum radius $\rho(A)=\lim_{n\to\infty}||A^n||^{\frac{1}{n}}=\inf||A^n||^{\frac{1}{n}}\le||A||$.

This formula is remarkable, as the LHS depends only on the algebraic structure, and the RHS depends on the metric structure. ⌟

Proof: For $r>\rho(x)$
$$x^n=\frac{1}{2\pi i}\int_{\Gamma_r}\lambda^n f(\lambda)d\lambda.$$
Let $M(r)=\max||f(re^{i\theta})||$, then $||x^n||\le r^{n+1}M(r)$, hence $\limsup||x^n||^{1/n}\le r$, so $\limsup||x^n||^{1/n}\le\rho(x)$.

For the converse, if $\lambda\in\sigma(x)$, then $\lambda^n\in\sigma(x^n)$, because $\lambda^n e-x^n=(\lambda e-x)(\lambda^{n-1}e+\ldots+x^{n-1})$, and this two commutes. So $|\lambda^n|\le||x^n||$, so $\rho(x)\le\inf||x^n||^{1/n}$. □

Prop. (11.9.1.9). $\sigma(A)=\sigma(A^*)$. ⌟

Proof: It suffices to show if T is invertible iff T^* is invertible. If T is invertible, then T^* is invertible with inverse $(T^{-1})^*$. Conversely, if T^* is invertible, then T^{**} is invertible, so, as the restriction of T^{**}, T is injective and image is closed. If the image is not X, then there is a f that vanish on the image, so $T^*f=0$, but then $f=0$. □

Prop. (11.9.1.10). In a Banach algebra A, $e-xy$ is invertible iff $e-yx$ is invertible, thus $\sigma(xy)\cup\{0\}=\sigma(yx)\cup\{0\}$. ⌟

Proof: Let $z=(e-xy)^{-1}$, then we claim $e+yzx$ is just the inverse of $e-yx$: $(e-yx)(e+yzx)=e-yx+yzx-yxyzx=e$ and $(e+yzx)(e-yx)=e+yzx-yx-yzxyx=e$. □

Lemma (11.9.1.11). If A is a Banach algebra and $x_n\in G(A)$ converges to $x\notin G(A)$, then $||x_n^{-1}||\to\infty$. ⌟

Proof: If $||x_n^{-1}||<M$, choose n that $||x_n-x||<1/M$, then $||e-x_n^{-1}x||=||x_n^{-1}(x_n-x)||<1$, so $x_n^{-1}x$ is invertible, so x is invertible. □

Prop. (11.9.1.12). For Banach algebra B and its closed subalgebra A, $\sigma_A(x)$ is obtained from $\sigma_B(x)$ by filling some holes. So when $\sigma_B(x)$ doesn't separate $\overline{\mathbb{C}}$ or $\sigma(A)$ has empty interior, then $\sigma_A(x)=\sigma_B(x)$. ⌟

Proof: Cf.[Rudin P256]. □

Prop. (11.9.1.13). if A is a Banach algebra over $\mathbb{C}$ that $||x||||y|| \leq M||xy||$ for some fixed M, then A is isomorphic to $\mathbb{C}$. ⌟

Proof: If y is a boundary pt of $G(A)$, $y = \lim y_n$, then $||y_n^{-1}|| \to \infty$. But $||y_n||||y_n^{-1}|| \leq M||e||$, so $y_n \to 0$, so $y = 0$.

But any boundary point of $\sigma(x)$ gives a boundary point $\lambda e - x$ of $G(A)$, so $x = \lambda e$, so $A \cong \mathbb{C}$. □

Complex Homomorphism

Prop. (11.9.1.14). Suppose A is a Banach algebra over $\mathbb{C}$, $x \in A$ satisfies $||x|| < 1$, then $||(e-x)^{-1} - e - x|| \leq \frac{||x||^2}{1-||x||}$, and $|\varphi(x)| < 1$ for any complex homomorphism φ on A. In particular, any complex homomorphism is continuous. ⌟

Proof: $||(e-x)^{-1} - e - x|| = ||x^2 + x^3 + \ldots|| \leq \sum_{n=2}^{\infty} ||x||^n = \frac{||x||^2}{1-||x||}$.

For the second, notice $e - \lambda^{-1}x$ is invertible for each $|\lambda| \geq 1$, so $1 - \lambda\varphi(x) \neq 0$, so $\varphi(x) \neq \lambda$. □

Prop. (11.9.1.15)[Gleason-Kahane-Zelazko]. If φ is a linear functional on a Banach algebra A over $\mathbb{C}$, if $\varphi(e) = 1$ and $\varphi(x) \neq 0$ for every invertible element $x \in A$, then φ is a complex homomorphism. ⌟

Proof: Cf.[Rudin P251]. □

Symbolic Calculus

Prop. (11.9.1.16)[Symbolic Calculus]. For a Banach algebra A. For a domain Ω in $\mathbb{C}$, define A_Ω as the set of x that $\sigma(x) \in \Omega$, it is an open set by(11.9.1.7), then:

$$f \mapsto \tilde{f}(x) = \frac{1}{2\pi \mathrm{i}} \int_\Gamma f(\lambda)(\lambda e - x)^{-1} d\lambda$$

for any contour Γ that surrounds $\sigma(x)$, is a continuous algebra isomorphism of $H(\Omega)$ into the set of A-valued functions on A_Ω with the compact-open topology.

We have $\widetilde{g \circ f} = \tilde{g} \circ \tilde{f}$. ⌟

Proof: The nontrivial part is that this map is multiplicative, but for this we can use Runge's theorem to approximate any function on $\sigma(x)$. □

This theorem makes it possible to implant complex analysis to the study of Banach Algebra.

Cor. (11.9.1.17). $\exp(x)$ is defined on A and is continuous. If $\sigma(x)$ doesn't separate 0 from ∞, then $\log(x)$ is defined but might not be continuous. ⌟

Prop. (11.9.1.18)[Spectral Mapping Theorem]. $\tilde{f}(x)$ is invertible in A iff $f(\lambda) \neq 0$ on $\sigma(x)$. Thus we have $\sigma(\tilde{f}(x)) = f(\sigma(x))$. ⌟

Prop. (11.9.1.19). If f doesn't vanish identically on any component of Ω, then $f(\sigma_p(T)) = \sigma_p(\tilde{f}(T))$. Cf.[Rudin P266]. ⌟

Commutative Banach Algebra

Lemma (11.9.1.20). For A a commutative Banach algebra, the set of maximal ideals has codimension 1 corresponds to kernels of complex homomorphisms to $\mathbb{C}$. (Consider the quotient space and use Gelfand-Mazur). Note that a complex homomorphism is all continuous because $\lambda e - x$ maps to nonzero.

$\lambda \in \sigma(x)$ iff there is a complex homomorphism h s.t. $h(x) = \lambda$. (Because x is invertible iff it is not contained in any proper ideal of A. ⌟

Proof:

□

Prop. (11.9.1.21)[Gelfand Transform]. The **spectrum** Δ_A of a unital commutative Banach algebra A is defined to be the set Δ of maximal ideals of A. It is a locally compact Hausdorff space w.r.t to the weak*-topology and the Gelfand transform: $x \mapsto \widehat{x}(h) = h(x)$ is a continuous map of A into $C(\Delta)$. And the range of $\widehat{x}$ equals $\sigma(x)$, so $||\widehat{x}|| = \rho(x) \leq ||x||$. ⌟

Proof: First we prove it is compact Hausdorff: As $\sigma(A) = \{h \in \text{closed ball of } A^*|h(e) = 1, h(xy) = h(x)h(y)\}$ which is a closed subset of the closed ball of A^*, so it is compact Hausdorff. The rest is clear and follows from(11.9.1.20). □

Prop. (11.9.1.22). For $A = C(X)$ where X is compact Hausdorff, Δ is homeomorphic to X. (otherwise it has finite $f_i \neq 0$, then $\sum |f_i|^2$ is positive thus invertible but maps to 0). In fact, for a space X, $\Delta(C(X))$ is the stone-Čech compactification of X. ⌟

Prop. (11.9.1.23). For $A = L^\infty(m)$, the spectrum of f is just the essential range of f. ⌟

Lemma (11.9.1.24). If $\widehat{A} \subset C(\Delta)$ with a chosen topology that makes it compact, and A separate points, then the topology of it is the same of the weak*-topology. (Compact to Hausdorff). ⌟

Prop. (11.9.1.25). The algebra $L^1(\mathbb{R}^n) \oplus \delta$ with the multiplication by convolution has the spectrum $R^n \cap \{\infty\}$. (Use $(L^p)* = L^q$ and see when will it be homomorphism). ⌟

2 Hilbert spaces

Prop. (11.9.2.1)[Optimal Approximation]. A closed convex subset in a Hilbert space has a unique element that attains the minimum norm. ⌟

Proof: Assume $0 \notin C$, so let $d = \inf_{z\in C} ||z|| > 0$, then there are x_n that $d \leq ||x_n|| \leq d + 1/n$. It suffices to show that x_n is a Cauchy sequence, because then it has a convergent point in C. Now

$$||x_n - x_m||^2 = 2(||x_n||^2 + ||x_m||^2) - 4||\frac{x_n + x_m}{2}||^2 \leq 2[(d + 1/n)^2 + (d + 1/m)^2] - 4d^2 \to 0.$$

For the unicity, if $||x_1|| = ||x_2|| = d$, then

$$||x_1 - x_2||^2 = 2(||x_1||^2 + ||x_2||^2) - 4||\frac{x_1 + x_2}{2}||^2 \leq 4d^2 - 4d^2 = 0.$$

□

Cor. (11.9.2.2) [Orthogonal Decomposition]. The orthogonal complement of a closed subspace of a Hilbert space exists. and the projection on to a closed subspace exists. This is a good trait of Hilbert space. ⌟

Proof: For any element x, let y be the optimal approximation(11.9.2.1) of x, then $z = x - y$ is orthogonal to y. □

Thm. (11.9.2.3) [Riesz]. Linear functionals on a Hilbert space over $\mathbb{C}$ are all of the form $x \mapsto (x, z)$ (Choose an orthogonal of the kernel). In other words, Hilbert spaces are reflexive. ⌟

Proof: Choose a x_0 orthogonal to $N(f)$ by(11.9.2.2) and $||x_0|| = 1$, then any $x = \alpha x_0 + y$ where $y \in N(f)$. Inner product with x_0, we get $\alpha = (x, x_0)$, so $f(x) = \alpha f(x_0) = (x, \overline{f(x_0)} x_0)$. □

Cor. (11.9.2.4). For Hilbert spaces $\mathcal{H}, \mathcal{H}'$ and $T \in \mathcal{L}(\mathcal{H}, \mathcal{H}')$, $||T|| = \sup\{(Tx, y) | ||x|| \leq 1, ||y|| \leq 1\}$. ⌟

Proof: Use(11.8.3.6) to find for each x a functional f of norm 1 that $|f(Tx)| = ||Tx||$, then use Riesz theorem. In particular, if we define □

Cor. (11.9.2.5) [Reproducing Kernel]. For a Hilbert space H, if elements of H are all complex valued functions on a set S, and $J_x : f \mapsto f(x)$ is continuous functional for H, then there is a function $K(x, y)$ on $S \times S$ that $K_y(x) = K(x, y) \in H$, and $f(y) = (f, K_y)_H$, called the **reproducing kernel**.

And if e_α is a basis for H, then $K(x, y) = \sum e_\alpha(x) \overline{e_\alpha}(y)$. ⌟

Proof: For any y, there is a $K_y \in H$ that $f(y) = (f, K_y)_H$ by Riesz representation. If we let $K(x, y) = (K_y, K_x) = K_y(x)$, then this is the desired kernel.

If e_α is a basis, then $K_x = (K_x, e_n) e_n = \overline{e_n(x)} e_n$, so by Parseval equality, $K(x, y) = \sum e_\alpha(x) \overline{e_\alpha(y)}$. □

Prop. (11.9.2.6). Let $\mathcal{H}$ be a Hilbert space, then a sequence x_n converges to x iff x_n converges to x weakly and $||x||_n \to ||x||$. ⌟

Proof: One direction is trivial, for the other, notice that $||x_n - x||^2 = ||x_n||^2 + ||x||^2 - 2\,\mathrm{Re}(x, x_n)$ which converges to 0. □

Thm. (11.9.2.7) [Lax-Milgram]. If $a(x, y)$ is a sesquilinear form on a Hilbert space H over $\mathbb{C}$ that $|a(x, y)| \leq M ||x|| ||y||$, then there is a unique continuous operator $A \in L(H)$ that $a(x, y) = (x, Ay)$. If moreover $|a(x, x)| \geq \delta ||x||^2$, then A is bijective and $||A^{-1}|| \leq \frac{1}{\delta}$. ⌟

Proof: For any y, $x \mapsto a(x, y)$ is a continuous functional, so by Riesz, there is an element Ay that $a(x, y) = (x, Ay)$.

Now Ay depends linearly on y, and $||Ay|| = \sup |a(x, y)| / ||x|| \leq M ||y||$.

If $|a(x, x)| \geq \delta ||x||^2$, then A is clearly injective, and $R(A)$ is closed, because for any $z = \lim Av_n$, it is easily verified that v_n is a Cauchy sequence. And $R(A)^\perp = 0$, because if $(w, Av) = 0$ for any $v \in H$, then $\delta ||w||^2 \leq |a(w, w)| = 0$. A^{-1} exists by Banach theorem(11.7.2.6), and $\delta ||x||^2 \leq |a(x, x)| = (x, Ax)| \leq ||x|| ||Ax||$, so $\delta ||x|| \leq ||Ax||$. □

Cor. (11.9.2.8) [Variational Inequality]. If H is a Hilbert space that $a(x, y)$ is an anti-symmetric bilinear function that $\delta ||x||^2 \leq a(x, x) \leq M ||x||^2$, then if $u_0 \in H$, and C is a closed convex subset of X, the function

$$f : x \mapsto a(x, x) - \mathrm{Re}(u_0, x)$$

attains minimum at C. ⌟

Proof: Similar to the proof of(11.9.2.1). $f(x) \geq \delta ||x||^2 - ||u_0||||x||$ is bounded below on C. if x_n is a sequence that converse to the infimum d, then

$$\begin{aligned} a(x_n - x_m, x_n - x_m) &= 2(a(x_n, x_n) + a(x_m, x_m)) - 4a(\frac{x_n + x_m}{2}, \frac{x_n + x_m}{2}) \\ &= 2(f(x_n) + f(x_m)) - 4f(\frac{x_n + x_m}{2}) \leq 2[(d + 1/n)^2 + (d + 1/m)^2] - 4d^2 \to 0. \end{aligned}$$

So x_n is a Cauchy sequence by the condition, and it contains a unique minimum. □

Cor. (11.9.2.9) [Involutions]. For a Hilbert space $\mathcal{H}$ over $\mathbb{C}$, for any $T \in L(H)$, there is an operator $T^* \in L(H)$ that $(Tx, y) = (x, T^*y)$, which is called the **formal adjoint** or involution of T. Notice it is defined on H, not on H^*.

Moreover, $||T|| = ||T^*|| = ||T^*T||^{1/2}$. ⌟

Proof: Use Lax-Milgram(11.9.2.7) for $a(x, y) = (Tx, y)$. For the last assertion, $|||T|| = ||T^*||$ by(11.9.2.4). And we notice

$$||Tx||^2 = (Tx, Tx) = (T^*Tx, x) \leq ||T^*T||||x||^2,$$

so $||T|| \leq ||T^*T||^{1/2}$. □

Remark (11.9.2.10) [Examples]. The dual operator of the integral operators(11.8.5.2) with kernel $K(x, y)$ is also an integral operator with kernel $K^*(x, y) = \overline{K(y, x)}$, by Fubini-Tonelli theorem. ⌟

3 C^*-algebra

Def. (11.9.3.1)[C^*-Algebras]. A **B^*-algebra**(or C^*-algebra) is a Banach algebra A with an involution $* : A \to A$ s.t. $||xx^*|| = ||x||^2$ for any $x \in A$. ⌟

Prop. (11.9.3.2). For a Hilbert space, the adjoint operation serves as an involution and makes $B(H)$ into a B^*-algebra by(11.9.2.9). ⌟

Prop. (11.9.3.3) [Gelfand-Naimark]. For a commutative C^*-algebra, the Gelfand transform $x \mapsto \widehat{x}$ is an isomorphism from A to $C(\Delta)$ with $||x|| = ||\widehat{x}||_\infty$ and $\widehat{x^*} = \overline{\widehat{x}}$. ⌟

Proof: First use $||xx^*|| = ||x||^2$ to prove that a Hermitian element is mapped to real function, and use Stone-Weierstrass to show that the image is dense, then let $y = xx^*$ and $||y^{2^m}|| = ||y||^{2^m}$ to prove $||\widehat{x}|| = ||x||$, so its image is closed. □

Cor. (11.9.3.4). If A is a commutative B^*-algebra that contains an element x s.t polynomials of x, x^* are dense in A, then $\widehat{x}$ is an isomorphism from Δ_A to $\sigma(x)$, in particular, the Gelfand transform(11.9.1.21) is an isomorphism from $C(\sigma(x))$ to A. ⌟

Proof: Cf.[Rudin P290]. □

Now we want to apply commutative algebra methods in the non-commutative case, there are two ways.

Prop. (11.9.3.5). For a commutative set of elements S in A, its bicommutant(11.16.1.2) $B = \Gamma(\Gamma(S))$ is commutative, closed and contains S. And $\sigma_B(x) = \sigma_A(x)$ for $x \in B$. ⌟

Proof: Because $S \subset \Gamma(S)$, $\Gamma(\Gamma(S)) \subset \Gamma(S)$, thus $\Gamma(\Gamma(S))$ is commutative. And if $xy = yx$, then $x^{-1}y = yx^{-1}$, so the inverse, if exists, are in B. □

Cor. (11.9.3.6). In a Banach algebra, if x, y commutes, then

$$\sigma(x+y) \subset \sigma(x) + \sigma(y), \quad \sigma(xy) \subset \sigma(x)\sigma(y).$$

⌟

Proof: Because $\sigma(x)$ is just the range of $\widehat{x}$ on Δ_A where $A = \Gamma(\Gamma(\{x, y\}))$(11.9.3.5)(11.9.1.21). □

The second method applies to normal elements:

Def. (11.9.3.7) [Normal]. In a Banach algebra with an involution, a set S is called **normal** if it is commutative and $S^* = S$. An element x is called:

- **normal** iff x commutes with x^*.
- **unitary** iff $x^* = x^{-1}$.
- **Hermitian** iff $x^* = x$.
- **positive** iff $x = x^*$ and $\sigma(x) \subset [0, \infty)$.

⌟

Prop. (11.9.3.8). A maximal normal set B in A is a closed subalgebra and $\sigma_B(x) = \sigma_A(x)$ for $x \in B$. ⌟

Proof: Cf.[Rudin P294]. □

Cor. (11.9.3.9) [Normalness and Spectra]. In a B^*-algebra A,

- Hermitian elements have real spectra.
- If x is normal, then $\rho(x) = ||x||$.
- If $u, v \geq 0$, then $u + v \geq 0$.
- $yy^* \geq 0$. Thus $e + yy^*$ is invertible.

⌟

Proof: Cf.[Rudin P295]. □

Def. (11.9.3.10)[Positive Functional]. Let $(A, *)$ be a Banach algebra with an involution, a **positive functional** on A is a function $F : A \to \mathbb{C}$ such that $F(xx^*) \geq 0$. It has the following properties.

- $F(x^*) = \overline{F(x)}$ and $|F(xy^*)|^2 \leq F(xx^*)F(yy^*)$. (Use Swartz like trick).
- $|F(x)|^2 \leq F(e)F(xx^*) \leq F(e)^2\rho(xx^*)$, because $e = ee^*$. Thus $|F(x)| \leq F(e)\rho(x)$ for every normal x by(11.9.3.9), so $||F|| = F(e)$ if A is commutative.

⌟

Proof: Cf.[Rudin P297]. □

Prop. (11.9.3.11) [Positive Functionals and Measures]. If A is a commutative Banach algebra with an involution that $h(x^*) = \overline{h(x)}$, then The map

$$\mu \to F(x) = \int_\Delta \widehat{x} d\mu$$

is a one-to-one correspondence between the convex set of measures μ that $\mu(\Delta) \leq 1$ to the convex set K of positive functionals on A of norm ≤ 1, i.e. $F(e) \leq 1$, so maps the extreme points, i.e. the point mass to extremes points, thus the extreme points of K is exactly Δ. This can be used to prove Bochner's theorem**??** ⌟

Proof: Use the last prop to show that there is a functional on $C(\Delta)$ and use Riesz representation. It is positive and by Stone-Weierstrass, it is unique. □

Thm. (11.9.3.12) [Gelfand-Naimark-Segal]. Any C^*-algebra is isomorphic to a closed subspace of $B(\mathcal{H})$ for some $\mathcal{H} \in \mathcal{H}\mathrm{ilb}\mathcal{S}\mathrm{pa}$. ⌟

Proof: Cf.[Rudin]. □

4 Spectral Theory on Hilbert Spaces

The most useful tool is the general symbolic calculus for normal operators.

Resolution of Identity

Def. (11.9.4.1). A **resolution of identity** on a Hilbert space H for a σ-algebra on a set Ω is a E that:

1. $E(\varnothing) = 0, E(\Omega) = 1$.
2. $E(\omega)$ is self-adjoint projection.
3. $E(\omega' \cap \omega) = E(\omega')E(\omega)$.
4. $E(\omega \cup \omega') = E(\omega) + E(\omega')$ for disjoint ω, ω'.
5. $E_{x,y}(\omega) = (E(\omega)x, y)$ is a complex measure on E.

Thus for any x, $\omega \to E(\omega)x$ is a countably additive H-valued measure.

This will generate an isometric*-isomorphism Ψ of the Banach algebra $L^\infty(E)$ onto a closed normal subalgebra A of $B(H)$. (Define on simple function first).

$$\Psi(f) = \int_\Omega f dE, \quad (\Psi(f)x, y) = \int_\Omega f dE_{x,y}$$

⌟

Proof: Cf.[Rudin P319]. □

Prop. (11.9.4.2) [Spectral Decomposition for Normal Algebra]. For any closed normal algebra A of $B(H)$, there is a unique resolution E of identity on the Borel subsets of Δ_A that the inverse of Gelfand transform extends to an isometric *-isomorphism Φ of the algebra $L^\infty(E)$ to a closed subalgebra B containing A.

In fact, $B = \Gamma(\Gamma(A))$ is normal by Fuglede theorem(11.9.4.10). ⌟

Proof: Cf.[Rudin P322]. □

Cor. (11.9.4.3)[Generalized Symbolic Calculus for Normal Operator]. For a normal operator T and the minimal closed commutative B^*-algebra A it generates, then the inverse of Gelfand transform gets us a map $\Psi : C(\sigma(x)) \to A$ that $\Psi(z) = x$, $\Psi(\overline{z}) = x^*$, by(11.9.3.4).

Then the above proposition says there is a resolution of identity on the Borel set of $\sigma(T)$ that Ψ extends to a function that maps $L^\infty(m)$ to $B(H)$ and $||\Psi(f)|| = ||f||_\infty$. ⌟

Cor. (11.9.4.4)[Normal and Invariant Subspace]. Any closed normal algebra A has many invariant subspaces, just choose a decomposition of Borel sets $\Delta_A = \omega \coprod \omega'$, then $R(E(\omega)) \oplus R(E(\omega')) = H$.

In particular, any normal operator has an invariant subspace. ⌟

Normal Operators on Hilbert Space

Lemma (11.9.4.5). For a Hilbert space H and $T \in L(H)$, T is defined by values (Tx, x). ⌟

Proof: If $(Tx, x) = 0$, then $(Tx, y) + (Ty, x) = 0$, so $-i(Tx, y) + i(Ty, x) = 0$, solving $(Tx, y) = 0$ for all x, y, so $T = 0$. □

Prop. (11.9.4.6) [Normal Operators].

1. An operator is normal iff $||Tx|| = ||T^*x||$. So $N(T) = N(T^*)$ thus $\sigma_p(T^*) = \overline{\sigma_p(T)}$, and $R(T)$ is dense iff T is injective. And different eigenspaces are orthogonal.
2. An operator is unitary iff $R(U) = H$ and $||Ux|| = ||x||$ for every x. (Because an operator is defined by its value (Tx, y).

⌟

Proof: $||Tx||^2 = (T^*Tx, x)$, $||T^*x|| = (TT^*x, x)$, and they are equal iff T, T^* commutes by(11.9.4.5). In particular, for different eigenvectors, $\alpha(x, y) = (Tx, y) = (xT^*y) = (x, \overline{\beta}y) = \beta(x, y)$.

For unitary, one way is obvious, for the other, if $||Ux|| = ||x||$, then $(U^*Ux, x) = (x, x)$, so $U^*U = id$ by(11.9.4.5), and U is a bijection. So it is invertible. □

Cor. (11.9.4.7). For a normal operator T on a Hilbert space T is invertible iff there is a δ that $||Tx|| = ||T^*x|| \geq \delta||x||$. ⌟

Proof: T is injective iff $R(T)$ is dense, and if $||Tx|| = ||T^*x|| \geq \delta||x||$, then $R(T)$ is closed by(4.4.8.10), so it is invertible by Banach theorem. □

Prop. (11.9.4.8). If T is normal, then

1. $||T|| = \sup\{|(Tx, x)|\ ||x|| = 1\}$.
2. T is self-adjoint iff $\sigma(T)$ is real.
3. T is unitary iff $|\sigma(T)| = 1$.

⌟

Proof: For 1, $||T|| = \rho(T) = ||z_0||$ for some $z_0 \in \rho(T)$ by Naimark(11.9.3.3), then Urysohn lemma to show $E(U) \neq 0$ for a open U near x(because otherwise there is a continuous function supported in U that are mapped to 0), then there are $||x_0|| = 1$ that $E(U)x_0 = x_0$.

Consider now $f = (z - z_0)i_U(z)$, then $f(T)(x_0) = Tx_0 - \lambda_0 x_0$, so

$$(Tx_0, x_0) - \lambda_0| = |(f(T)x_0, x_0)| \leq ||f(T)|| = ||f|| \leq \varepsilon$$

This shows that $||T|| = \sup\{|(Tx, x)|\ ||x|| = 1\}$.

For $2, 3$, by generalized symbolic calculus(11.9.4.3), $\widehat{T} = \lambda$ on σ and $\widehat{T^*} = \overline{\lambda}$ on σ, so they are equal iff $\sigma(T)$ is real, and $TT^* = I$ iff $\lambda\overline{\lambda} = 1$ on $\sigma(T)$. □

Prop. (11.9.4.9) [Decomposition of Operators]. Every operator $S \in L(\mathcal{H})$ on a Hilbert space $\mathcal{H}$ is a linear combination of two self-adjoint operator and a linear combination of four unitary operator. ⌟

Proof: The first assertion is easy as $S = (S + S^*)/2 + (S - S^*)/2$. Now any self-adjoint operator is a multiple of a self-adjoint operator of norm $||S|| \le 1$, so $1 - S^2$ is positive, and we have $S = \frac{1}{2}(f_+(S) + f_-(S))$, where $f_\pm(s) = s \pm i\sqrt{1 - s^2}$. □

Prop. (11.9.4.10) [Fuglede]. If N_1 and N_2 are normal operators and A is a bounded linear operator on a Hilbert space such that $N_1 A = AN_2$, then $N_1^* A = AN_2^*$. ⌟

Proof: For any $S \in B(H)$, $\exp(S - S^*)$ is unitary thus $||\exp(S - S^*)|| = 1$, $\exp(N_1)A = A\exp(N_2)$. Because $\exp(M)T = T\exp(N)$, if we let $U_1 = \exp(M^* - M), U_2 = \exp(N - N^*)$, then

$$||\exp(N_1^*)T\exp(-N_2^*)|| = ||U_1 T U_2|| \le ||T||$$

because λN_i is normal. Now

$$||\exp(\lambda N_1^*)T\exp(-\lambda N_2^*)|| = ||U_1 T U_2|| \le ||T||$$

also holds, thus by Liouville, $\exp(\lambda N_1^*)T\exp(-\lambda N_2^*) = T$. Compare the coefficients of λ, we get the result. □

Prop. (11.9.4.11). An operator $T \in B(H)$ has the same spectrum w.r.t all the closed B^*-algebras of $B(H)$ containing it. ⌟

Proof: If T is invertible, because TT^* is self-adjoint thus has real spectrum(11.9.4.8) so doesn't separate $\mathbb{C}$ thus it is invertible in any closed B^*-algebra of $B(H)$(11.9.1.12). so does $T^{-1} = T^*(TT^*)^{-1}$. □

Prop. (11.9.4.12). For T normal and E its spectral decomposition, then if $f \in C(\sigma(T))$ and $\omega_0 = f^{-1}(0)$, then $N(f(T)) = R(E(\omega_0))$. ⌟

Proof: $\chi_{\omega_0} f = 0$, so $f(T)R(E(\omega_0)) = 0$, and if we let $\omega_n = f^{-1}([1/(n-1), 1/n))$, and let $f_n(\lambda) = 1/f(\lambda)\chi_{\omega_n}$, then $f_n(T)f(T) = E(\omega_n)$, so if $f(T) = 0$, then $E(\omega_n)x = 0$, so countable additivity shows that $E(\sigma \backslash \omega_0)x = 0$, so $E(\omega_0)x = x$. These shows the desired result. □

Cor. (11.9.4.13).

1. $N(T - \lambda I) = R(\{\lambda\})$.
2. every isolated point of $\sigma(T)$ is point spectrum, because this point is open thus is $E(\{x\}) \ne 0$ by Urysohn lemma.
3. if $\sigma(T)$ is countable, then every $x \in H$ has a unique orthogonal decomposition $x = \sum E(\lambda_i)x$ and $T(E(\lambda_i)x) = \lambda_i E(\lambda_i)x$.

⌟

Prop. (11.9.4.14) [Normal Compact Operator]. A normal operator $T \in B(H)$ is compact iff $\sigma(T)$ has no limit point except possibly 0 and $\dim N(T - \lambda I) < \infty$ for $\lambda \ne 0$.

In particular, a normal compact operator is a limit of f.d. operators ⌟

Proof: One direction is general, by(11.8.5.9), for the other, it is a limit of operators of finite dimensional range by general symbolic calculus(11.9.4.3). □

Cor. (11.9.4.15) [Spectral Theorem]. A compact normal operator (in particular a normal operator on a f.d linear space) is unitarily diagonalizable. ⌟

Proof: it suffices to find a basis of eigenvectors, but this is easy, just by(11.9.4.13). □

Cor. (11.9.4.16) [Hilbert-Schmidt]. For a self-adjoint compact operator A on a Hilbert space H, there is a set of orthonormal basis that A is diagonal on it. And of course, its eigenvalues are real and can only converges to 0(11.9.4.8). ⌟

Prop. (11.9.4.17). For a normal compact operator $T \in L(H)$, then:

1. T has an eigenvalue $|\lambda|$ that $|\lambda| = ||T||$.
2. $f(T)$ is compact if $f \in C(\sigma(T))$ and $f(0) = 0$.
3. $f(T)$ is not compact if $f \in C(\sigma(T))$ and $f(0) \neq 0$ and $\dim H = \infty$.

⌟

Proof: 1: The spectrum of maximal norm is isolated(11.8.5.9) hence a point spectrum by(11.9.4.13). And $|\lambda| = ||T||$ by symbolic calculus(11.9.4.3).

2: Cf.[Rudin P330].

3: The 2 sill show that $f(0)I - f$ is compact, If f is compact, then $f(0)I$ is compact, so $\dim H < \infty$(11.8.5.3). □

Prop. (11.9.4.18) [Freudenthal Spectral Theorem]. ⌟

Prop. (11.9.4.19) [Positive Equivalent Definition]. A $T \in L(H)$ is positive, i.e. $T = T^*$ and $\sigma(T) \subset [0, \infty)$ iff $(Tx, x) \geq 0$. ⌟

Proof: If $(Tx, x) \geq 0$, then $(Tx, x) = (x, Tx) = (T^*x, x)$, so $T = T^*$ by(11.9.4.5), so $\sigma(T)$ is real(11.9.4.8), and for $\lambda > 0$,

$$\lambda ||x||^2 = (\lambda x, x) \leq ((T + \lambda I)x, x) \leq ||(T + \lambda I)x|| ||x||,$$

so $T + \lambda I$ is invertible by(11.9.4.7), so $\sigma(T) \subset [0, \infty)$.

Conversely, if T is positive, then it is normal, so $(Tx, x) = \int_{\sigma(T)} \lambda dE_{x,x} \geq 0$. □

Prop. (11.9.4.20) [Polar Decomposition].

1. Every positive operator T has a positive square root, which is invertible if T is.
2. Polar decomposition exists in $B(H)$: Any $T \in L(H)$ invertible has a unique decomposition $T = UP$ where U is unitary and P is positive. And $||Px|| = ||Tx||$ for all x.
3. Any normal operator has commuting decomposition UP, where U, P, T commutes.

⌟

Proof: 1: Use general symbolic calculus, then $S = \sqrt{\lambda}(T)$ is the square root of T. If T is invertible, then $S^{-1} = T^{-1}S$.

2: $(T^*Tx, x) = (Tx, Tx) \geq 0$, so T^*T is positive(11.9.4.19), so let $P = \sqrt{T}$, then it is also invertible, and $U = TP^{-1}$ is unitary.

3: Use general symbolic calculus, let $p(\lambda) = |\lambda|$, $u(\lambda) = \lambda/|\lambda|$ if $\lambda \neq 0$, and $u(0) = 0$. Then $T = UP$, and they are commutative. □

Cor. (11.9.4.21) [Similar Normal Operator]. Similar normal operators are unitarily equivalent. ⌟

Proof: It suffices to show that if $M = TNT^{-1}$, and $T = UP$ is the polar decomposition, then $M = UNU^{-1}$. Fuglede(11.9.4.10) shows $M^*T = TN^*$, so $NP^2 = NT^*T = T^*MT = T^*TN = P^2N$, so N commutes with any functions $f(P)$, in particular P. Hence $M = (UP)N(UP)^{-1} = UNU^{-1}$. □

5 Hilbert-Schmidt Operators & Trace Classes

References are [Trace Classes and Hilbert-Schmidt Operators].
In this subsection, all Hilbert spaces are separable.

Def. (11.9.5.1) [Hilbert-Schmidt Operator]. Let $\mathcal{H},\mathcal{K}$ be Hilbert spaces and $T\in L(\mathcal{H},\mathcal{K})$. Then for any orthonormal basis $\{e_k\}$ of $\mathcal{H}$ and $\{f_k\}$ of $\mathcal{K}$,

$$\sum_j ||Te_j||_{\mathcal{K}}^2 = \sum_j ||T^* f_j||_{\mathcal{H}}^2.$$

T is called a **Hilbert-Schimidt** iff

$$||T||_{\text{H-S}} = (\sum_j ||Te_j||_{\mathcal{K}}^2)^{1/2} < \infty$$

for some/all basis e_j of $\mathcal{H}$. The space of all Hilbert-Schimidt between $\mathcal{H},\mathcal{K}$ is denoted by $S_2(\mathcal{H},\mathcal{K})$. ⌟

Proof:

$$\sum_i ||Te_k||^2 = \sum_i\sum_j |(Te_i,f_j)|^2 = \sum_i\sum_j |(T^*f_j,e_i)|^2 = \sum_j ||T^*f_j||^2$$

□

Cor. (11.9.5.2) [Properties of $S_2(\mathcal{H},\mathcal{K})$].

- If $A\in S_2(\mathcal{H},\mathcal{K})$ then $A^*\in S_2(\mathcal{K},\mathcal{H})$ with the same HS-norm.
- For $A\in S_2(\mathcal{H},\mathcal{K})$, $||A||\le ||A||_{\text{H-S}}$.
- $S_2(\mathcal{H},\mathcal{K})$ is a Banach space in the HS-norm.
- If $\mathcal{H}_1,\mathcal{K}_1$ are separable Hilbert spaces and $T\in S_2(\mathcal{H},\mathcal{K}), A\in\mathcal{L}(\mathcal{H}_1,\mathcal{H}), B\in\mathcal{L}(\mathcal{K},\mathcal{K}_1)$, then $BTA\in S_2(\mathcal{H}_1,\mathcal{K}_1)$.

⌟

Proof: 1 follows from(11.9.5.1). 2 is because we can extend u to a basis of $\mathcal{H}$.

3: $||-||_{HS}$ is clearly a semi-norm(11.7.1.7), and it is a norm by item2. To show the completeness, if A_j is an HS-Cauchy sequence, then it is a Cauchy sequence in the operator norm, thus converges to an operator A. Then for any ε, there is an N that for any $j,k\ge N$, $||A_j-A_k||_{HS}\le\varepsilon$. This implies

$$\sum_{\alpha\in S} ||(A_k-A_j)e_\alpha||_{\mathcal{K}}^2 \le \varepsilon^2$$

for any finite subset $S\subset I$. Then letting $k\to\infty$ and then letting S be any subset, we get $||A-A_j||_{HS}\le\varepsilon$. Thus A is Hilbert-Schmidt and $A_j\to A$ in HS-norm.

4: it is clear that $||BT||_{\text{H-S}}\le ||B||||T||_{\text{H-S}}$, and use the transpose invariance of HS-norms and operator norms(11.9.2.9). □

Prop. (11.9.5.3) [Hilbert-Schmidt Operator is Compact]. If $A\in S_2(\mathcal{H},\mathcal{K})$ and $\{f_k\}$ is an orthonormal basis of $\mathcal{K}$, and we denote pr_n as the projection of $\mathcal{K}$ onto the span of $\{f_1,\ldots,f_n\}$, then

$$||\operatorname{pr}_n A - A||_{\text{H-S}} \to 0.$$

In particular, A is compact, by(11.9.5.2) and(11.8.5.3). ⌟

Proof: By(11.9.5.2), it suffices to show that $||A^*\pi_n - A^*||_{HS} \to 0$. But this norm is just $\sum_{k>N} ||A^* f_k||^2_{\mathcal{H}}$, which converges to 0. □

Prop. (11.9.5.4)[Hilbert-Schmidt Inner Product]. If $\mathcal{H}$ is a Hilbert space and $A, B \in S_2(\mathcal{H})$, then $B^*A \in S_1(\mathcal{H})$ by(11.9.5.2)(11.9.5.7), then we can define an **Hilbert-Schmidt inner product** on $S_2(\mathcal{H})$:

$$(A, B)_{\text{H-S}} = \text{tr}(B^*A)(11.9.5.9).$$

Then this makes $S_2(\mathcal{H})$ a Hilbert space. ⌟

Proof: This follows from(11.9.5.2). □

Prop. (11.9.5.5) [Integral Operator is Hilbert-Schmidt]. Let Ω be a σ-finite measure space and $K(x, y) \in L^2(\Omega \times \Omega)$, then the operator $Lu(x) = \int_\Omega K(x, y)u(y)dy$ defined in(11.8.5.2) is a Hilbert-Schmidt operator on $L^2(\Omega)$. In fact, $||L||_2 = ||K||_{L^2}$. ⌟

Proof: Let $\mathcal{E}$ be an Hilbert basis of $L^2(\Omega)$, then we have

$$||L||_2^2 = \sum_{f_1, f_2 \in \mathcal{E}} |(Lf_1, f_2)|^2 = \sum_{f_1, f_2 \in \mathcal{E}} |\int_X \int_X \overline{f_2(y)} K(x, y) f_1(x) dxdy|^2 = \sum_{f_1, f_2 \in \mathcal{E}} (K, f_1 \otimes f_2)^2$$

But by(11.3.6.4) $\{f_i \otimes f_j\}$ form a Hilbert Basis for $L^2(\Omega \times \Omega)$, then the equation equals $||K||_2^2$ □

Trace Classes

Def. (11.9.5.6) [Trace Classes]. Let $\mathcal{H}$ be a Hilbert space, $\{e_i\}, \{f_i\}$ are two orthonormal basis, $A \in B(\mathcal{H})$. Let $|A| = (A^*A)^{1/2}$ which is positive, then

$$\sum_i (|A|e_i, e_i) = \sum_i (|A|^{1/2} e_i, |A|^{1/2} e_i) = \sum_i |||A|^{1/2} f_i|| = \sum_i (|A| f_i, f_i)$$

by(11.9.5.1), thus we can define $||A||_1 = \sum_i (|A|e_i, e_i)$, and say A is a **trace class** if $||A||_1 < \infty$. The space of trace classes is denoted by $S_1(\mathcal{H})$.

A trace-class A is clearly compact as $|A|$ is a limit of f.d. range operators.(Use diagonalization, then there are only countably many eigenvectors of $|A|$). ⌟

Prop. (11.9.5.7). If $A \in \mathcal{B}(\mathcal{H})$, then the following are equivalent:

- $A \in S_1(\mathcal{H})$.
- $|A|^{1/2} \in S_2(\mathcal{H})$.
- $|A|$ is a product of two elements in $S_2(\mathcal{H})$.
- A is a product of two elements in $S_2(\mathcal{H})$.

⌟

Proof: $1 \to 2 \to 3$ is clear, for $3 \to 4$: if $|A| = TS$, then by polar decomposition $A = U|A| = (UT)S$, and $UT \in S_2(\mathcal{H})$ by(11.9.5.2), so A is a product of two elements in $S_2(\mathcal{H})$.

$4 \to 3$ is similar to $3 \to 4$.

$3 \to 1$: if $A = BC$ where $B, C \in S_2(\mathcal{H})$, then $B^* \in S_2(\mathcal{H})$ also by(11.9.5.2), and

$$||A||_1 = \sum_i (Ae_i, e_i) = \sum_i (Ce_i, B^*e_i) \le \sum_i ||Ce_i|| ||B^*e_i|| \le ||C||_2 ||B^*||_2 < \infty$$

□

Lemma (11.9.5.8). if T is a positive trace-class and $S \in \mathcal{L}(\mathcal{H})$, then if x_i is an orthonormal basis of $\mathcal{H}$, then

$$\sum_i (STx_i, x_i) \leq ||S||||T||_1$$

is absolutely convergent, and is independent of the basis chosen. ⌟

Proof: Let e_i be the basis of eigenvectors of T of eigenvalues $\lambda_i > 0$, then $\sum_i \lambda_i < \infty$ by(11.9.5.7), and

$$(STx_i, x_i) = \sum_j (x_i, e_j)(STe_j, x_i) = \sum_j \lambda_j (x_i, e_j)(Se_j, x_i)$$

And

$$\sum_i \sum_j \lambda_j |(x_i, e_j)(Se_j, x_i)| \leq \sum_j \lambda_j ||e_j||||Se_j|| \leq ||S|| \sum \lambda_\alpha < \infty.$$

Moreover:

$$\sum_i (STx_i, x_i) = \sum_i \sum_j ((x_i, e_j)STe_j, x_i) = \sum_i \sum_j (STe_j, (e_j, x_i)x_i) = \sum_j (STe_j, e_j).$$

□

Prop. (11.9.5.9) [Singular Trace]. If $\mathcal{H} \in \mathcal{H}\text{ilb}\mathcal{S}\text{pa}$ with an orthonormal Hilbert basis $\{x_\alpha\}$ and $T \in S_1(\mathcal{H})$, then $\sum (Tx_\alpha, x_\alpha)$ absolutely converges, and is independent of the basis chosen, called the **singular trace** $\operatorname{tr} T$ of T. The singular trace is a positive definite linear functional on $S_1(\mathcal{H})$. ⌟

Proof: Use polar decomposition $T = U|T|$(11.9.4.20) and notice $|T|$ is a positive trace class(11.9.5.7) and then use(11.9.5.8). □

Prop. (11.9.5.10) [Trace of Integral Operators]. Let A, B be L^2 integral operators on a σ-finite measure space Ω with kernel $K_1(x, y), K_2(x, y) \in L^2(\Omega \times \Omega)$, then AB is also an integral operator with kernel

$$\int K_1(x, z)K_2(z, y)dz,$$

and

$$\operatorname{tr}(AB) = \int \int K_1(x, y)K_2(y, x)dxdy.$$

⌟

Proof: The formula for integral kernel is an immediate consequence of Fubini-Tonelli theorem. For the trace, observe that A^* is the integral operator with kernel $\overline{K_1(y, x)}$(11.9.2.10), thus

$$\begin{aligned}
\operatorname{tr}(AB) &= \sum_i (ABe_i, e_i) = \sum_i (Be_i, A^* e_i) \\
&= \sum_i \sum_k (e_k, A^* e_i)(Be_i, e_k) \\
&= \sum_i \sum_k (e_k \otimes \overline{e_i}, K_1^*)(K_2, e_k \otimes \overline{e_i}) \\
&= (K_2, K_1^*) = \int \int K_1(x, y)K_2(y, x)\mathrm{d}x\mathrm{d}y
\end{aligned}$$

as $\{e_i \otimes \overline{e_k}$ is a Hilbert basis for $\Omega \times \Omega$(11.3.6.4). □

Prop. (11.9.5.11) [Properties of Trace Classes].

1. $S_1(\mathcal{H})$ is a two-sided *-ideal of $\mathcal{L}(\mathcal{H})$.
2. $||\cdot||_1$ is a norm on $S_1(\mathcal{H})$.
3. If $T\in S_1(\mathcal{H})$, then $\mathrm{tr}\, T^*=\overline{\mathrm{tr}\, T}$.
4. For any $T\in S_1(\mathcal{H})$ and $S\in L(\mathcal{H})$, $\mathrm{tr}(ST)=\mathrm{tr}(TS)$, and $|\,\mathrm{tr}(ST)|\leq ||S||||T||_1$. In particular the singular trace is a bounded linear functional on $S_1(\mathcal{H})$.

⌟

Proof: Let $S,T\in S_1(\mathcal{H})$, $S=V|S|, T=W|T|$, $S+T=X|S+T|$ where V,W,X are unitary, then $|S+T|=X^*(S+T)$ is positive compact, so it has an orthonormal eigenbasis e_n by(11.9.4.16), so

$$\sum(|S+T|x_i,x_i)=\sum(X^*V|S|x_i,x_i)+\sum(X^*W|S|x_i,x_i)\leq ||S||_1+||T_1||$$

by(11.9.5.8). So $S+T$ is a trace class, and $||S+T||_1\leq ||S||_1+||T||_1$.

Now if U is unitary and $T\in S_1(\mathcal{H})$, then $(UT)^*UT=T^*T$, so UT is a trace class, and $(TU)^*TU=U^{-1}TU$ has $|TU|=U^{-1}|T|U$, so TU is also a trace class. Moreover, $\mathrm{tr}(TU)=\sum(TUx_i,x_i)=\sum(UTUx_i,Ux_i)=\mathrm{tr}(UT)$.

Then notice very $S\in L(\mathcal{H})$ is a linear combination of four unitary operator(11.9.4.9), so the proposition is true, and if T is a trace class, then $T=V|T|$, and $T^*=|T|V^*$ is also a trace class.

4: $|\,\mathrm{tr}(ST)|\leq ||SV||||T||_1=||S||||T||_1$ by(11.9.5.8). □

Prop. (11.9.5.12) [Trace Classes form a Banach Space]. Let $S_0(\mathcal{H})$ be the space of operators of f.d. range, then the map

$$\rho: S_1(\mathcal{H})\to S_0(\mathcal{H})^*:\rho(A):C\mapsto \mathrm{tr}(CA)$$

is an isometric isomorphism. In particular, $S_1(\mathcal{H})$ is a Banach space, by(11.7.3.1). ⌟

Proof: Clearly ρ is a linear map as singular trace is. For $T\in S_1(\mathcal{H})$, $||\rho(T)||\leq ||T||_1$ by(11.9.5.11).

If $\Phi\in S_0(\mathcal{H})^*, g,h\in\mathcal{H}$, consider $g\otimes h^*\in S_0(\mathcal{H})$ that $g\otimes h^*(v)=(v,h)g$, then $B(g,h)=\Phi(g\otimes h^*)$ is a sesquilinear form on H that is bounded by $||\Phi||$. Thus by Lax-Milgram(11.9.2.7), there is a unique $T\in\mathcal{B}(\mathcal{H})$ that $B(g,h)=(g,Th)$.

Now let $A=T^*$ and let $A=U|A|$ be the polar decomposition, $\mathcal{E}$ an orthonormal basis of $\mathcal{H}$ and $S\subset\mathcal{E}$ a finite subset, define

$$C_S=(\sum_{e\in S}e\otimes e^*)U^*=\sum_{e\in S}e\otimes(Ue)^*.$$

Then C_S is of f.d. and $||C_S||\leq 1$. And:

$$\sum_{e\in S}(|A|e,e)=\sum_{e\in S}(U^*Ae,e)=\sum_{e\in S}(e,TUe)=\sum_{e\in S}B(e,Ue)=\sum_{e\in S}\Phi(e\otimes(Ue)^*)=\Phi(C_S).$$

So $||A||_1\leq ||\Phi||$.

If C is any operator of f.d. range that $C=\oplus g_k\otimes h_k^*$, then

$$\Phi(C)=\sum\Phi(g_k\otimes h_k^*)=\sum B(g_k,h_k)=\sum(Ag_k,h_k)=\sum\mathrm{tr}(A(g_k\otimes h_k^*))=\mathrm{tr}(AC)=\rho(A)(C)$$

so the image is A is just Φ. This shows that ρ is surjective and moreover $||A||_1=||\rho(A)||$, so we are done. □

11.10 Analysis on Locally Compact Groups

Main references are [Fol15], [Bum98].

All representations in this section are assumed to be over $\mathbb{C}$.

1 Locally Compact Groups

Def. (11.10.1.1) [Left and Right Regular Actions]. On a topological group G, the **left regular action** and **right regular action** are defined as follows: $L_y f(x) = f(y^{-1}x), R_y f(x) = f(xy)$. ⌟

Def. (11.10.1.2) [Involution]. For $f \in C_c(G)$ or $f \in L^p(G)$ for some p, let $\widetilde{f}(x) = \overline{f(x^{-1})}$. ⌟

Prop. (11.10.1.3) [Translation is Continuous]. If $f \in C_c(G)$, then f is left and right uniformly continuous. Equivalently, $G \to C_c(G) : y \mapsto R_y(f)$ and $y \mapsto L_y(f)$ are continuous group homomorphisms from G to $C_c(G)$. ⌟

Proof: Cf.[Folland Abstract Harmonic Analysis P38]. □

Prop. (11.10.1.4). Locally compact Hausdorff group is normal. ⌟

Proof: Notice that by choosing a precompact symmetric open neighbourhood U of identity, there exists a σ-compact clopen subgroup H. So H can σ-locally refine every open cover, thus G can, too. So by (4.4.7.2) G is paracompact. As a topological group, G is regular, thus G is normal by (4.4.7.6). □

Prop. (11.10.1.5) [Dirac sequence]. For a locally compact Hausdorff group G , a **Dirac sequence** is a sequence $f_n \in C_c(G)$ that $f_n \to \delta_1$ in the weak topology of $Meas_c(G)$.

Dirac sequences exist. ⌟

Proof: □

Prop. (11.10.1.6). Every locally compact group G has a subgroup G_0 that is clopen and σ-compact. ⌟

Proof: Let U be a symmetric precompact nbhd of 1 in G, then let $U_n = U^n$, then $\overline{U_n} \subset U_{n+1}$, so let $G_0 = \cup_n U^n = \cup \overline{U_n}$, then it is open because each U_n does, and compact because each $\overline{U_n}$ does. □

Prop. (11.10.1.7). If G is locally compact Hausdorff, and H is subgroup that is locally compact in the induced topology, then H is closed in G. ⌟

Proof: By hypothesis there exists an open nbhd U of $e \in G$ that $U \cap H$ has compact closure $K \subset H$. But then K is also compact in G thus closed. So K is the closure of $U \cap H$ in G. Choose a symmetric open nbhd V of $e \in G$ that $VV \subset U$, and suppose $x \in \overline{H}$, then $x^{-1} \in \overline{H}$ and $Vx^{-1} \cap H \neq \varnothing$. Let $y \in Vx^{-1} \cap H$. For any nbhd U_i of $e \in G$, choose $x' \subset xU_i \cap H$, then $yx' = yx(x^{-1}x') \in yxU_i$ and also $yx' \in H$, $yx' \in Vx^{-1}xV \subset U$. By arbitrariness of U_i, this means $yx \in \overline{U \cap H} = K \subset H$, thus $x \in H$, and H is closed. □

Integration on Locally Compact Groups

Def. (11.10.1.8)[Positive Linear Functional]. A **positive linear functional** is a linear functional I on $C_c(X)$ that $I(f)\geq 0$ whenever $f\geq 0$. How is this definition compatible with that of(11.9.3.10)**?**. ⌟

Lemma (11.10.1.9) [Positive Linear Functional is Continuous]. For a LCH space X, a positive linear functional(11.10.1.8) I on $C_c(X)$ is automatically continuous, where $C_c(X)$ is given compact convergence topology as in(11.8.2.1). ⌟

Proof: We need to prove that for any compact subset K of X, there is a constant C_K that for any $f\in C(G)$ with support in K, we have $|I(f)|\leq C_K||f||_\infty$.

Given any K, choose by Urysohn lemma a $\varphi\in C_c(X,[0,1])$ that $\varphi=1$ on K, so if $\operatorname{Supp} f\subset K$, then $|f|\leq ||f||_\infty\varphi$, thus the positivity of I shows that $|I(f)|\leq I(\varphi)||f||_\infty$. □

Prop. (11.10.1.10)[Riesz-Markov-Kakutani Representation Theorem]. Let X be a locally compact Hausdorff space.

- If I is a positive linear functional(11.10.1.8) on $C_c(X)$, there is a unique Radon measure μ on X such that $I(f)=\int f d\mu$. Moreover,

$$\mu(U)=\sup\{I(f): f<U\}\text{ for } U \text{ open},$$

$$\mu(K)=\inf\{I(f): f>\chi_K\}\text{ for } K \text{ compact}.$$

- If I is a continuous linear functional on $C_0(X)$, there is a unique regular complex Borel measure μ on X that $I(f)=\int f d\mu$.

In particular if X is compact, $M(X)$ the space of Radon measures on X is the dual space of $C(X)$. ⌟

Proof: Cf.[Real Analysis Folland P212]. □

Prop. (11.10.1.11) [Haar Measure]. A left(right) **Haar measure** on a topological group G is a non-zero Radon measure(11.3.1.12) μ on G that satisfies $\mu(xE)=\mu(E)(\mu(Ex)=\mu(E))$. A Radon measure μ is a Haar measure iff it satisfies $\int L_y f d\mu=\int f d\mu$ for any $f\in C_c^+(G)$ and $y\in G$(11.10.1.3).

Every Locally compact group G possesses a unique left Haar measure μ. ⌟

Proof: If μ is a Haar measure, then $\int L_y f d\mu = \int f d\mu$ by approximation by simple functions(11.3.8.4). Conversely, if $\int L_y f d\mu=\int f d\mu$ for any $f\in C_c(G)$, then it holds for all $f\in C_c(G)$, hence $\mu(xE)=\mu(E)$ by Riesz-Markov-Kakutani representation theorem(11.10.1.10).

For $f,\varphi\in C_c^+(G)$, define $(f:\varphi)$ to be the infimum of all finite sms $\sum_{i=1}^n c_i$ that $f\leq\sum_{i=1}^n c_i L_{x_i}\varphi$ for some $x_1,\ldots,x_n\in G$. This makes sense because f has finite support so can be covered by f.m. translation of any open set. This quantity satisfies the following properties:

- $(f:\varphi)=(L_y f:\varphi)$ for any $y\in G$.
- $(f_1+f_2:\varphi)\leq(f_1:\varphi)+(f_2:\varphi)$.
- $(cf:\varphi)=c(f:\varphi)$.
- $(f_1:\varphi)\leq(f_2:\varphi)$ for $f_1\leq f_2$.
- $(f:\varphi)\geq ||f||_{sup}/||\varphi||_{sup}$.
- $(f:\varphi)\leq(f:\psi)(\psi:\varphi)$ for any $\psi\in C^+(G)$.

Now choose a $f_0 \in C_c^+(G)$ and define $I_\varphi(f) = \frac{(f:\varphi)}{(f_0,\varphi)}$ for $f, \varphi \in C_c^+(G)$. Then I_φ is left-invariant, subadditive, homogeneous of degree 1, and monotone. Moreover, it satisfies $(f_0 : f)^{-1} \le I_\varphi(f) \le (f : f_0)$.

Let X_f be the interval $[(f_0 : f)^{-1}, (f : f_0)]$, and let $X = \prod_{f \in C_c^+(G)} X_f$, then for each nbhd V of $1 \in G$, let $K(V)$ be the closure in X of $\{I_\varphi | \operatorname{Supp}(\varphi) \subset V\}$, then these sets satisfy finite intersection property. So by compactness, there is an I contained in every $K(V)$. Which means for any nbhd V of $1 \in G$ and $\varepsilon > 0$ and $f_1, \ldots, f_n \in C_c^+(G)$, there exists $\varphi \in C_c^+(V)$ that $|I(f_i) - I_\varphi(f_i)| < \varepsilon$. Then by some argument, I commutes with left translation, addition and multiplication by positive scalars. Now extend I to a positive linear functional on $C_c(G)$, and then use Riesz-Markov-Kakutani representation theorem(11.10.1.10) to finish. □

Lemma (11.10.1.12). For any $f_1, f_2 \in C_c^+(G)$ and $\varepsilon > 0$, there is a neighborhood V of $1 \in G$ that in the notation in the proof of(11.10.1.11), $I_\varphi(f_1) + I_\varphi(f_2) \le I_\varphi(f_1 + f_2) + \varepsilon$ whenever $\operatorname{Supp}(\varphi) \subset V$. ⌟

Proof: Let $g \in C_c^+(G)$ that $g = 1$ on $\operatorname{Supp}(f_1 + f_2)$ and $\delta > 0$, let $h_i = f_i/(f_1 + f_2 + \delta g)$, then $h_i \in C_c^+(G)$ and there is a nbhd V of $1 \in G$ s.t. $|h_i(x) - h_i(y)| < \delta$ for $i = 1, 2$ and $y^{-1}x \in V$. Take $\varphi \in C_c^+(G)$ with $\operatorname{Supp}(\varphi) \subset V$. If $h \le \sum c_i L_{x_i}\varphi$, then

$$f_i(x) = h(x)h_i(x) = \sum c_j \varphi(x_j^{-1}x)h_i(x) \le \sum c_j \varphi(x_j^{-1}x)[h_i(x_j) + \delta]$$

because whenever $\varphi(x_j^{-1}x) \ne 0$, $|h_i(x) - h_i(x_j)| < \delta$. As $h_1 + h_2 < 1$,

$$(f_1 : \varphi) + (f_2 : \varphi) \le \sum c_j[h_1(x_j) + \delta] + \sum c_j[h_2(x_j) + \delta] \le \sum c_j[1 + 2\delta]$$

which implies

$$I_\varphi(f_1) + I_\varphi(f_2) \le (1 + 2\delta)I_\varphi(h) \le (1 + 2\delta)[I_\varphi(f_1 + f_2) + \delta I_\varphi(g)].$$

Notice δ is arbitrary, thus we can choose δ small enough that the assertion is true. □

Prop. (11.10.1.13). If G is a locally compact group and μ is a Haar measure on G, then for any open subset U of G, $\mu(U) > 0$. ⌟

Proof: By inner regularity, $\mu(K) > 0$ for some compact subset K. Suppose $\mu(U) = 0$ for an open subset U, then f.m. translates of U covers K, contradiction. □

Prop. (11.10.1.14). Integration of a nontrivial character on a compact group G w.r.t. the Haar measure is 0. ⌟

Proof: $\int f(x)d\mu(x) = \int f(yx)d\mu(yx) = f(y)\int f(x)d\mu(x)$. Now choose a y that $f(y) \ne 1$. □

Def. (11.10.1.15) [Modular Function]. For a left Haar measure μ on a locally compact group G, $\mu_x(E) = \mu(Ex)$ is also a left Haar measure, so there is a $\Delta(x)$ that $\mu_x = \Delta(x)\mu$. Then the function Δ is a group homomorphism from G to $\mathbb{R}^+$, which is called the **modular function** of G.

G is called **unimodular** iff $\Delta = 1$, i.e. a left Haar measure is also a right Haar measure. Obviously, a locally compact Abelian group is unimodular. ⌟

Prop. (11.10.1.16). Δ is a continuous group homomorphism from G to $\mathbb{R}^+$, and

$$\int R_y f d\mu = \Delta(y^{-1}) \int f d\mu.$$

equivalently, $d\mu(xy_0) = \Delta(y_0)d\mu(x)$. ⌟

Proof: For the continuity of Δ, because $y \mapsto R_y(f)$ is continuous for each f(11.10.1.3), so $y \mapsto \int R_y f d\lambda$ is continuous, as μ is Radon measure, so by the equation just proved, Δ is continuous.

Now for any measurable function E, $\chi_E(xy) = \chi_{Ey^{-1}}(x)$, thus

$$\int \chi_E(xy) d\mu = \mu(Ey^{-1}) = \Delta(y^{-1})\mu(E) = \Delta(y^{-1}) \int \chi_E(x) d\mu(x),$$

which proves the equation for $f = \chi_E$. Then the general case follows from approximating f by simple functions(11.3.8.5). □

Prop. (11.10.1.17) [Involution Measure]. If μ is a left Haar measure and ρ is defined by $\rho(E) = \mu(E^{-1})$, then ρ is a right Haar measure, and $d\rho(x) = d\mu(x^{-1}) = \Delta(x^{-1})d\mu(x)$. ⌟

Proof: Notice

$$\int R_y(f)(x)\Delta(x^{-1})d\mu(x) = \Delta(y) \int f(xy)\Delta((xy)^{-1})d\mu(x) = \int f(x)\Delta(x^{-1})d\mu(x),$$

so $\Delta(x^{-1})d\mu(x)$ is a right Haar measure, hence $cd\mu(x^{-1})$ for some c. If $c \neq 1$, we let U be a precompact symmetric nbhd U of 1 that $|\Delta(x^{-1}) - 1| \leq \frac{1}{2}|c-1|$ on U. But then $|c-1|\mu(U) = |\int_U (\Delta(x^{-1}) - 1)d\mu(x)| \leq \frac{1}{2}|c-1|\mu(U)$, contradiction. □

Prop. (11.10.1.18). For a compact group K of G, Δ is trivial on K. So compact group is unimodular, and if $G/[G,G]$ is compact, then it is also unimodular. ⌟

Proof: These all follow from(11.10.1.16) and the fact that a compact subgroup of $\mathbb{R}^+$ is $\{1\}$, and $\mathbb{R}$ is Abelian. □

Prop. (11.10.1.19) [Lie Type Case]. Suppose G is an open subset of K^N where K is a local field, and the left translation is given by

$$xy = A(x)y + b(x)$$

then the Haar measure of G is given by $|\det A(x)|^{-1}dx$, where dx is the Lebesgue measure on $\mathbb{R}^N$.

Also when we want to calculate the right Haar measure, consider the right action. ⌟

Proof: Use change of variable formula, because $A(xy) = A(x)A(y)$, and

$$|\det A(ax)|^{-1}d(ax) = |\det A(ax)|^{-1}d(A(a)x + b(x)) = |\det A(x)|^{-1}dx.$$

□

Cor. (11.10.1.20) [Examples of Lie Group Measures].

- $dx/|x|$ is the Haar measure on $\mathbb{R}^*$.
- $dxdy/x^2 + y^2$ is the Haar measure on $\mathbb{C}^*$.
- $x_{11}x_{22}^2 \ldots x_{nn}^n \prod_{i<j} dx_{ij}$(resp. $x_{11}^n x_{22}^{n-1} \ldots x_{nn} \prod_{i<j} dx_{ij}$) are the left(resp. right) Haar measure on the group of upper-triangular matrixes in $GL(n, \mathbb{R})$.
- $\prod_{i<j} dx_{ij}$ is the left and right Haar measure on the group of upper-triangular unipotent matrices in $GL(n, \mathbb{R})$.
- $|\det T|^{-n}dT$ is the left and right Haar measure on the group $GL(n, \mathbb{R})$, where dT is the Lebesgue measure on $M_n(\mathbb{R}) = \mathbb{R}^{n^2}$.

- The $ax+b$ group G of all affine (invertible)translations of $\mathbb{R}$ has left measure $dadb/a^2$ and right Haar measure $dadb/a$.

⌟

Proof: Clear. □

Prop. (11.10.1.21) [Modular Function of Lie Groups]. If G is a Lie group and Ad is the adjoint action of G on $\mathfrak{g}$, then $\Delta(x) = |\det \mathrm{Ad}(x^{-1})|$. ⌟

Proof: Let G be a Lie group of dimension m, then the Haar measure on a Lie group is given by the absolute value of a left-invariant m-form ω. Now for any $X \in \mathfrak{g}$ corresponding to a left invariant vector space L_X,

$$d(R_g)_p((L_X)_p) = (L_{\mathrm{Ad}(g^{-1})X})_{pg}$$

by(12.11.3.5), so $R_g^*\omega = \det(\mathrm{Ad}(g^{-1}))\omega$. So $\Delta(g)\omega = R_g^*|\omega| = |\det(\mathrm{Ad}(g^{-1}))||\omega|$. □

Cor. (11.10.1.22) [Unimodular Lie Groups]. Any Abelian/compact/semisimple/reductive/nilpotent Lie group is unimodular. ⌟

Proof: The nilpotent case follows directly from(11.10.1.21), as $\det \mathrm{Ad}(x) = \exp(\mathrm{tr}\,\mathrm{ad}(x))$ and $\mathrm{ad}(x)$ is nilpotent. The compact case is by(11.10.1.18). For the semisimple case, $G = [G, G]$ because $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$(3.7.2.4) and it is connected, so we are done by(11.10.1.18). For the reductive case: Cf.[Kna96]P467. □

Convolutions

Def. (11.10.1.23) [Convolution of Measures]. If μ, ν are two complex(hence finite) Radon measures on G, the map

$$I(\varphi) = \int\int \varphi(xy)d\mu(x)d\nu(y)$$

is clearly a linear functional on $C_c(G)$ that satisfies $|I(\varphi)| \leq ||\varphi||_{\sup}||\mu||||\nu||$, so it defines a measure on G by Riesz representation(11.10.1.10), called the **convolution** of μ and ν, denoted by $\mu * \nu$, that $||\mu * \nu|| \leq ||\mu||||\nu||$. ⌟

Prop. (11.10.1.24) [Measure Algebra].

- The convolution of measure is associative.
- $\delta_x * \delta_y = \delta_{xy}$.
- The convolution of measure is commutative iff G is commutative.
- The convolution makes $M(G)$ into a unital Banach algebra, called the **measure algebra** of G.

⌟

Proof: 1: If $\varphi \in C_c(G)$, then

$$\begin{aligned}\int_G \varphi d[\mu * (\nu * \sigma)] &= \int\int \varphi(xy)d\mu(x)d(\nu * \sigma)(y) \\ &= \int\int\int \varphi(xyz)d\mu(x)d\nu(y)d\sigma(z) \\ &= \int\int \varphi(yz)d(\mu * \nu)(y)d\sigma(z)\end{aligned}$$

$$= \int \varphi d[(\mu * \nu) * \sigma]$$

by Fubini theorem, which shows $\mu * (\nu * \sigma) = (\mu * \nu) * \sigma$.

2:
$$\int\int \varphi d(\delta_x * \delta_y) = \int\int \varphi(uv) d\delta_x(u) d\delta_y(v) = \varphi(xy) = \int \varphi d\delta_{xy}.$$

3: If G is commutative, then $\varphi(xy) = \varphi(yx)$, then the commutativity follows from Fubini theorem. The converse follows from item2.

4 It is a Banach algebra because $||\mu * \nu|| \le ||\mu|| ||\nu||$(11.10.1.23). And the point measure δ_1 is the unit:
$$\int \varphi d(\delta * \mu) = \int\int \varphi(xy) d\delta(x) d\mu(y) = \int \varphi(y) d\mu(y)$$
shows $\delta * \mu = \mu$ for any μ, and similarly $\mu * \delta = \mu$, so δ is the identity. □

Prop. (11.10.1.25) [Involution of Measure]. $M(G)$ has a canonical involution that preserves measure:
$$\mu \mapsto \mu^* : \mu^*(E) = \overline{\mu(E^{-1})}.$$
⌟

Proof: μ^* clearly satisfies $||\mu^*|| = \mu^*(G) = \mu(G) = ||\mu||$. And for any $\varphi \in C_c(G)$,
$$\varphi d(\mu * \nu)^* = \int \varphi(x^{-1}) d(\overline{\mu * \nu})(x) = \int \varphi((xy)^{-1}) d\overline{\mu}(x) d\overline{\nu}(y) = \int\int \varphi(yx) d\mu^*(x) \nu^*(y) = \int \varphi d(\nu^* * \mu^*),$$
which shows $(\mu * \nu)^* = \nu^* * \mu^*$. □

Def. (11.10.1.26) [L^1 Group Algebra]. Fix a Haar measure $d\mu$ on G, $L^1(G)$ embeds into the $M(G)$ by identifying f with the measure $f(x)d\mu(x)$, and this is an isometry.

So the convolution and involution can be defined on $L^1(G)$, and the outcome turns out to be a.e. defined and in $L^1(G)$ too:
$$f * g(x) = \int f(y) g(y^{-1}x) dy$$
by Fubini-Tonelli theorem, and the involution
$$f^*(x) = \Delta(x^{-1}) \overline{f(x^{-1})}.$$
⌟

Proof:
$$(f * g)(\varphi) = \int\int \varphi(xy) f(x) g(y) dx dy = \int\int \varphi(y) f(x) g(x^{-1}y) dx dy = \int \varphi(y) (\int f(x) g(x^{-1}y) dx) dy.$$
$$(f d\mu)^* = \overline{(f d\mu)(x^{-1})} = \overline{f(x^{-1})} \Delta(x^{-1}) d\mu(x) \text{(11.10.1.17)}.$$
□

Prop. (11.10.1.27). The convolution $f * g$ can be calculated in multiple ways by left invariance and(11.10.1.17):
$$f * g(x) = \int f(y) g(y^{-1}x) dy = \int f(xy) g(y^{-1}) dy = \int f(y^{-1}) g(yx) \Delta(y^{-1}) dy = \int f(xy^{-1}) g(y) \Delta(y^{-1}) dy.$$
In particular, if G is unimodular, then it can be calculated anyway you want. ⌟

Prop. (11.10.1.28). For $1 \leq p < \infty$, the left and right translations of G on $L^p(G)$ are all continuous. ⌟

Proof: Cf.[Fol15]P58. □

Prop. (11.10.1.29) [L^p-Estimate]. If $1 \leq p < \infty$, $f \in L^1(G)$ and $g \in L^p(G)$, then

- $f * g \in L^p(G)$, and $||f * g||_p \leq ||f||_1 ||g||_p \leq ||f||_p ||g||_p$.
- If G is unimodular or f has compact support, then the same as above holds for $g * f$.

⌟

Proof: 1: By Minkowski's inequality(11.3.6.5),

$$||f * g||_p = |\int f(y) L_y g dy||_p \leq \int |f(y)| ||L_y g||_p dy = ||f||_1 ||g||_p.$$

2: This is similar, using(11.10.1.27). □

Prop. (11.10.1.30) [Convolution].

- Suppose G is unimodular and $f \in L^p(G), g \in L^q(G)$ with $1/p + 1/q = 1, 1 < p < \infty$, then $f * g \in C_0(G)$, and $||f * g||_{sup} \leq ||f||_p ||g||_q$.
- Suppose $f \in L^1(G), g \in L^\infty(G)$, then $f * g$ is left uniformly continuous, and $g * f$ is right uniformly continuous.

⌟

Proof: Cf.[Fol15]P57, P58. □

Prop. (11.10.1.31) [Approximate Identity]. Let $\mathcal{U}$ be a neighborhood base of $1 \in G$. A family of L^∞ functions $\{\varphi_U\}$ are called an **approximate identity** if:

1. $\int_0^1 \Phi_U(x) dx = 1$.
2. $\sup \int_0^1 |\Phi_U(x)| dx < \infty$.
3. For any $\delta > 0$, $\int_{G \setminus U} |\Phi_U(x)| dx \to 0$ as $N \to +\infty$.

For any approximate identity, if $1 \leq p < \infty$ and $f \in L^p(G)$ for $1 \leq p < \infty$, or $p = \infty$ and f is left uniformly continuous, then $\Phi_U * f \to f \in L^p(G)$. ⌟

Proof: Cf.[Fol15]P58. □

Homogenous Spaces

Def. (11.10.1.32) [Notations]. If G is a locally compact group with left Haar measure dx and H is a closed subgroup with left Haar measure $d\xi$, let $q : G \to G/H$ be the quotient map. ⌟

Prop. (11.10.1.33). If G is a σ-compact locally compact group and S is a transitive G-space that is locally compact and Hausdorff, then if $s_0 \in S$ and $\mathrm{Stab}(s_0) = H$, then $G/H \cong S$ as G-spaces. ⌟

Proof: Cf,[Folland P60]. □

Lemma (11.10.1.34). If $E \subset G/H$ is compact, then there is a compact $K \subset G$ that $q(K) = E$. ⌟

Proof: Choose a precompact nbhd V of 1 in G, since q is open, the set $q(xV)$ is an open cover of E, so there are f.m. x_i that $E \subset \cup q(x_i V)$. Then let $K = q^{-1}(E) \cap (\cup x_i \overline{V})$, this will suffice. □

Def. (11.10.1.35) [Fundamental Domain]. A **fundamental domain** for a group Γ acting discontinuously on a locally compact second countable Hausdorff space X is an Borel subset $F \in X$ that:

- $\cup_{\gamma\in\Gamma}\gamma F = \mathcal{H}$.
- if $\gamma \neq 1 \in \Gamma$, then $\gamma F \cap F = \varnothing$.

Then fundamental domains exist. ⌟

Proof: The quotient space $G\backslash\Gamma$ is locally compact second countable, thus there is a countable set of precompact open basis $\{B_i\}$ for $G\backslash\Gamma$, and a countable set of precompact open basis $\{C_i\}$ for X. For each $\overline{x} \in G\backslash\Gamma$, choose $\overline{x} \in B_{i(\overline{x})}$ and choose a preimage $x \in X$ and a nbhd $C_{i(x)}$ that $C_{i(x)} \cap \gamma(C_{i(x)}) = \varnothing$ for any $\gamma \neq 1$, then there is a nbhd $B_{j(x)}$ contained in the image of $C_{i(x)}$. Then we can take a precompact preimages of $B_{j(\overline{x})}$ in $C_{i(x)}$(by(11.10.1.34)), labeled by U_i. Then U_i maps isomorphically to their images in $G\backslash\Gamma$ and covers $G\backslash\Gamma$.

Now take $V_1 = W_1 = U_1$, and $W_{n+1} = U_{n+1}\backslash \cup_{\gamma\in\Gamma} \gamma(V_n), V_{n+1} = V_n \cup W_{n+1}$. Then $\cup V_i$ is a fundamental domain. □

Prop. (11.10.1.36) [Projection of Functions]. There is a map $P : C_c(G) \to C_c(G/H) : Pf(xH) = \int_H f(x\xi)d\mu(\xi)$. Pf is continuous and this map is well-defined and surjective.

And $\mathrm{Supp}(Pf) \subset q(\mathrm{Supp}\, f)$, and if $\varphi \in C_c(G/H)$, then $P((\varphi \circ q)f) = \varphi Pf$. ⌟

Proof: Pf is continuous because f is left uniformly continuous(11.10.1.3). By(11.10.1.37), there is a $g \geq 0 \in C_c(G)$ that $Pg = 1$ on $\mathrm{Supp}\,\varphi$. Let $f = (\varphi \circ f)g$, then $Pf = \varphi(Pg) = \varphi$. □

Lemma (11.10.1.37). If $F \in G/H$ is compact, then there is a $f \in C_c(G)$ that $f \geq 0$ and $Pf = 1$ on F. ⌟

Proof: Let E be a precompact nbhd of F in G/H, choose a compact $K \subset G$ that $q(K) = \overline{E}$ by(11.10.1.34). Choose $g \in C_c(G) \geq 0$ that is positive on K and $\varphi \in C_c(G/H)$ that is 1 on F and vanish outside E, then set

$$f = \frac{\varphi \circ q}{Pg \circ q}g$$

then $f \geq 0$ and $Pf = (\varphi/Pg)Pg = \varphi$. □

Prop. (11.10.1.38) [Quotient Measure Regular Case]. If G is a locally compact group and H is a closed subgroup, then there is a G-invariant positive Radon measure μ on G/H iff $\Delta_G|_H = \Delta_H$. And if this is the case, then this measure is unique up to constant, and if suitably chose, satisfies:

$$\int_G f(x)dx = \int_{G/H} Pf d\mu = \int_{G/H}\int_H f(x\xi)d\xi d\mu(xH).$$

for any $f \in C_c(G)$. ⌟

Proof: Cf.[Folland Abstract Analysis P62]. □

Cor. (11.10.1.39) [Decomposition of Measure]. If G is a unimodular locally compact group and P, K be closed subgroups s.t. $P \cap K$ is compact and $G = PK$. Let d_Lp, d_Rk be the left and right Haar measure on P, K respectively, then a Haar measure on G is given by

$$\int_G f(g)dg = \int_K\int_P f(pk)d_Lpd_Rk.$$

⌟

Proof: Consider $H = P \times K$ and $M = P \cap K$ embedded diagonally in H, then there is a homeomorphism $H/M \cong G$ given by $(p,k) \mapsto pk^{-1}$. Then we can verify both side are H-invariant quotient measure on $G \cong H/M$, so by uniqueness in(11.10.1.38), the equation is true. □

Def. (11.10.1.40) [Rho-Functions]. If G is a locally compact subgroup and H is a closed subgroup. Let $\Delta = \Delta_G/\Delta_H$. Let $\mathcal{S}(G,\Delta)$ be the space of continuous functions on G that satisfies

- for any $h \in H$, $f(hg) = \Delta(h)f(g)$.
- f is compactly supported in $H\backslash G$.

⌟

Lemma (11.10.1.41). Let G be a locally compact group and H a closed subgroup, then there is a continuous function $f_0 : G \to [0,\infty)$ that

- $f_0^{-1}((0,\infty)) \cap Hx \neq \varnothing$ for any $x \in G$.
- Supp $f_0 \cap HK$ is compact for any compact group K of G.

⌟

Proof: Cf.[Folland, P64]. □

Lemma (11.10.1.42). If $f \in C_c(G)$ and $Pf = 0$, then $\int f\rho = 0$ for any rho-function ρ. In fact, this is true if ρ is allowed to take value 0. ⌟

Proof: Cf.[Folland P65]. □

Lemma (11.10.1.43). There is an operator $p : C_c(G) \to C(G)$ given by

$$p(f)(g) = \int_H f(hg)\Delta_G^{-1}(h)d\mu_H(h).$$

Then p is right G-invariant, and $p(ff') = fp(f')$ for any $f' \in C_c(G)$ and $f \in C(G)$ that is H-invariant.

- The image of p is $\mathcal{S}(G,\Delta)$, and if $s \geq 0 \in S(G,\Delta)$, then there is a non-negative $f \geq 0 \in C_c(G)$ that $p(f) = s$.
- If $p(f) = 0$, then $\int_G f(x)d\nu_G(x) = 0$, where $d\nu_G$ is a right Haar measure on G.

⌟

Proof: 1: It is clearly that $p(f)(gh) = \Delta(h)p(f)(g)$, and let f_0 be defined as in(11.10.1.41), then $s_0 = p(f_0)$ is positive-valued. Now for any $s \in \mathcal{S}(G,\Delta)$, $p(ss_0^{-1}f_0) = ss_0^{-1}p(f_0) = s$, and $sf_0 \in C_c(G)$ by hypothesis.

2: If $p(f) = 0$, then

$$\begin{aligned}\int_G\int_H s_0^{-1}(g)f_0(g)f(hg)\Delta_G^{-1}(h)d\mu_H(h)d\nu_G(g) &= \int_G\int_H \Delta(h)s_0^{-1}(g)f_0(h^{-1}g)f(g)d\mu_H(h)d\nu_G(g)\\ &= \int_G[\int_H f_0(hg)\Delta_G(h)^{-1}d\mu_H(h)]s_0^{-1}(g)f(g)d\nu_G(g)\\ &= \int_G f(g)d\nu_G(g)\end{aligned}$$

□

Prop. (11.10.1.44) [Haar Measure on Rho-Functions]. There exists a unique continuous positive functorial $\nu_{H\backslash G}$ on $S(G,\Delta)$ that for any $f\in C_c(G)$,

$$\int_G f(x)d\nu_G(x)=\int_{H\backslash G}p(f)(y)d\nu_{H\backslash G}(y)=\int_{H\backslash G}\int_H f(hg)\Delta_G^{-1}(h)d\mu_H(h)d\nu_{H\backslash G}.$$

and it is invariant under the right action of G. We denote $\nu_{H\backslash G}(s)=\int_{H\backslash G}s(g)d\nu_{H\backslash G}(g)$ for $s\in S(G,\Delta)$. ⌟

Proof: This follows from(11.10.1.43). □

Cor. (11.10.1.45). If G is a unimodular locally compact group and H,K be closed subgroups s.t. $H\cap K$ is compact and $G=PK$, then the the quotient measure $\mu_{H\backslash G}$ is given by

$$f\mapsto\int_K f(k)d\nu_K(k).$$

where $d\mu_K(k)$ is a right Haar measure on K, by comparison with(11.10.1.39). ⌟

Maximal Compact Subgroup

Def. (11.10.1.46) [Maximal Compact Subgroup]. A **maximal compact subgroup** of a locally compact group G is a maximal object in the set of all compact subgroup of G. ⌟

Prop. (11.10.1.47) [Cartan-Iwasawa-Malcev theorem]. Maximal compact subgroup exists for any locally compact group G. ⌟

Proof: □

Locally Profinite Groups

Def. (11.10.1.48) [Locally Profinite Group]. A **locally profinite group** is a locally profinite topological group. A profinite group is locally profinite, and any compact open subgroup of a locally profinite group is profinite. ⌟

Cor. (11.10.1.49). A closed subgroup of a locally profinite group is locally profinite, and a quotient group is locally profinite. ⌟

Proof: The proof is very similar to that of(3.1.13.4), as the result of(4.4.1.25) remains true, because any connected nbhd of e is contained in any compact open subgroup. □

Prop. (11.10.1.50) [Compact Open Subgroups Form a Basis]. If G is a locally profinite group, then the set of compact open subgroups form a basis of the nbhd of 1. ⌟

Proof: For any nbhd U of 1, choose a precompact nbhd V of 1 contained in U, then there is another compact open subgroup contained in V, by(4.12.1.24). □

Prop. (11.10.1.51) [Quotient of Locally Profinite Group]. A quotient subspace of a locally profinite group is locally profinite. ⌟

Proof: Consider the H action on G, then it is regular, because the graph is the preimage of H in the map $G\times G\to G:(g_1,g_2)\mapsto g_1^{-1}g_2$. So by(4.12.1.10) G/H is Hausdorff. But clearly $G\to G/H$ is open and G/H is locally profinite as it has a basis of locally compact subsets. □

Lemma (11.10.1.52). Let G be a locally profinite group and H a closed subgroup, then for any open compact subspace $V \subset G/H$, there is an open compact subspace $U \subset G$ that $p(U) = V$. ⌟

Proof: The preimage $p^{-1}(V)$ is open, so there is a covering of $p^{-1}(V)$ by open compact subsets U_i. Then $p(U_i)$ are open and covers V, thus there are f.m. U_i that $p(\cup U_i) = V$. □

Prop. (11.10.1.53) [Homogeneous Group]. Let G is a locally profinite group that is σ-compact. If G acts transitively on a locally profinite space X, let $x_0 \in X$ and $\mathrm{Stab}(x_0) = H$, then $G/H \to X$ is a homeomorphism. ?Is this true for locally compact groups? ⌟

Proof: Let N be a compact open subset of N, and g_i be the left coset representatives for N, which is countable. Now $X = \cup_i \gamma(g_i N)x_0$. Because a locally profinite space is a Baire space, some $\gamma(g_i N)x_0$ contains a nbhd of $\gamma(g_i n)x$. Now left acts $(g_i n)^{-1}$, we see x_0 is an interior point of $\gamma(N)x_0$. Now N is arbitrary, thus(11.10.1.50) shows $g \mapsto \gamma(g)x$ is open, thus $G/H \to X$ is open. It is clearly continuous, thus $G/H \cong X$. □

2 Unitary Representations

Def. (11.10.2.1) [Intertwining Operators]. if π_1, π_2 are unitary representations of G, then the space $C(\pi_1, \pi_2)$ of **intertwining operators** of π_1, π_2 as:

$$C(\pi_1, \pi_2) = \{T : \mathcal{H}_{\pi_1} \to \mathcal{H}_{\pi_2} : T\pi_1(x) = \pi_2(x)T, \quad \forall x \in G\}.$$

And denote $C(\pi_1, \pi_1)$ by $C(\pi_1)$. ⌟

Lemma (11.10.2.2). The adjoint operator $S \mapsto S^*$ induces a bijection between the spaces $C(\pi_1, \pi_2) \cong C(\pi_2, \pi_1)$. ⌟

Lemma (11.10.2.3). If $\mathcal{H}_\pi$ is a representation of G, M is a closed subspace. Let P be the orthogonal projection onto M, then M is invariant under π iff $P \in C(\pi)$. ⌟

Proof: If $P \in C(\pi)$ and $v \in M$, then $\pi(x)v = \pi(x)Pv = P\pi(x)v \in M$, so M is π-invariant. Conversely if M is π-invariant, then so does $M^\perp$, so $\pi(x)Pv = \pi(x)v = P\pi(x)v$, and also for $v \in M^\perp$, so $\pi(x)P = P\pi(x)$, for any x. □

Prop. (11.10.2.4) [Schur's Lemma].

- A unitary representation π of G is irreducible iff $C(\pi)$ consists only of scalar multiples of identity.
- If π_1, π_2 are non-equivalent irreducible unitary representations of G, then $C(\pi_1, \pi_2) = 0$.

⌟

Proof: 1: if π is reducible, then it contains a non-trivial projection by lemma(11.10.2.3). Conversely, if $T \neq cI \in C(\pi)$, then we consider $A = \frac{1}{2}(T + T^*), B = \frac{1}{2i}(T - T^*)$, then at least one of them are not cI. But they are normal, thus by symbolic calculus(11.9.4.3) any $\chi_E(A)$ for some $E \subset \mathbb{R}$ Borel is non-trivial(because the spectrum of A is not a single point) and commutes with π, so $\mathcal{H}_\pi$ is reducible by(11.10.2.3) again.

2: By(11.10.2.2), for $T \in C(\pi_1, \pi_2)$, $T^* \in C(\pi_2, \pi_1)$, $TT^* = cI, T^*T = cI$. so $T = 0$ or $c^{-1/2}T$ is unitary, and it is an isomorphism between π_1, π_2. □

Cor. (11.10.2.5). if G is Abelian, then any irreducible representation of G is 1-dimensional. ⌟

Proof: If π is a representation of G, then any $\pi(x)$ commutes with π, thus $\pi(x) = c_x I$ for some c_x, so every subspace of $\mathcal{H}_\pi$ is irreducible, thus $\dim \mathcal{H} = 1$. □

Prop. (11.10.2.6) [Unitary Representation and $L^1(G)$-Representation]. Any unitary representation $(\pi, \mathcal{H})$ of G determines a representation of $L^1(G)$ by

$$f \mapsto \int f(x)\pi(x)dx$$

This is a non-degenerate *-representation of $L^1(G)$.

And conversely, any non-degenerate *-representation of $L^1(G)$ arises from a unitary representation of G. ⌟

Proof: If π is a unitary representation and $f \in L^1$, let $\pi(f)$ be defined as

$$\pi(f)u = \int f(x)\pi(x)udx,$$

where the integral is in the weak sense(11.8.3.25), and it satisfies $||\pi(f)|| \leq ||f||_1$.

For the $*$-algebra structure(11.10.1.26), it suffices to prove that

$$\pi(f * g) = \pi(f)\pi(g), \quad \pi(f^*) = \pi(f)^*,$$

which are true for formal reason:

$$\pi(f * g) = \int\int f(y)g(y^{-1}x)\pi(x)dydx = \int\int f(y)g(x)\pi(yx)dxdy = \pi(f)\pi(g),$$

$$\pi(f^*) = \int \Delta(x^{-1})\overline{f(x^{-1})}\pi(x)dx = \int \overline{f(x)}\pi(x^{-1})dx = \int (f(x)\pi(x))^* dx = \pi(f)^*.$$

and verified by supplying u, v. For the non-degeneracy, for any $u \neq 0 \in \mathcal{H}$, choose a precompact nbhd V of identity that $||\pi(x)u - u|| < ||u||$ for $x \in V$, and let $f = |V|^{-1}\chi_V$, then it can be verified that $||\pi(f)u|| \neq 0$.

For the converse, Cf.[Folland P79-81]? □

Prop. (11.10.2.7). We want to consider the difference of the image of $L^1(G)$ and G under these two representations: Let π be a unitary representation of G, then

- The bicommutant(11.16.1.2) of $\pi(G)$ and $\pi(L^1(G))$ are identical.
- $T \in \mathcal{L}(\mathcal{H})$ intertwines π iff it commutes with every $\pi(f) \in \pi(L^1(G))$.
- A closed subspace M of $\mathcal{H}$ is invariant under π iff $\pi(f)M \subset M$ for any $f \in L^1(G)$.

⌟

Proof: 1: Cf.[Folland, P82].

2 follows from 1 noticing the fact that T commutes with an algebra iff it commutes with its von-Neumann algebra.

3 follows from 2 and(11.10.2.3). □

Prop. (11.10.2.8) [Completion of Unitary Representation]. If $\mathcal{H}_0$ is a Hermitian inner product space that G is a topological group acting continuously on $\mathcal{H}_0$ that preserves the inner product, then if $\mathcal{H}$ is the Hilbert completion of $\mathcal{H}_0$, then the action of G extends to a continuous unitary action on $\mathcal{H}$. ⌟

Proof: The extension is clear as $||\pi(g)f|| = ||f||$. For the continuity, if $v \in \mathcal{H}, g \in G, \varepsilon > 0$, let $v_0 \in \mathcal{H}_0$ that $|v-v_0| < \varepsilon/6$, then there is a nbhd W of g that if $g_1 \in W$, then $|\pi(g_1)v_0 - \pi(g)v_0| < \varepsilon/3$.

Then if $|v_1 - v| < \varepsilon/6$ and $g_1 \in W$, then

$$\begin{aligned}
|\pi(g_1)v_1 - \pi(g)v| &= |\pi(g_1)v_1 - \pi(g_1)v_0 + \pi(g_1)v_0 - \pi(g)v_0 + \pi(g)v_0 - \pi(g)v| \\
&\leq |\pi(g_1)v_1 - \pi(g_1)v_0| + |\pi(g_1)v_0 - \pi(g)v_0| + |\pi(g)v_0 - \pi(g)v| \\
&= |v_1 - v_0| + |\pi(g_1)v_0 - \pi(g)v_0| + |\pi(g)v_0 - \pi(g)v| \\
&\leq \varepsilon
\end{aligned}$$

which shows the action is continuous. □

Cor. (11.10.2.9). Given a locally compact group G and a discrete subgroup Γ, the right regular action of G extends to a continuous unitary representation of G on $L^2(\Gamma\backslash G, \omega)$. ⌟

Proof: Because we can approximate $f \in L^2(\Gamma\backslash G)$ by compactly supported continuous functions(11.3.8.6), then the G action is uniformly continuous. □

Lemma (11.10.2.10) [Auxiliary Compact Supported Function Approximation]. Let G be a locally compact Lie group and K a compact subgroup. If $(\pi, \mathcal{H})$ is a unitary representation of G on a Hilbert space, and let $f \neq 0 \in \mathcal{H}$, then for any $\varepsilon > 0$, there is a $\varphi \in C_c^\infty(G)$ s.t. $\pi(\varphi)$ is self-adjoint and $|\varphi(\rho)f - f| < \varepsilon$.

Moreover, if $f \in \mathcal{H}^\xi$ which is the decomposition part for K, we can assume $\varphi(kg) = \varphi(gk) = \xi(k)^{-1}\varphi(g)$. In particular if $\mathcal{H}^\xi$ is f.d., we find a φ that $\pi(\varphi)f = f$. ⌟

Proof: By continuity, there is a nbhd H of 1 that $|\pi(g)f - f| < \varepsilon$, then we can choose a φ positive real valued with support in U with integral 1, then $|\pi(\varphi)f - f| < \varepsilon$ by(11.8.3.22). We can also choose $\varphi(g) = \varphi(g^{-1})$, then $\pi(\varphi)$ is self-adjoint.

For the second case, notice first there is a nbhd V of 1 that $kVk^{-1} \in U$ for any $k \in K$(4.12.1.6), so let φ_1 be a positive real valued function supported in V, and let

$$\varphi_0(g) = \int_K \varphi_1(kgk^{-1})dk$$

then φ_0 is supported in U and $\varphi(kgk^{-1}) = \varphi_0(g)$ for any $k \in K$. Assume now that $\pi(k_\theta) = e^{ik\theta}f$, then we can use(11.10.1.39) for $P = G$ to see that

$$\pi(\varphi_0)f = \int_G \varphi_0(h)\pi(h)f dh = \int_G \int_K \varphi_0(hk)\pi(hk)f dk dh = \int_G \int_K \xi(k)\varphi_0(hk)dk\pi(h)f dh = \pi(\varphi)f$$

where

$$\varphi(g) = \int_K \xi(k)\varphi_0(gk)dk = \int_K \xi(k)\varphi_0(kg)dk$$

so $\varphi(k) = \varphi(gk) = \xi^{-1}(k)\varphi(g)$ as required. □

Functions of Positive Type

Def. (11.10.2.11)[Positive Type Function]. A function of **positive type** on a closed compact group G is a function $\varphi \in L^\infty(G)$ that defines a positive linear functional on the B^*-algebra $L^1(G)$. In other word,

$$\int f(x)\overline{f(y)}\varphi(y^{-1}x)dydx \geq 0, \quad \forall f \in L^1(G).$$

We denote by $P(G)$ the set of continuous functions of positive type on G. ⌟

Prop. (11.10.2.12). If φ is of positive type, then so does $\overline{\varphi}$. (Easy calculation). ⌟

Prop. (11.10.2.13). If π is a unitary representation of G and $u\in\mathcal{H}_\pi$, then $\varphi(x)=(\pi(x)u,u)\in P$. ⌟

Proof: φ is continuous by definition, so if $f\in L^1$, then

$$\int\int f(x)\overline{f(y)}\varphi(y^{-1}x)d\mu(x)d\mu(y)=\int\int(f(x)\pi(x)u,f(y)\pi(y)u)dxdy=||\pi(f)u||^2\leq 0$$

□

Prop. (11.10.2.14). If $f\in L^2(G)$, then $f*\widetilde{f}\in P(G)$(11.10.1.2). ⌟

Proof: Cf.[Folland, P84]. □

Prop. (11.10.2.15) [Cyclic Representations and Functions of Positive Type]. Any function of positive type arises from a irreducible representation and a cyclic vector ε as in(11.10.2.13) ⌟

Proof: Cf.[Folland P84-85]. □

Cor. (11.10.2.16). If φ is a function of positive type, then φ can be chosen to be continuous. ⌟

Cor. (11.10.2.17). If $\varphi\in P$, then $||\varphi||_\infty=\varphi(1)$, and $\varphi(x^{-1})=\overline{\varphi(x)}$. ⌟

Proof: $\varphi(x)=(\pi(x)u,u)$ for some representation π and $u\in\mathcal{H}$, so $|\varphi(x)|\leq||u||^2=\varphi(1)$ and $\varphi(x^{-1})=(\pi(x^{-1})u,u)=(u,\pi(x)u)=\overline{\varphi(x)}$. □

Def. (11.10.2.18). We set:

- $P_0(G)=\{\varphi|||\varphi||_\infty\leq 1\}=\{\varphi(1)=1\}$.
- $P_1(G)=\{\varphi|||\varphi||_\infty=1\}=\{0\leq\varphi(1)\leq 1\}$.

By Banach-Alaoglu, $P_0(G)$ and $P_1(G)$ are a weak*-compact set. ⌟

Prop. (11.10.2.19) [Extreme Points of P_1]. A $\varphi\in P_1$ is an extreme point iff the representation it corresponds is irreducible. And $E(P_0)=E(P_1)\cup\{0\}$. ⌟

Proof: Cf.[Folland P86]. □

Prop. (11.10.2.20) [Two Topologies Coincide]. On P_1, the compact-open topology coincides with that of the weak*-topology. ⌟

Proof: Cf.[Folland Abstract Harmonic Analysis P80]. □

Prop. (11.10.2.21). The linear span $B(G)$ of $C_c(G)\cap P(G)$ includes all functions of the form $f*g$ where $f,g\in C_c(G)$. And it is dense in $C_c(G)$ and $L^p(G)$ for $p<\infty$.

Denote $B^p(G)=B(G)\cap L^p(G)$. ⌟

Proof: By(11.10.2.14), $P\cap C_c(G)$ includes all functions of the form $f*\widetilde{f}$ with $f\in C_c(G)$, thus its linear span includes all $f*g$ for $f,g,\in C_c(G)$ by polarization. Thus it is dense in $C_c(G)$ and $L^p(G)$ because we can use approximate identity(11.10.1.31). □

Prop. (11.10.2.22) [Gelfand-Raikov]. If G is a locally compact group, then the irreducible representations of G separate points of G. ⌟

Proof: Cf.[Folland Abstract Analysis P91]. □

3 Locally Compact Abelian Group

Dual Group

Def. (11.10.3.1) [Dual Space]. If G is locally compact, denote $\widehat{G}$ the set of all irreducible unitary representations of G, called the **dual space** of G. ⌟

Def. (11.10.3.2)[Dual Group]. If G is locally compact Abelian, the irreducible unitary representations of G are all 1-dimensional by(11.10.2.5), so it forms a group, called the **dual group** of G, denoted by $\widehat{G}$.

An element of $\widehat{G}$ is called a **character of** G, denoted by ξ. And a continuous homomorphism from G to $\mathbb{C}$ is called a **quasi-character**.

The topologies on $\widehat{G}$ that makes it into a LCA group is given in(11.10.3.6). ⌟

Remark (11.10.3.3). $\widehat{\mathbb{R}}\cong\mathbb{R}$, and the quasi-characters of $\mathbb{R}$ are all of the form $x\to e^{sx}$ for $s\in\mathbb{C}$. ⌟

Proof: If $\varphi\in\widehat{\mathbb{G}}$, then $\varphi(0)=1$, and there is an $a>0$ that $\int_0^a\varphi(t)dt\neq 0=A$. Now $A\varphi(x)=\int_x^{x+a}\varphi(t)dt$, so taking derivative,

$$\varphi'(x)=\frac{\varphi(x+a)-\varphi(x)}{A}=\frac{\varphi(a)-1}{A}\varphi(x),$$

which shows $\varphi(x)=e^{sx}$ for some $s\in\mathbb{C}$. □

Prop. (11.10.3.4) [Dual Group as Spectrum of $L^1(G)$]. The dual group $\widehat{G}$ can be regarded as the spectrum of $L^1(G)$, i.e. multiplicative homomorphism of $L^1(G)$:

$$\xi\mapsto\Big(\xi(f)=\int\overline{(x,\xi)}f(x)dx\Big).$$

⌟

Proof: First, ξ is multiplicative because

$$\xi(f*g)=\int\int f(y)g(y^{-1}x)(x,\xi)dydx=\int\int f(y)g(x)(xy,\xi)dydx=\xi(f)\xi(g).$$

Conversely, any continuous functional on L^1 is like $\varphi(f)=\int f(x)\varphi(x)dx$ for some $\varphi\in L^\infty$, and it is multiplicative, so

$$\varphi(f)\int\varphi(x)g(x)=\varphi(f)\varphi(g)=\varphi(f*g)=\int\int\varphi(y)f(yx^{-1})g(x)dxdy=\int\varphi(L_x(f))g(x)dx$$

So $\varphi(x)=\frac{\varphi(L_x(f))}{\varphi(f)}$, a.e., for any f. so $\varphi(x)$ can be chosen to be continuous, as $x\to L_x(f)$ is continuous(11.10.1.3). And clearly φ is multiplicative. □

Cor. (11.10.3.5). $\widehat{G}\subset P_1(G)$, because $\int(f^**f)\varphi\mathrm{d}\mu=|\Phi(f)|^2\geq 0$. ⌟

Cor. (11.10.3.6) [Dual Group as a LCA Group]. Now we can give $\widehat{G}$ the compact-open topology, then the group operation is clearly continuous, and the topology coincides with that inherited by the weak*-topology of the L^∞ by(11.10.2.20), so $\widehat{G}\cup\{0\}$ is a compact Hausdorff space because $\widehat{G}\subset P_1(G)$ and it is the subset of L^∞ that $\{h(xy)=h(x)h(y)\}$ which is weak*-closed hence weak*-compact. In particular, $\widehat{G}$ is a locally compact topological group. ⌟

Prop. (11.10.3.7) [Duality between Discrete Groups and Compact Groups]. if G is discrete, then $G^\vee$ is compact, if G is compact, then $G^\vee$ is discrete. ⌟

Proof: if G is discrete, then there is a unit δ in $L^1(G)$, which is 1 on e and 0 otherwise. So the spectrum of $L^1(G)$ is compact by(11.9.1.21).

If G is compact, then $1 \in L^1$, so $U = \{f \in L^\infty ||f| > \frac{1}{2}\}$ is weak*-open, but $U \cap \widehat{G} = \{1\}$ by(11.10.1.14), so $\widehat{G}$ is discrete. □

Fourier Transform

Prop. (11.10.3.8) [Fourier Transforms]. The **Fourier transform** on G is defined as in(11.10.3.4) to be the map

$$L^1(G) \to C(G^\vee) : f \mapsto \mathcal{F}f(\xi) = \widehat{f}(\xi) = \int f(x)\overline{(x,\xi)}.$$

It is a norm-decreasing *-homomorphism form $L^1(G)$ to $C_0(\widehat{G})$, and its range is a dense subspace of $C_0(G^\vee)$.

Equivalently, the Fourier transform is just the Gelfand transform of $L^1(G)$(11.9.1.21) composed with an inverse map. ⌟

Proof: Cf.[Folland Abstract Harmonic Analysis P102]. □

Prop. (11.10.3.9). There is another map from $M(\widehat{G})$ to bounded continuous functions on G:

$$\mu \mapsto \Big(\varphi_\mu : x \mapsto \int (x,\xi) d\mu(\xi)\Big).$$

This is a norm decreasing injection from $M(\widehat{G})$ to $L^\infty(G)$, and if μ is positive, then φ_μ is a function of positive type. ⌟

Proof: It suffices to prove injectivity, but if $\varphi_\mu = 0$, then $0 = \int\int f(x)(x,\xi)d\mu(\xi)dx = \int \widehat{f}(\xi^{-1})d\mu(\xi)$ for all $f \in L^1(G)$, so but this shows $\mu = 0$ because of(11.10.3.8) and Riesz representation.

For the positive type, notice that

$$\int\int f(x)\overline{f(y)}vp_\mu(y^{-1}x)dxdy = \int\int\int f(x)\overline{f(y)(y,\xi)}(x,\xi)d\mu(\xi)dxdy = \int |\widehat{f}(\xi)|^2 d\mu(\xi) \geq 0$$

□

Prop. (11.10.3.10) [Bochner's Theorem]. If $\varphi \in P(G)$, there is a unique positive $\mu \in M(\widehat{G})$ s.t. $\varphi = \varphi_\mu$. ⌟

Proof: We have the map defined in(11.10.3.9) injects $M(\widehat{G})$ into $P(G)$(norm-decreasing), so it suffices to prove the existence. For this, we may assume $\varphi \in P_0(G)$. Let M_0 be the set of positive measure $\mu \in M(\widehat{G})$ that $\mu(\widehat{G}) \leq 1$, then M_0 is weak*-compact in $M(\widehat{G})$. Now

$$\int f(x)\varphi_\mu(x)dx = \int\int f(x)d\mu(\xi)dx = \int \widehat{f}(\xi^{-1})\mu(x)$$

so the mapping $\mu \to P_0$ must be continuous w.r.t their weak*-topologies, so the image is a compact convex subset of P_0. But the image contains all characters and 0(by taking the point mess), which are the extreme points of P_0, by(11.10.2.19), so it contains all the P_0, by Krein-Milman(11.8.3.15). □

Cor. (11.10.3.11). $\{\varphi_\mu\} = B(G)$(11.10.2.21), by(11.10.3.10) and(11.10.3.9). Thus the inverse $B(G) \to M(\overline{G})$ is denoted by $f \mapsto d\mu_f$. ⌟

Cor. (11.10.3.12) [Herglotz]. A numerical sequence $\{a_n\}$ is positive iff there is a positive measure $\mu \in M(T)$ s.t. $a_n = \widehat{\mu}(n)$. ⌟

Prop. (11.10.3.13). The set of regular Borel probability measures on a compact X is weak*-compact in $C(X)^*$. (Use Alaoglu). ⌟

Prop. (11.10.3.14) [Fourier Inversion Formula]. (special case of(11.10.3.24)) If $f \in B^1(G)$(11.10.2.21), then $\widehat{f} \in L^1(\widehat{G})$, and if the Haar measure $d\xi$ of $\widehat{G}$ is suitably normalized w.r.t. the Haar measure of G, then $d\mu_f(\xi) = \widehat{f}(\xi)d\xi$(11.10.3.11), i.e. $f(x) = \int (x,\xi)\widehat{f}(\xi)d\xi$. This measure $d\xi$ is called the **dual measure** of dx. ⌟

Proof: Cf.[Folland Abstract Harmonic Analysis P105].? □

Cor. (11.10.3.15). If $f \in L^1(G) \cap P$, then $\widehat{f} \geq 0$, as $d\mu_f(\xi) = \widehat{f}(\xi)d\xi$ and μ_f is positive, by Bochner's theorem(11.10.3.10). ⌟

Prop. (11.10.3.16) [Dual Measure of Discrete Group]. If μ is the counting measure on a discrete group, then its dual measure satisfies $|\widehat{G}| = 1$, and if G is compact and $|G| = 1$, then the dual measure is the counting measure on $\widehat{G}$. ⌟

Proof: First(11.10.3.7) should be noticed. If G is compact and $|G| = 1$, then if $g = 1$, then $\widehat{g} = \chi_{\{1\}}$, so $g(x) = \sum (x,\xi)\widehat{g}(\xi)$, which shows the dual measure is counting measure by definition(11.10.3.14). □

Prop. (11.10.3.17)[Plancherel Theorem]. The Fourier transform on $L^1(G) \cap L^2(G)$ extends uniquely to an isomorphism from $L^2(G)$ to $L^2(\widehat{G})$ that satisfies Fourier inversion formula. ⌟

Proof: Cf.[Folland P108]. □

Cor. (11.10.3.18). If G is compact and $\mu(G) = 1$, then $\widehat{G}$ is an orthonormal basis of $L^2(G)$. ⌟

Proof: Firstly $\widehat{G}$ is an orthonormal set by(11.10.1.14). And if $f \in L^2(G)$ is orthogonal to all $\xi \in \widehat{G}$, then $\int_G f\overline{\xi} = \widehat{f}(\xi) = 0$, thus $\widehat{f} = 0$, and then $f = 0$ by Plancherel(11.10.3.17). □

Cor. (11.10.3.19) [Hausdorff-Young Inequality]. Let $1 \leq p \leq 2$ and $p^{-1} + q^{-1} = 1$. If $f \in L^p(G)$, then $\widehat{f} \in L^q(G)$, and $||\widehat{f}||_q \leq ||f||_p$. ⌟

Proof: Cf.[Folland, P109]. □

Schrödinger Representations

Def. (11.10.3.20) [$A(G)$]. Let G be an locally compact Abelian group, denote $\mathbb{T} = \{c \in \mathbb{C} \mid |c| = 1\}$, $A(G) = G^* \times G \times \mathbb{T}$ with the group law

$$(v_1^*, v_1, t_1)(v_2^*, v_2, t_2) = (v_1^* + v_2^*, v_1 + v_2, t_1 t_2 \langle v_1, v_2^* \rangle).$$

Also we denote for $w, w' \in G^* \times G$, $[w, w'] = \langle v_1, v_2^* \rangle$.

Let $B(G) = \mathrm{Aut}(A(G))$, $B_0(G) \subset B(G)$ be the group of elements fixing elements in the center $Z(A(G))$.

Note the commutator

$$(v_1^*, v_1, 1)(v_2^*, v_2, 1)(v_1^*, v_1, 1)^{-1}(v_2^*, v_2, 1)^{-1} = (0, 0, \langle v_1, v_2^*\rangle\langle v_2, v_1^*\rangle^{-1}),$$

thus $\langle v_1, v_2^*\rangle\langle v_2, v_1^*\rangle^{-1}$ defines a multiplicative skew-symmetric, bilinear and perfect pairing $[\cdot,\cdot]$ of $G^* \times G$ with itself, ⌟

Prop. (11.10.3.21) [Segal-Shale-Weil]. There is an unitary representation of $A(G)$ on $L^2(G)$ given by

$$(\rho(v^*, v, t)\Phi)(u) = t\langle u, v^*\rangle\Phi(u + v),$$

called the **Schrödinger representation**. In fact, it is the induced representation $\mathrm{Ind}_{G\times\mathbb{T}}^{A(G)}\chi$, where $\chi(g, t) = t$. This representation is irreducible, and for any $\sigma \in B_0(G)$, there exists uniquely up to scalar a unitary operator $\omega(\sigma)$ on $L^2(G)$ s.t.

$$\rho(\sigma(h)) = \omega(\sigma) \circ \rho(h) \circ \omega(\sigma)^{-1}.$$

⌟

Remark (11.10.3.22). This should be a direct consequence of the Stone-Von Neumann theorem. Cf.[History of Stone Von-Newmann Theorem] or [Easy proof of the Stone-Von Neumann Theorem].**?** ⌟

Proof: This is clearly a unitary representation. ρ induces an action of $G^* \times G$ on $L^2(G)$ via $t = 1$, thus an action of $C_c(G^* \times G)$ on $L^2(G)$:

$$(\rho(\varphi)\Phi)(u) = \int_{G^*\times G} \varphi(w)(\rho(w, 1)\Phi)(u)dw = \int_G K_\varphi(u, v)\Phi(v)dv$$

where $K_\varphi(u, u + v) = \int_{G^*} \varphi(v^*, v)\langle u, v^*\rangle dv^*$ is the Fourier transform of φ w.r.t. G^*. As Fourier transform is L^2-isometry, $\varphi \mapsto K_\varphi$ extends to an isometry $\lambda : L^2(G^* \times G) \cong L^2(G \times G)$, whose inverse is given by

$$\varphi(v^*, v) = \int_G K_\varphi(u, u + v)\langle -u, v^*\rangle du,$$

and also the action ρ extends to all $\varphi \in L^2(G^* \times G)$.

It can be verified that $\rho(\varphi_1) \circ \rho(\varphi_2) = \rho(\varphi_1 \star \varphi_2)$, where

$$(\varphi_1 \star \varphi_2)(w) = \int_{G^*\times G} \varphi_1(w_1)\varphi_2(w - w_1)[w_1, w - w_1]dw_1.$$

Then by comparison with the equation above, $K_{\varphi_1\star\varphi_2} = K_{\varphi_1} \star K_{\varphi_2}$, where $\star$ is defined in(11.3.6.6).

$\sigma \in B_0(G)$ is of the form $\sigma(w, t) = (s(w), f(w)t)$, where $w \in G^* \times G$, $f : G^* \times G \to \mathbb{T}$ is a map satisfying

$$f(w_1 + w_2) = f(w_1)f(w_2)[s(w_1), s(w_2)][w_1, w_2]^{-1}.$$

Notice s preserves Haar measure on $G^* \times G$: it is preserved the pairing $[\cdot,\cdot]$ as it is a commutator and σ fixes $Z(A(G))$. Thus s preserves Haar measure of $G^* \times G$, by(11.10.3.34).

Now we define a unitary transformation Σ of $L^2(G^* \times G)$ by $(\Sigma\varphi)(w) = f(w)^{-1}\varphi(s(w))$, then it can be checked**?** by using the equations above that

$$\Sigma(\varphi_1 \star \varphi_2) = \Sigma(\varphi_1) \star \Sigma(\varphi_2).$$

Thus by the isomorphism $\lambda : L^2(G^* \times G) \cong L^2(G \times G)$, Σ induces a unitary transformation on $L^2(G \times G)$, also denoted by Σ and it preserves $\star$. Then by(11.3.6.7), there is a unitary map $\omega : L^2(G) \to L^2(G)$ that
$$\Sigma(P \otimes \overline{Q}) = \omega^{-1}(P) \otimes \overline{\omega^{-1}Q}.$$

Next, notice for any $(w,t) \in A(G)$,

$$\bar{t}\lambda^{-1}(P \otimes Q)(w) = \int_G P(u)\overline{tQ(u+v)\langle u, v^*\rangle}du = (P, \rho(w,t)Q)_{L^2},$$

thus

$$\begin{aligned}(P, \rho(\sigma(w,t)))_{L^2} &= (P, \rho(s(w), f(t))Q)_{L^2} = \overline{tf(w)}\lambda^{-1}(P \otimes \overline{Q})(s(w))\\ &= \bar{t}(\Sigma\lambda^{-1}(P \otimes \overline{Q}))(w) = \bar{t}\lambda^{-1}(\omega^{-1}(P) \otimes \omega^{-1}(Q))(w)\\ &= (\omega^{-1}(P), \rho(w,t)\omega^{-1}(Q))_{L^2}\\ &= ((P), \omega\rho(w,t)\omega^{-1}(Q))_{L^2}\end{aligned}$$

Because P, Q are arbitrary, this means $\rho(\sigma(w,t)) = \omega(\sigma) \circ \rho(w,t) \circ \omega(\sigma)^{-1}$.

It remains to show that ρ is irreducible: For any endomorphism of $L^2(G)$ commuting with ρ, it commutes with $\rho(\varphi)$ for any $\varphi \in L^2(G^* \times G)$. Take $\varphi = \lambda^{-1}(P \otimes \overline{Q})$, where $P, Q \in L^2(G)$, then $\rho(\varphi)\Phi = (\Phi, Q)_{L^2}P$, so $(T\Phi, Q)_{L^2}P = (\Phi, Q)_{L^2}TP$. Then T is a scalar. □

Pontryagin Duality

Prop. (11.10.3.23) [Pontryagin Duality]. For a locally compact Abelian group G, $G \to (G^\wedge)^\wedge$ is an isomorphism of topological groups. ⌟

Proof: Cf.[Folland Abstract Harmonic Analysis P110]. □

Cor. (11.10.3.24) [Fourier Inversion Theorem]. If $f \in L^1(G)$ and $\widehat{f} \in L^1(\widehat{G})$ and the measure are dual to each other(11.10.3.14), then $f(x) = \widehat{\widehat{f}}(x^{-1})$, i.e. $f(x) = \int(x,\xi)\widehat{f}(\xi)d\xi$ a.e.. ⌟

Proof: As
$$\widehat{f}(\xi) = \int \overline{(x,\xi)}f(x)dx = \int(x^{-1},\xi)f(x)dx = \int(x,\xi)f(x^{-1})dx,$$
so by definition $\widehat{f} \in B^1(\widehat{G})$, and $d\mu_{\widehat{f}}(x) = f(x^{-1})dx$. Then by(11.10.3.14), $f(x^{-1}) = (f^\wedge)^\wedge(x)$. □

Cor. (11.10.3.25) [Fourier Uniqueness Theorem]. If $u, v \in M(G)$ satisfy $\widehat{u} = \widehat{v}$, then $u = v$. In particular, if $f, g \in L^1(G)$ and $\widehat{f} = \widehat{g}$, then $f = g$. ⌟

Proof: By(11.10.3.9)(norm decreasing), μ is uniquely determined by $\varphi_\mu(\xi) = \widehat{\mu}(\xi^{-1})$ by Fourier inversion. □

Lemma (11.10.3.26). If $\varphi, \psi \in C_c(\widehat{G})$, then $\varphi * \psi = \widehat{h}$ where $h \in B^1(G)$. In particular, $\mathcal{F}(B^1(G))$ is dense in $L^p(\widehat{G})$ for $p < \infty$. ⌟

Proof: Cf.[Folland, P109]. □

Prop. (11.10.3.27). $(fg)^\wedge = \widehat{f} * \widehat{g}$ is satisfied for $f, g \in L^2(G)$ also. ⌟

Proof: Cf.[Folland, P112]. □

Prop. (11.10.3.28)[Duality of Subgroups]. $(H^\perp)^\perp = H$ for closed subgroup H of a locally compact Abelian group G. ⌟

Proof: Suffices to prove $(H^\perp)^\perp \subset H$. If $x_0 \notin H$, then Gelfand-Raikov shows that there is a character η on G/H that $\eta(q(x_0)) \neq 1$, so $x_0 \notin (H^\perp)^\perp$. □

Prop. (11.10.3.29). If H is a closed subgroup of G, then there are natural isomorphisms of LCA groups:

$$\Phi : \widehat{(G/H)} \cong H^\perp, \quad \Psi : \widehat{G}/H^\perp \cong \widehat{H}$$

⌟

Proof: Φ is clearly algebraic isomorphism. If $|\eta(q(K)) - 1| < \varepsilon$, then $|\eta(K) - 1| < \varepsilon$, so Φ is continuous in the compact-open topology. Similarly, to show Φ is open, it suffices to show a compact subset of G/H has a compact inverse image in G, but this is just(11.10.1.34).

Now for Ψ, notice $\widehat{\widehat{G}/H^\perp} \cong (H^\perp)^\perp \cong H$ by(11.10.3.28), so by Pontryagin duality theorem, $\widehat{G}/H^\perp \cong \widehat{H}$. □

Cor. (11.10.3.30) [Hahn-Banach for LCA Groups]. By the surjectivity of Ψ, any character of $\widehat{H}$ extends to a character of G. ⌟

Prop. (11.10.3.31) [Poisson Summation Formula]. Suppose H is a closed subgroup of G, if $f \in L^1(G)$, define $F(xH) = \int_H f(xy)dy$ on G/H, then $F \in L^1(G/H)$ by(11.10.1.38), then:

- $\widehat{F} = \widehat{f}|_{H^\perp}$, where $\widehat{G/H}$ is identified with $H^\perp$ by(11.10.3.29).
- If $\widehat{f}|_{H^\perp} \in L^1(H^\perp)$, then with the dual measure of G/H on $H^\perp$(11.10.3.14), we have

$$\int_H f(xy)dy = \int_{H^\perp} \widehat{f}(\xi)(x,\xi)d\xi.$$

In particular, take $x = e$, then

$$\int_H f(y)dy = \int_{H^\perp} \widehat{f}(\xi)d\xi.$$

⌟

Proof: Notice for $\xi \in H^\perp$,

$$\widehat{F}(\xi) = \int_{G/H} F(xH)\overline{(x,\xi)}d(xH) = \int_{G/H}\int_H f(xy)\overline{(xy,\xi)}dyd(xH) = \int_G f(x)\overline{(x,\xi)}dx = \widehat{f}(\xi)$$

by(11.10.1.38). And 2 is just(11.10.3.24) applied to $F(xH)$ on G/H. □

Cor. (11.10.3.32). In the situation of(11.10.3.31), if H is discrete in G and G/H is compact, then both $H, H^\perp$ are discrete, then by considering the dual measure using(11.10.3.16), the Poisson summation reads:

$$\sum_H f(xy) = \frac{1}{\mu(G/H)}\sum_{H^\perp} \widehat{f}(\xi)(x,\xi).$$

⌟

Perfect Pairing

Def. (11.10.3.33) [Self-Adjoint Haar Measures]. If G is a locally compact Abelian group, and there is an isomorphism $G \cong \widehat{G}$, or a perfect bilinear pairing $G \times G \to \mathbb{C}^*$, then by Fourier inversion(11.10.3.14), a Haar measure $d\mu$ on G corresponds to a Haar measure $d\alpha$ on $\widehat{G}$, but via the isomorphism, $d\alpha$ corresponds to a measure $\widetilde{d\alpha}$ on G. Now anyway, there is a unique $d\mu$ that $d\mu = \widetilde{d\alpha}$, and this is called the **self-dual Haar measure** on G.

Via this pairing, we define the Fourier transform as an isomorphism

$$L^2(G) \cong L^2(G) : \Phi(f)(x) = \int_G f(y)\overline{\langle x, y\rangle} d\mu(y).$$

Then $d\mu$ is a self-dual measure is equivalent to $\Phi(\Phi(f))(x) = f(-x)$, or equivalently $f(y) = \int_G \widehat{f}(y)\langle x, y\rangle d\mu(y)$. ⌟

Prop. (11.10.3.34). If G is a locally compact Abelian group, and there is a perfect bilinear pairing $G \times G \to \mathbb{C}^*$ and $\sigma : G \to G$ is a group automorphism of G that preserves this pairing, then σ preserves the Haar measure on G. ⌟

Proof: It is clear that $\sigma^* d\mu = |\sigma| d\mu$ for some real constant $|\sigma| > 1$. Consider the Fourier transform w.r.t. this pairing: $\mathcal{F}\varphi(x) = \int_G \varphi(y)\langle x, y\rangle dy$, then $\mathcal{F}(\varphi \circ \sigma) = |\sigma|^{-1}\mathcal{F}(x)$. But $\mathcal{F}$ is an isomorphism $L^2(G) \cong L^2(G)$, so $|\sigma|^{-1} = |\sigma|$, thus $|\sigma| = 1$. □

Prop. (11.10.3.35) [Self Duality of Topological Fields]. Let K be a locally compact topological field. If X is a non-trivial character on the additive group K^+, then for any $\eta \in K^+$, $\xi \mapsto X(\eta\xi)$ is also a character, and

$$F_X : \eta \mapsto (\xi \to X(\eta\xi))$$

is an isomorphism of topological groups of K^+ and $\widehat{K^+}$.

Then by(11.10.3.33), we find a self-dual measure Haar measure dx on K^+ w.r.t. X.

In fact, such a character X does exist, by Gelfand-Raikov(11.10.2.22). ⌟

Proof: First this is clearly a homomorphism of groups, and it is injective, because if $X(\eta\xi) = 1$ for all ξ, then $\eta K^+ \neq K^+$(because X is nontrivial), so $\eta = 0$.

Now the image of F is dense, because if $X(\eta\xi) = 1$ for all η, then $\xi = 0$, so $\overline{\mathrm{Im}(F)}^{\perp} = 1$. Now $(H^{\perp})^{\perp} = H$ for H closed(11.10.3.28) and use Pontryagin duality(11.10.3.23), so $\mathrm{Im}\, f$ is dense in $\widehat{G}$.

Now F is open and continuous, because: for any $B \in G$ compact, there is a nbhd V of 0 that $|X(V) - 1| < \varepsilon$, so there is a nbhd V' that $V'B \subset V$, so if $\eta \in V$, $|X(\eta B) - 1| < \varepsilon$, so F is continuous($\widehat{K^+}$ has the compact-open topology). And if we choose ξ_0 that $X(\xi_0) \neq 1$, then choose $B = \overline{B(0, \frac{|\varepsilon_0}{\varepsilon})}$ compact, if $|X(\eta B) - 1| < |X(\xi_0) - 1|$, then $\xi_0 \notin \eta B$, which means that $|\eta| < \varepsilon$. This means $F(B(0, \varepsilon))$ contains $V(B, |X(\xi_0) - 1|)$, so F is open.

So the image of F is a locally compact subgroup of $\widehat{G}$, so by(11.10.1.7) it is closed, hence equals G as it is dense, so F is surjective, and is an isomorphism. □

4 Compact Group

Cf.[群表示论 notes] and [Fol15]Chap5.

In this subsection, we consider representations of a compact group over $\mathbb{C}$.

Unitary Representations

Prop. (11.10.4.1) [F.d. Representation is Unitary]. If V is a real/complex f.d. representation π of a compact group G, then there is an inner product on V that the action of G is orthogonal/unitary. ⌟

Proof: Choose an arbitrary inner product $(\cdot,\cdot)_0$ on V, then consider

$$(u,v)=\int_G(\pi(x)u,\pi(x)v)_0dx.$$

where dx is a Haar measure on G. Then

$$(\pi(y)u,\pi(y)v)=\int_G(\pi(xy)u,\pi(xy)v)_0dx=\Delta(y)\int_G(\pi(x)u,\pi(x)v)_0dx=\int_G(\pi(x)u,\pi(x)v)_0dx$$

because G is compact hence unimodular(11.10.1.18). Thus this is an inner product on V that is invariant under G. □

Cor. (11.10.4.2) [F.D. Representation of Compact Groups Totally Decomposable]. Any f.d. representation of a compact group is totally decomposable. ⌟

Proof: This is because we can assume this representation is unitary by(11.10.4.1), and then for any subrepresentation we can take the orthogonal complement. □

Lemma (11.10.4.3). Suppose $(\pi,\mathcal{H})$ is a continuous unitary representation of the compact group G, let $u\neq 0\in\mathcal{H}$ be a unit vector, if the operator T on $\mathcal{H}$ is defined by

$$Tv=\int_G(v,\pi(x)u)\pi(x)udx,$$

then T is a positive, non-zero compact operator in $C(\pi)$. ⌟

Proof:

$$(Tv,v)=\int_G(v,\pi(u)u)(\pi(x)u,v)dx=\int_G|(\pi(x)u,v)|^2dx\geq 0,$$

so it is positive. Moreover, if $v=u$, then $x\mapsto|(\pi(x)u,v)|$ is a positive on a nbhd of 1, so $T\neq 0$.

Finally, because G is compact, $x\mapsto\pi(x)u$ is uniformly continuous, so for any $\varepsilon>0$, there is a disjoint partition E_i of G and $x_i\in E_i$ that if $x\in E_i$, then $||\pi(x)u-\pi(x_i)u||\leq\varepsilon/2$. Then

$$||(v,\pi(x)u)\pi(x)u-(v,\pi(x_i)u)\pi(x_i)u||\leq|(v,[\pi(x)-\pi(x_i)]u)\pi(x)u||+||(v,\pi(x_i)u)[\pi(x)-\pi(x_i)]u||<\varepsilon||v||.$$

So consider

$$T_\varepsilon(v)=\sum|E_j|(v,\pi(x_j)u)\pi(x_j)u=\sum\int_{E_i}(v,\pi(x_j)u)\pi(x_j)udx$$

then $||T-T_\varepsilon||<\varepsilon$, and T_ε has f.d image, thus T is compact, by(11.8.5.3).

Also $T\in C(\pi)$ because

$$\pi(y)Tv=\int_G(v,\pi(x)u)\pi(yx)udx=\int_G(v,\pi(y^{-1}x)u)\pi(x)udx=\int_G(\pi(y)v,\pi(x)u)\pi(x)udx=T\pi(y)v.$$

□

Prop. (11.10.4.4) [Unitary Representations of Compact Groups]. If G is compact group, then every unitary representation (ρ, V) of G is an orthogonal sum of irreducible unitary subrepresentations. Moreover, the isotopic part V^π for any irreducible representation π of G is uniquely determined. And very irreducible representation of G is of f.d.(thus unitary by(11.10.4.1)). ⌟

Proof: By taking orthogonal complements and Zorn's lemma, it suffices to show any unitary representation π has an irreducible subrepresentation. Choose T as in(11.10.4.3), then T is compact nonzero self-adjoint, so by Riesz-Fredholm(11.8.5.9) it has a finite-dimensional eigenspace, which is π-invariant, and it clearly has an irreducible subrepresentation by taking orthogonal complements.

For the orthogonality, Let V^π be the linear span of invariant subspaces isomorphic to π, for L_1, L_2 of type $\pi_1 \neq \pi_2$, then consider the orthogonal projection P onto L_2, then $P|_{L_1} \in C(\pi_1, \pi_2)$, which vanishes by Schur(11.10.2.4), so they are orthogonal.

The final assertion follows from(11.10.4.19). □

Cor. (11.10.4.5). The cardinality of irreducible constituents of V that is isomorphic to π is independent of the decomposition, and it is equal to $\dim \mathrm{Hom}_G(\pi, \rho)$, and is denoted by $\mathrm{mult}(\pi, \rho)$. ⌟

Proof: Cf.[Folland, P137].**?** □

Cor. (11.10.4.6). Let G be a compact subgroup and H a closed subgroup, then G acts unitarily on $L^2(G/H)$, and it decomposes as

$$L^2(G/H) \cong \widehat{\oplus}_{\pi \in \widehat{G}} N_H(\pi)\pi$$

where $N_H(\pi) = \dim \pi^H$ the dimension of H-fixed vectors in V. ⌟

Proof: By(11.10.4.4), it suffices to determine the multiplicity of π in $L^(G/H)$, which is just dimension of $\mathrm{Hom}_G(\pi, L^2(G/H))$, which can be viewed as G-invariant L^2 functions on G/H with values on π^*. For any such function f, $f(1)$ is H-invariant, and for any H-invariant vector v, $g \mapsto gv$ is continuous, thus is L^2. So the dimension of this space is just $\dim \pi^H$. □

Matrix Coefficients and Peter-Weyl Theorem

Def. (11.10.4.7) [K-Finite Vectors]. Let K be compact group. For an irreducible representation ρ of K, denote $V^\rho = \rho \otimes \mathrm{Hom}_K(\rho, V)$ the ρ-isotypic component in V. And let $V^{K-\mathrm{fin}} = \oplus_\rho V^\rho$ the space of **K-finite vectors** in V(11.10.4.4). ⌟

Def. (11.10.4.8) [Matrix Coefficients]. Firstly $C(G)$ is a representation of $G \times G$ by $((g_1, g_2)f)(g) = f(g_1^{-1} g g_2)$.

For a f.d. representation (π, V) of a topological group G, we can view $\mathrm{End}(V)$ as a representation of $G \times G$ via

$$(g_1, g_2)S = \pi(g_1) S \pi(g_2^{-1})$$

There is a **matrix coefficient map**:

$$MC_V : \mathrm{End}(V) \to C(G), \quad MC_V(S)(g) = MC_{S,V}(g) = \mathrm{tr}(S\pi(g^{-1})|V)$$

is a map of $K \times K$-representations. And denote $\mathcal{E}_\pi$ the image of of MC_V, and let $L^2_{alg}(G) = \oplus_{\pi \in \widehat{G}} \mathcal{E}_\pi$. ⌟

Prop. (11.10.4.9) [Schur Orthogonality Conditions]. Let $(\pi_1, V_1), (\pi_2, V_2)$ be f.d. continuous irreducible representations of K, then

$$\int_K MC_{S_1,V_1}(k) MC_{S_2,V_2}(k) = 0$$

unless $V_2 \cong V_1^*$, in which case

$$\int_K MC_{S_1,V}(k) MC_{S_2,V^*}(k) = \frac{1}{\dim V} \operatorname{tr}(S_1 \circ S_2^* | V).$$

In particular, $\mathcal{E}_\pi$ is orthogonal to $\mathcal{E}_{\pi'}$ for $[\pi] \neq [\pi']$, and if $\{e_i\}$ is any orthonormal basis of V, $\sqrt{d_\pi}\pi_{ij}$ is an orthonormal basis of $\mathcal{E}_\pi$, and $\mathcal{E}_\pi$ is isomorphic to $\operatorname{End}(V)$ as $K \times K$-representations. ⌟

Proof: Cf.[Gaitsgory P3]. □

Cor. (11.10.4.10). $MC_{S,V}(k^{-1}) = MC_{S^*,V^*}(k)$. ⌟

Prop. (11.10.4.11). $\mathcal{E}_\pi$ is invariant under left and right translations of G, and it is a two-sided ideal in $L^1(G)$. ⌟

Proof: It can be shown that $f \star \varphi_{u,v} = \varphi_{u,\pi(\overline{f})v}$, and $\varphi_{u,v} \star f = \varphi_{\pi(\widehat{f})u,v}$, where $\widehat{f}(x) = f(x^{-1})$. □

Prop. (11.10.4.12). If ρ is an irreducible f.d representation of K and V is a continuous representation of K, then for any $S \in \operatorname{End}(\rho^*)$, the image of

$$MC_{S,\rho}\mu_{Haar} \in M(K)$$

acting on V(11.8.3.24) belongs to V^ρ. ⌟

Proof: Cf.[Gaitsgory P7]. □

Cor. (11.10.4.13). For an irreducible representation ρ of K, the element $\xi_\rho\mu_{Haar} \in Meas(K)$ acts in any continuous representation V as a projection with image equal to V^ρ. ⌟

Proof: Directly from the proposition and(11.10.4.26). □

Prop. (11.10.4.14). $\mathcal{E}$ is an algebra, Cf.[Folland, P141]. It is dense in $C(K)$, and dense in $L^p(K)$ for $p < \infty$. ⌟

Proof: □

Prop. (11.10.4.15) [Peter-Weyl]. For a compact group K,

- $\widehat{\otimes}_{\pi\in\widehat{G}}\mathcal{E}_\pi = L^2(K)$, where $\mathcal{E}_\pi \cong \operatorname{End}(V_\pi)$.
- $L^2_{alg}(K) = \otimes_{\pi\in\widehat{G}}\mathcal{E}_\pi$ identifies with the K-finite vectors in $L^2(K)$ w.r.t. the left translation.

⌟

Proof: 1: By(11.10.4.4), the multiplicity of π in $L^2(K)$ is just $\dim\pi$, and this is just the multiplicity of π in $\mathcal{E}_\pi$ by(11.10.4.9), so this is an surjection, thus an isomorphism.

2: Clearly every vector in $\otimes_{\pi\in\widehat{G}}\mathcal{E}_\pi$ is K-finite. Conversely, if some vector v is K-finite, then it generates a finite vector space V under the left translation action of G. Now the linear function $f \mapsto f(1)$ restricts to a linear function l on V, and then $l(L_g^* v) = v(g)$, so v is a matrix coefficient of V, so $v \in L^2_{alg}(K)$. □

Cor. (11.10.4.16) [Representations of Product Groups]. Any irreducible representation of a the product group $G \times H$ for G, H is of the form $\rho \boxtimes \psi$ where ρ and ψ are irreducible representations of G, H resp. ⌟

Proof: By orthogonality of characters(11.10.4.22), there representations are irreducible and different. They are all the representations because they already form a basis in $L^2(G \times H)$. □

Prop. (11.10.4.17). For any continuous representation K, the subset V^{K-fin} is dense in V. ⌟

Proof: For any $v \in V$, choose a Dirac sequence f_n, then $\pi(f_n)v \to v$. Then by Peter-Weyl(11.10.4.15), we can choose K-finite functions g_n that $||g_n - f_n||_{L^2} < \frac{1}{n}$. Then g_n also converges to δ_1 in the weak topology. Thus

$$\pi(g_n)v \to v$$

and(11.10.4.12) shows $\pi(g_n)v \in V^{K-fin}$. □

Cor. (11.10.4.18). Matrix coefficients of f.d. representations are dense in $C(K)$. (Immediate from the proposition and Peter-Weyl theorem(11.10.4.15). ⌟

Cor. (11.10.4.19). Every irreducible continuous representation of a compact group is of f.d.. ⌟

Proof: This is because V^{K-fin} is a sub-representation of V and it is dense in V, thus $V = V^{K-fin}$ is of f.d. because it is irreducible. □

Fourier Analysis on Compact Groups

Def. (11.10.4.20)[Characters]. Let V is a f.d. continuous representation of K, let $\chi_V = MC_V(\mathrm{Id}_V) = \mathrm{tr}(g|V)$, called the **character** of V, and if V is irreducible, define $\xi_V = \dim V \cdot \chi_V$.

This definition of character is compatible the abstract definition viewed as a representation of the group algebra $\mathbb{C}[G]$. ⌟

Prop. (11.10.4.21). If we take an invariant inner product on V, and e_i an orthonormal basis, then

$$\chi_V(g) = \sum_i (ge_i, e_i),$$

and

$$\chi_{V^*}(g) = \chi_V(g^{-1}) = \overline{\chi_V(g)}, \quad \chi_{V\oplus W} = \chi_V + \chi_W, \quad \chi_{V\otimes W} = \chi_V \cdot \chi_W$$

⌟

Cor. (11.10.4.22) [Orthogonality of Characters]. Let V, W be irreducible, then

$$\int_K \chi_V(k)\chi_W(k^{-1}) = \int_K \chi_V(k)\chi_{W^*}(k) = \int_K \chi_V(k)\overline{\chi_W(k)}$$

so by(11.10.4.9) this equals 1 if $V \cong W$ and 0 otherwise. ⌟

Prop. (11.10.4.23). Let χ be a character of a representation of compact group K of dimension n, then

- $\chi(1) = n$.
- $\chi(s^{-1}) = \chi(s)^*$.
- $\chi(tst^{-1}) = \chi(s)$.

⌟

Proof: Notice the eigenvalues of $\rho(g)$ all have absolute value 1, because this representation is unitarizable(11.10.4.1) thus $\rho^*(g) = \rho(g)^*$. □

Prop. (11.10.4.24) [Fourier Transform on Compact Groups]. Let K be a compact group and $f \in L^2(K)$, then by Peter-Weyl(11.10.4.15) and(11.10.4.9),

$$f = \sum_{\pi \in \widehat{G}} \sum_{i,j=1}^{d_\pi} c_{ij}^\pi \pi_{ij}, \quad c_{ij}^\pi = d_\pi \int_G f(x)\overline{\pi_{ij}(x)}dx.$$

So

$$f(x) = \sum_{\pi \in \widehat{G}} \sum_{i,j=1}^{d_\pi} d_\pi \int_G f(y)\overline{\pi_{ij}(y)}\pi_{ij}(x)dx = \sum_{\pi \in \widehat{G}} d_\pi f(y)\operatorname{tr}(\pi(y^{-1}x)) = \sum_{\pi \in \widehat{G}} d_\pi (f * \chi_\pi)(y).$$

Thus

$$f = \sum_{\pi \in \widehat{G}} d_\pi f * \chi_\pi,$$

and $d_\pi f * \chi_\pi$ are the projection of f onto $\mathcal{E}_\pi$(11.10.4.9). ⌟

Cor. (11.10.4.25). $\xi_V * \xi_W = 0$ unless $W \cong V$ and $\xi_V * \xi_V = \xi_V$(11.10.4.20). ⌟

Cor. (11.10.4.26). For continuous irreducible representations V, W of K, $\pi(\xi_V) \in \operatorname{End} W$ equals Id_W if $W \cong V$ and zero otherwise. ⌟

Def. (11.10.4.27) [Class Functions]. A measurable function on G is called a **class function** iff $f(y^{-1}xy) = f(x)$ a.e. $(x, y) \in G \times G$. Denote $ZL^p(G)$ the space of class functions in $L^p(G)$ and $ZC(G)$ the space of continuous functions on G. ⌟

Prop. (11.10.4.28). For a compact group K and $1 \le p < \infty$, the spaces $L^p(K)$ and $C(K)$ are Banach algebras under convolution(11.10.1.26), and $ZL^p(K)$ and $ZC(K)$ are their centers. ⌟

Proof: By(11.10.1.29), $||f * g||_p \le ||f||_1||g||_p \le ||f||_p||g||_p$, for $1 \le p \le \infty$, thus $L^p(G)$ and $C(G)$ are Banach algebras.

For $f \in L^p(K)$, $f * g = g * f$ iff

$$\int_K f(xy)g(y^{-1})dy = \int_K g(y)f(y^{-1}x)dy = \int_K f(yx)g(y^{-1})dy, \quad a.e. x$$

for any $g \in L^p(K)$, which is equivalent to $f(xy) = f(yx)$ a.e. x, y. Similarly for $f \in C(K)$. □

Lemma (11.10.4.29). If $f \in ZL^1(K)$ and $\pi \in \widehat{K}$, then $d_\pi f * \chi_\pi = \int_K (f\overline{\chi}_\pi)\chi_\pi$. ⌟

Proof: For $x \in G$,

$$\pi(f)\pi(x) = \int_K f(y)\pi(yx)dy = \int_K f(yx^{-1})\pi(y)dy = \int_K f(x^{-1}y)\pi(y)dy = \int_K f(y)\pi(xy)dy = \pi(x)\pi(f)$$

so $\pi(f)$ is a scalar by Schur's lemma(11.10.2.4). Notice $f'(g) = f(g^{-1}) \in ZL^1(K)$ also, so

$$d_\pi[f * \chi_\pi](x) = d_\pi \int_K f(y^{-1})(\operatorname{tr}\pi)(yx)dy = d_\pi \operatorname{tr}(\int_K f(y^{-1})\pi(yx)dy) = \operatorname{tr}\pi(f')\operatorname{tr}(\pi(x))$$

and $\operatorname{tr}\pi(f') = \int_K f(y^{-1})\operatorname{tr}\chi(y)dy = \int_K f\overline{\chi_\pi}$. □

Prop. (11.10.4.30) [Characters Orthonormal Basis]. $\{\chi_\pi|\pi \in \widehat{K}\}$ is an orthogonal basis for $ZL^2(K)$. ⌟

Proof: $\chi_\pi \in ZC(K) \subset ZL^2(K)$ by(11.10.4.23), and they are orthonormal by(11.10.4.22). They are a basis by(11.10.4.29). □

Prop. (11.10.4.31). The linear spans of $\{\chi_\pi|\pi \in \widehat{K}\}$ is dense in $ZC(K)$ and $ZL^p(K)$ for $1 \le p < \infty$. ⌟

Proof: Cf.[Fol15] P148. □

Prop. (11.10.4.32) [Real Type]. Let G be a topological group and V is a complex representation, then the following are equivalent:

- $V = U \otimes_{\mathbb{R}} \mathbb{C}$ is a complexification of a real representation U of G.
- V admits a G-invariant anti-linear endomorphism S that $S^2 = 1$.
- There is a G-invariant symmetric form B on V inducing an isomorphism $V \cong V^*$.

⌟

Proof: $1 \iff 2$ is clear.

$2 \to 3$: By averaging there is a G-invariant Hermitian form h on V, then we can define $B(u,v) = h(u,Sv)$. As $h'(u,v) = h(Sv,Su)$ is also a G-invariant Hermitian form, $h(Sv,Su) = \pm h(u,v)$, so $B(v,u) = B(u,v)$.

$3 \to 1$: h induces a G-isomorphism $\overline{\varphi}_h : \overline{V} \cong V^*$. Then $\sigma = \overline{\varphi}_h \circ \varphi_B$ is a G-isomorphism $V \to \overline{V}$. Then $\overline{\sigma} \circ \sigma : V \to V$ is a G-isomorphism, thus by Schur's lemma $\overline{\sigma} \circ \sigma = \lambda$ for some $\lambda \in \mathbb{C}$. More explicitly, $B(v,u) = H(v,\sigma(u))$ for any $u,v \in V$. Because B is symmetric or symplectic, $B(u,v) = \pm B(v,u)$, thus $H(v,\sigma(u)) = \pm H(u,\sigma(v))$, and

$$\overline{\lambda}H(v,u) = H(v,\sigma^2(u)) = \pm H(\sigma(u),\sigma(v)) = \pm\overline{H(\sigma(v),\sigma(u))} = \overline{H(u,\sigma^2(v))} = \lambda H(v,u).$$

Thus λ is real. And then we can normalize σ that $\sigma = \pm 1$. If $\sigma^2 = 1$, then consider $V_0 = \ker(\sigma - 1)$, then $iV_0 = \ker(\sigma + 1)$, and $V_0 \oplus iV_0 = V$. If $\sigma^2 = -1$, then consider the action of $\mathbb{H}$ on V given by $(\alpha + \beta j)(v) = \alpha v + \beta\sigma(v)$. It is an action because σ is anti-linear and $\sigma^2 = -1$. □

Prop. (11.10.4.33) [Quaternion Type]. Let G be a topological group and V is a complex representation, then the following are equivalent:

- $V = W_{\mathbb{C}}$ is a restriction of a quaternionic representation W of G.
- V admits a G-invariant anti-linear endomorphism S that $S^2 = -1$.
- There is a G-invariant alternating form B on V inducing an isomorphism $V \cong V^*$.

⌟

Proof: $1 \iff 2$ is clear. The proof of $2 \to 3 \to 1$ is the same as the proof of(11.10.4.32). □

Prop. (11.10.4.34). An irreducible complex representation V of G, then V is of real/complex/quaternionic type iff $\mathrm{End}_{\mathbb{R}[G]}(V) \cong M_2(\mathbb{R})/\mathbb{C}/\mathbb{H}$ ⌟

Proof: By(11.10.4.32), if V is of real type, then $V \cong U \otimes_{\mathbb{R}} \mathbb{C} \cong V \oplus V$, then $\mathrm{End}_{\mathbb{R}[G]}(V) \cong M_2(\mathbb{R})$.

By(11.10.4.33), if V is of quaternionic type, then it is a restriction of a quaternionic representation, so $\mathbb{H} \subset \mathrm{End}_{\mathbb{R}[G]}(V)$. And for any $\mathbb{R}$-linear endomorphism f of V, $f = \frac{f+if\circ i}{2} + \frac{f-if\circ i}{2}$ is a sum of $\mathbb{C}$-linear and anti-linear endomorphisms of V. For an anti-linear endomorphism g, gj is $\mathbb{C}$-linear, thus $f \in \mathbb{H}$.

If V is of complex type, then there are no invariant anti-linear endomorphisms, thus $f = \frac{f+if\circ i}{2} + \frac{f-if\circ i}{2} = \frac{f+if\circ i}{2}$ is $\mathbb{C}$-linear, so $\mathrm{End}_{\mathbb{R}[G]}(V) \cong \mathbb{C}$. □

Prop. (11.10.4.35) [Types of Representations]. Let V be a finite-dimensional irreducible $\mathbb{C}$-representation of a compact group G. Let dg be the Haar measure on G with $\int_G dg = 1$, then:

$$\int_G \chi(g^2)dg = \begin{cases} 1 & \iff V \text{ is of real type} \\ 0 & \iff V \text{ is of complex type} \\ -1 & \iff V \text{ is of quaternionic type} \end{cases}$$

⌟

Proof: Notice that $\chi(g^2) = \chi_{\mathrm{Sym}^2(V)}(g) - \chi_{\wedge^2(V)}(g)$, so $\int_G \chi(g^2)dg = \dim \mathrm{Sym}^2(V)^G - \dim \wedge^2(V)^G$. Then it is clear by(18.1.1.6). □

5 Induced Representation

Lemma (11.10.5.1). If H is a closed subgroup of a locally compact subgroup G, $q : G \to G/H$, for any unitary representation $(\sigma, \mathcal{H})$ of H, let $\mathcal{F}_0$ be the space of continuous functions $f : G \to \mathcal{H}$ that $q(\mathrm{Supp}(f))$ is compact, and

$$f(x\xi) = \sqrt{\frac{\Delta_H(\xi)}{\Delta_G(\xi)}}\sigma(\xi^{-1})f(x).$$

Then if $\alpha : G \to \mathcal{H}$ is continuous with compact support, then

$$f_\alpha(x) = \int_H \sqrt{\frac{\Delta_G(\eta)}{\Delta_H(\eta)}}\sigma(\eta)\alpha(x\eta)d\eta \in \mathcal{F}_0$$

and is left uniformly continuous w.r.t G. Moreover, every element in $\mathcal{F}_0$ arises in this way. ⌟

Proof: Clearly $q(\mathrm{Supp}\, f_\alpha) \subset q(\mathrm{Supp}\, \alpha)$, and

$$f_\alpha(x\xi) = \int_H \sqrt{\frac{\Delta_G(\eta)}{\Delta_H(\eta)}}\sigma(\eta)\alpha(x\xi\eta)d\eta = \int_H \sqrt{\frac{\Delta_G(\xi^{-1}\eta)}{\Delta_H(\xi^{-1}\eta)}}\sigma(\xi^{-1}\eta)\alpha(x\eta)d\eta = \sqrt{\frac{\Delta_H(\xi)}{\Delta_G(\xi)}}\sigma(\xi^{-1})f_\alpha(x).$$

For left uniformly continuity, Cf.[Folland, P164].

For the surjectivity, if $f \in \mathcal{F}_0$, by(11.10.1.37), there exists $\psi \in C_c(G)$ that $\int_H \psi(x\eta)d\eta = 1$ for $x \in \mathrm{Supp}\, f$. So we can let $\alpha = \psi \cdot f$, then

$$f_\alpha(x) = \int_H \sqrt{\frac{\Delta_G(\eta)}{\Delta_H(\eta)}}\psi(x\eta)\sigma(\eta)f(x\eta)d\eta = \int_H \psi(x\eta)f(x)d\eta = f(x)$$

□

Remark (11.10.5.2)[Left and Right Compatibility]. If we consider the right action, then it suffices to consider all the functions $g(x) = f(x^{-1})$. Then g satisfied

$$g(\xi x) = \sqrt{\frac{\Delta_G(\xi)}{\Delta_H(\xi)}}\sigma(\xi)g(x).$$

⌟

Def. (11.10.5.3) [Induced Representations]. Let (σ, V) be a unitary representation of H, for any $f, f' \in \operatorname{ind}_H^G \rho$, consider the function $g \mapsto (f(g), f'(g))$, then it is a function on $\mathcal{S}(G, \mathcal{H})$(11.10.1.40), thus

$$(f, f') \mapsto \int_{H\backslash G} (f, f') d\nu_{H\backslash G}(g)$$

is a right G-invariant Hermitian inner product on $\operatorname{ind}_H^G \rho$, thus $\operatorname{ind}_H^G \rho$ is unitarizable, called the **induced representation**. ⌟

Prop. (11.10.5.4)[Induction and Restriction]. If $(\sigma, \mathcal{H})$ is a unitary representation of H and $(\pi, \mathcal{H}')$ is a unitary representation of G, then $\operatorname{ind}_H^G(\sigma \otimes \operatorname{res}(\pi)) \cong \operatorname{ind}_H^G(\sigma) \otimes \pi$. ⌟

Prop. (11.10.5.5) [Frobenius Reciprocity]. If G is compact group and H is a closed subgroup, π is an irreducible unitary representation of G, ρ is an irreducible unitary representation of H, then

$$C(\pi, \operatorname{ind}_H^G(\rho)) = C(\pi|_H, \rho), \quad \operatorname{mult}(\pi, \operatorname{ind}_H^G(\rho)) = \operatorname{mult}(\rho, \pi|_H).$$

⌟

Proof: It suffices to prove the first one, the second follows from(11.10.2.2) and(11.10.4.5).

G/H admits a G-invariant measure as $\Delta_G = \Delta_H = 1$. For the rest, it is semilar to that of(18.1.5.37), Cf.[Folland, P172]. □

11.11 Harmonic Analysis

Main reference are [Rud91], [泛函分析张恭庆] and [Harmonic Analysis: Real Variable Methods, Orthogonality, and Oscillatory Integrals, Stein]. Notice much should be rewritten in greater generality of Analysis on Locally Compact Groups.

1 Distributions

Def. (11.11.1.1) [Test Functions]. The space $D(\Omega)$ of **test functions** has the induced topology coincides with that of $D(K)$, and any bounded subsets are in some $D(K)$, thus it is complete and has Heine-Borel because $D(K)$ does.

The space of continuous linear functionals of $D(\Omega)$ is called the space of **distributions** $D'(\Omega)$. It is equivalence to the restriction to every $D(K)$ is continuous, Cf.[Rudin P155]. The **order** of a distribution Λ is the minimal N that $|\Lambda\varphi| \leq C_K||\varphi||_N$ for every $\varphi \in D(K)$, it might be ∞. ⌟

Def. (11.11.1.2) [Differentiation of Distributions]. The **differentiation of a distribution** Λ is defined as $D^\alpha\Lambda(\varphi) = (-1)^{|\alpha|}\Lambda(D^\alpha\varphi)$. The multiplication by a smooth function f is defined by $f\Lambda(\varphi) = \Lambda(f\varphi)$. Then

$$D^\alpha(f\Lambda) = \sum_{\beta\leq\alpha} C_{\alpha\beta}(D^{\alpha-\beta}f)(D^\beta\Lambda).$$

⌟

Support of a Distribution

Def. (11.11.1.3). The **support of a distribution** is the complement $\mathrm{Supp}(\Lambda)$ of the open sets U that $\Lambda(f) = 0$ for any f with support in U.

If $\mathrm{Supp}(\Lambda)$ is compact, then Λ has finite order and $|\Lambda\varphi| \leq C||\varphi||_N$ for some N, and Λ extends uniquely to a continuous linear functional on $C^\infty(\Omega)$. ⌟

Proof: This is because its support is compact so we can choose a smooth ψ that $= 1$ on $\mathrm{Supp}\,\varphi$ and has support in $W \subset \Omega$. Then by (11.11.1.1), there is a C that $|\Lambda(\psi\varphi)| < C||\psi\varphi||_N$, and Leibniz rule will give us the result. □

Prop. (11.11.1.4). If the support of a Λ is a pt p (thus has finite order m), then it is a linear combination of $D^\alpha\delta_p$,$|\alpha| \leq m$. (use approximate identity and show the kernel of Λ is contained in the kernel of $D^\alpha\delta_p$). ⌟

Proof: Cf.[Rudin P165]. □

Prop. (11.11.1.5). For any distribution Λ, there exist continuous functions g_α in $C^\infty(\Omega)$ that each compact K intersects support of f.m g_α and $\Lambda = \sum D^\alpha g_\alpha$. When Λ has finite order, we can use only f.m g_α. ⌟

Proof: use partition of unity. Then for a compact K, find a compact-open W, then find a bump function between $K \subset W$, thus reduce to the case of $D_{\overline{W}}$. For the rest, Cf.[Rudin P169]. □

Convolution on $\mathbb{R}^n$

Denote $\mathscr{D} = \mathscr{D}(\mathbb{R}^n), \mathscr{D}' = \mathscr{D}'(\mathbb{R}^n)$.

Def. (11.11.1.6). The **translation** of a distribution u is defined as $(\tau_x u)(\varphi) = u(\tau_{-x}\varphi)$, where $\tau_x\varphi(y) = \varphi(y-x)$.

The **convolution** of a test function with a distribution u is defined as $(u*\varphi)(x) = u(\tau_x\check{\varphi})$, where $\check{\varphi}(y) = \varphi(-y)$. ⌟

Prop. (11.11.1.7) [Special Case of (11.11.1.10)]. For $u \in D', \varphi \in D, \psi \in D$,

- $\tau_x(u*\varphi) = (\tau_x u)*\varphi = u*(\tau_x\varphi)$.
- $u*\varphi \in C^\infty$ and $D^\alpha(u*\varphi) = (D^\alpha u)*\varphi = u*(D^\alpha\varphi)$.
- $u*(\varphi*\psi) = (u*\varphi)*\psi$.

If u has compact support, then(11.11.1.3) shows that u can extend to C^∞, thus convolution is defined for $\varphi \in C^\infty$ and the first two formulae still hold, and when $\psi \in D$,

$$u*\psi \in D, \quad u*(\varphi*\psi) = (u*\varphi)*\psi = (u*\psi)*\varphi$$

⌟

Proof: Cf.[Rudin P171], [Rudin P174]. □

Cor. (11.11.1.8). $L : \varphi \mapsto u*\varphi$ is a continuous linear map into C^∞ that commutes with τ_x. And any these map comes from a $u*$:let $u = (L\check{\varphi})(0)$. ⌟

Proof: It is continuous because of of closed graph theorem(11.7.2.9), $\lim(u*\varphi_i)(x) = \lim u(\tau_x\check{\varphi}) = u(\tau_x\check{\varphi})$. □

Cor. (11.11.1.9). When $u, v \in D'$ and one of them has compact support, then similar to(11.11.1.8), $L\varphi = u*(v*\varphi)$ is a continuous linear map that commutes with τ_x, so there is a unique **convolution distribution** $u*v$ that $(u*v)*\varphi = u*(v*\varphi)$. This convolution is compatible with the previous one when $v \in D$. ⌟

Prop. (11.11.1.10) [Convolution of Distributions]. For $u, v, w \in D'$,

- if one of u, v has compact support, then $u*v = v*u$, and $\mathrm{Supp}(u*v) \subset \mathrm{Supp}(u) + \mathrm{Supp}(v)$.
- if two of three of u, v, w has compact support, then $(u*v)*w = u*(v*w)$.
- $D^\alpha u = (D^\alpha\delta)*u$.
- if one of u, v has compact support, then $D^\alpha(u*v) = (D^\alpha u)*v = u*(D^\alpha v)$.

⌟

Proof: Cf.[Rudin P177]. □

Def. (11.11.1.11). A **approximate identity** here is a $h \in D$ that $h_k(x) = k^n h(kx)$. Then we will have $\lim \varphi*h_j = \varphi$ for $\varphi \in D$, $\lim u*h_j = u$ in D'. ⌟

2 Fourier Analysis on $\mathbb{R}^n$

Def. (11.11.2.1) [Notations]. We denote the normalized notation $\mathbb{R}^n$ as $dm = (2\pi)^{-n/2}dx$ and

$$D_\alpha = \frac{1}{\mathrm{i}^{|\alpha|}}D^\alpha = \frac{1}{\mathrm{i}^{|\alpha|}}\frac{\partial}{\partial x^\alpha},$$

which will simplify many notations compared to D^α. The **Fourier transform** here of a function $f \in L^1(\mathbb{R}^n)$ is the function $\widehat{f}$ that $\widehat{f}(t) = \int_{\mathbb{R}^n} f e_{-t} dm_n = (f * e_t)(0)$.

See(11.11.2.12) for general Fourier transform. ⌟

Prop. (11.11.2.2). For $f \in L^1(\mathbb{R})$,

$$\widehat{\tau_x f} = e_{-x}\widehat{f}, \quad \widehat{e_{-x} f} = \tau_x \widehat{f},$$

$$\widehat{f * g} = \widehat{f}\widehat{g}, \quad \widehat{f(x/\lambda)}(t) = \lambda^n \widehat{f}(\lambda t).$$

(Note $||f * g||_1 \le ||f||_1 ||g||_1$). ⌟

Lemma (11.11.2.3). Let $f = e^{-1/2|x|^2}$, then $f \in \mathcal{S}$, $\widehat{f} = f$ and $f(0) = \int \widehat{f}$. ⌟

Proof: Reduce to the 1 dimensional case, in which case, $f' + xy = 0$, and $\widehat{f}$ also satisfies this. □

Lemma (11.11.2.4). For $f, g \in L^1$, Fubini theorem shows $\int \widehat{f} g = \int f \widehat{g}$. ⌟

Prop. (11.11.2.5) [Classical Fourier Transform].

- $\mathscr{S}$ is a Fréchet space in the topology defined by these norms.
- multiplication by $g \in \mathscr{S}$ and derivations are continuous linear map from S to S (direct calculation).
- $\widehat{P(D)f}(t) = P(t)\widehat{f}(t)$ and $\widehat{Pf} = P(-D)\widehat{f}$.
- The Fourier transform is a continuous linear one-to-one automorphism of $\mathcal{S}$, and $\Psi^2 g = \check{g}$.

⌟

Proof: 1:

2:

3: use(11.11.1.10) for the first one, and for the second one, should use definition of derivative and dominated convergence.

4:$\Psi f \in \mathcal{S}$ by 3, and it is continuous by closed graph theorem. By(11.11.2.4) and(11.11.2.2), $\int \widehat{f}(t)g(t/\lambda) = \int f(t/\lambda)\widehat{g}(y)$. If $\widehat{f}, \widehat{g} \in L^1$, dominant convergence shows $g(0)\int \widehat{f} = f(0)\int \widehat{g}$. So we only need one f that $f(0) = \int \widehat{f}$, $f = e^{-1/2|x|^2}$ will suffice(11.11.2.3). Hence $g(0) = \int \widehat{g}$ for every such g, and the conclusion follows by translation(11.11.2.2), and(11.10.3.14) also follows. □

Cor. (11.11.2.6). If $f \in L^1(\mathbb{R}^n)$, then $\widehat{f} \in C_0(\mathbb{R}^n)$, and $||\widehat{f}||_\infty \le ||f||_1$, because $\mathscr{S}$ is dense in $L^1(\mathbb{R}^n)$. ⌟

Prop. (11.11.2.7) [Inversion Theorem]. If $f \in L^1(\mathbb{R}^n)$ and $\widehat{f} \in L^1(\mathbb{R}^n)$, then $\check{f} = \Psi^2 f$ a.e. ⌟

Proof: In(11.11.2.4), let $g \in \mathcal{S}$ and substitute $g = \Psi g$ and use Fubini, we get $\check{f} - \Psi^2 f$ is orthogonal to every $\mathcal{S}$, then every continuous function with compact support by(11.3.8.10). Thus they equal a.e. □

Cor. (11.11.2.8). If $f, g \in \mathcal{S}$, then $\widehat{fg} = \widehat{f} * \widehat{g}$ (apply Fourier one time and use(11.11.2.2)), and thus $f * g \in \mathscr{S}$. ⌟

Prop. (11.11.2.9) [Fourier-Plancherel]. If $f, g \in \mathcal{S}$, then

$$\int f\overline{g} = \int \overline{g}(x)\widehat{f}(t)e^{ixt} = \int \widehat{f}(t)\int \overline{g}(x)e^{ixt} = \int \widehat{f}\widehat{\overline{g}}$$

by inversion formula. And $\mathcal{S}$ is dense in L^2, thus it extends to a linear isometry of $L^2(\mathbb{R}^n) \to L^2(\mathbb{R}^n)$. This coincides with the Fourier transform on $L^1 \cap L^2$. ⌟

Prop. (11.11.2.10). D injects into $\mathcal{S}$ and is dense.(Notice they both are complete, but the subspace topology are different)(Use scaling, Cf.[Rudin Functional Analysis P189]). So we call a distribution **tempered** iff it comes from a continuous functional of $\mathcal{S}$.

From(11.11.1.3), we know any distribution with compact support is tempered. By Holder, every $f \in L^p(\mathbb{R}^n), p \geq 1$ is tempered distribution, and every polynomial or functions of polynomial growth are tempered distribution.

$$D \subset \mathcal{S} \subset L^2 = (L^2)^\vee \subset \mathcal{S}' \subset D'.$$

$\mathcal{S}, \mathcal{S}'$ is complete(11.7.4.3). ⌟

Prop. (11.11.2.11). A $f \in \mathcal{S}'$ iff $f = \sum_{|\alpha|\leq m} D_\alpha(u_\alpha(1+|x|^2)^{m/2})$ for some m, where $u_\alpha \in L^2(\mathbb{R}^n)$. ⌟

Proof: In fact,

$$||\varphi||'_m = (\sum_{|\alpha|\leq m}\int (1+|x|^2)^m |D_\alpha\varphi|^2 \,\mathrm{dx})^2$$

is an equivalent set of norms of $\mathcal{S}'$, Cf.[泛函分析张恭庆 P182]. And each of them defines a Hilbert space. So by Riesz we get the result. □

Prop. (11.11.2.12)[Generalized Fourier Transform]. For a tempered distribution $u \in \mathcal{S}'$, we define the **Fourier transformation** as the tempered distribution $\widehat{u}(\varphi) = u(\widehat{\varphi})$. It is easily verified that it is compatible with previously defined Fourier transform when seen as tempered distributions by**??** In particular, this is defined for compactly supported distribution, $L^p(\mathbb{R}^n), p \geq 1$ and smooth functions of polynomial growth(11.11.2.10). ⌟

Prop. (11.11.2.13). $\widehat{P(D)u} = P\widehat{u}$ and $\widehat{Pu} = P(-D)\widehat{u}$. And The Fourier transformation is a continuous linear isometry of $\mathcal{S}'$ in the weak* topology. ⌟

Cor. (11.11.2.14). $\widehat{1} = \delta$, thus $\widehat{P} = P(-D)\delta$ and $\widehat{P(D)\delta} = P$. Now(11.11.1.4) tells us a distribution is the Fourier transform of a polynomial iff it has support in the origin. ⌟

Prop. (11.11.2.15) [Convolution of Tempered Distributions]. Let $u \in \mathcal{S}'$ and $\varphi, \psi \in \mathcal{S}$, then

- $u * \varphi \in C^\infty$ of polynomial growth and $D^\alpha(u * \varphi) = (D^\alpha u) * \varphi = u * (D^\alpha\varphi)$.
- $u * (\varphi * \psi) = (u * \varphi) * \psi$.
- $\widehat{u * \varphi} = \widehat{\varphi}\widehat{u}, \widehat{u} * \widehat{\varphi} = \widehat{\varphi u}$.
- If P is a polynomial and $g \in \mathcal{S}$, then $D^\alpha u, Pu$ and gu are all tempered.

⌟

Proof: Cf.[Rudin Functional Analysis P195] for the first 3. □

Variants

Prop. (11.11.2.16) [Mellin Inversion Formula]. Given a function $f:\mathbb{R}^+\to\mathbb{C}$ satisfying suitable conditions**?**, its **Mellin transformation** is defined to be

$$M(f)(s)=\int_0^\infty f(t)t^s\frac{dt}{t}.$$

where $s\in\mathbb{C}$ is in the domain s.t. this integral is absolutely convergent.

Notice if $\int_0^1 f(t)t^s\frac{\mathrm{d}t}{t}$ is convergent for some s, then it converges for any bigger s, and if $\int_1^\infty f(t)t^s\frac{dt}{t}$ converges for some s, then it converges for any smaller s. So the domain of $M(f)$ if nonempty, is a vertical strip $\sigma_1<\mathrm{Re}(\sigma)<\sigma_2$ for $\sigma_1,\sigma_2\in[-\infty,\infty]$.

Then f can be recovered from $M(f)$: for any $\sigma_1<\sigma<\sigma_2$,

$$f(x)=\frac{1}{2\pi\,\mathrm{i}}\int_{\sigma-\mathrm{i}\,\infty}^{\sigma+\mathrm{i}\,\infty}x^{-s}M(f)(s)ds.$$

⌟

Proof: Using the isomorphism of groups $t=e^x:\mathbb{R}^+\to\mathbb{R}$, this is just the usual Fourier transformation on $\mathbb{R}$. □

Def. (11.11.2.17) [Laplace Transformation]. Let $h:\mathbb{R}_+\to\mathbb{R}$ be a piecewise-continuous function, the **Laplace transformation** of h is the function

$$(\mathcal{L}h)(s)=\int_0^\infty e^{-st}h(t)\mathrm{d}t,\ s\in\mathbb{C}$$

whenever it is convergent. It is a holomorphic function for $\mathrm{Re}(s)>c$ if $h(t)=O(e^{ct})$. ⌟

Proof: The last assertion follows from(11.4.2.14). □

Thm. (11.11.2.18). Let $f:\mathbb{R}_{\geq 0}\to\mathbb{R}$ be a bounded piecewise-continuous function that its Laplace transform $(\mathcal{L}f)(s)$ extends to a holomorphic function on $\mathrm{Re}(s)\geq 0$, then the integral $\int_0^\infty f(t)\mathrm{d}t$ converges and equals $(\mathcal{L}f)(0)$. ⌟

Proof: Cf.[Suthurland, Number Theory1, L16].**?** □

Paley-Wiener Theory

Prop. (11.11.2.19). For $\varphi\in D(\mathbb{R}^n)$ that has support in rB, the You-Know-How defined $\widehat{\varphi}(z)$ is an entire function of several variable and satisfies:

$$|\varphi'(z)|\leq\gamma_N(1+|z|)^{-N}e^{r|\operatorname{Im}z|}.$$

For $N\geq 0$. Conversely, any such function correspond to a $\varphi\in D(\mathbb{R}^n)$ that has support in rB. ⌟

Proof: Cf.[Rudin P198]. □

Prop. (11.11.2.20) [Fourier-Laplace transformation]. For $u\in D'(\mathbb{R}^n)$ that has support in rB, of order N, the $\widehat{u}(z)=u(e_{-z})$ is an entire function of several variable and satisfies:

$$|f(z)|\leq\gamma(1+|z|)^Ne^{r|\operatorname{Im}z|}.$$

Conversely, any such function correspond to a $u\in D'(\mathbb{R}^n)$ that has support in rB. ⌟

Proof: Cf.[Rudin P199]. □

Gaussian Integrals

Notation (11.11.2.21). Let $V \in \mathcal{V}\mathrm{ect}^d/\mathbb{R}$ and $M(V)$ be the set of non-degenerate complex symmetric bilinear forms B on V with $\mathrm{Re}\, B \geq 0$. And let $M^0(V) \subset M(V)$ be the open dense subset consisting of forms B with $\mathrm{Re}\, B > 0$.

Suppose V is endowed with an Haar measure $\mathrm{d}x$, so we can define $\det B$ for $B \in M(V)$. As $M(V)$ is star-shaped thus simply-connected, we can also define the principle square $(\det B)^{1/2}$.

Any such B induces an isomorphism $\varphi_B : V \to V^* : x \mapsto B(x, -)$, and thus induces an inner product on the dual space:

$$B^{-1}(l, l') = B(\varphi_B^{-1} l, \varphi^{-1} l') = l(\varphi^{-1} l').$$

And there are isomorphisms:

$$B \mapsto B^{-1} : M(V) \cong M(V^*), \quad M^0(V) \cong M^0(V^*).$$

⌟

Lemma (11.11.2.22) [Gaussian Integral]. For $B \in M(V)$, $e^{-\frac{1}{2}B(x,x)} \in \mathscr{S}(V)$, and its Fourier transform is

$$\mathscr{F}(e^{-\frac{1}{2}B(x,x)})(p) = (\det B)^{-1/2} e^{-\frac{1}{2}B^{-1}(p,p)}, \quad p \in V^*.$$

⌟

Proof: By continuity**?**, it suffices to prove this for $B \in M^0(V)$. In this case B is diagonalizable and the statement is reduced to the case $\dim V = 1$. In this case, it suffices to show that for any $a \in \mathbb{C}, \mathrm{Re}\, a > 0$ and $p \in \mathbb{R}$,

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\mathrm{i}\, px - \frac{1}{2}ax^2} \mathrm{d}x = \frac{1}{\sqrt{a}} e^{-\frac{1}{2a}p^2}.$$

And this follows from**??**. □

Prop. (11.11.2.23). For $g \in \mathscr{S}(V), B \in M(V)$, consider the integral

$$I_g(\hbar) = \int_V g(\hbar x) e^{-B(x,x)} \mathrm{d}x, \quad \hbar \geq 0,$$

then $I_g \in C^\infty([0, \infty))$ with

$$I_g'(\hbar) = I_{\frac{1}{2}\Delta_B(g)}(\hbar)(11.12.3.2).$$

And also

$$I_g(0) = (2\pi)^{d/2} \frac{g(0)}{\sqrt{\det B}}.$$

⌟

Proof: The last assertion follows from(11.11.2.22) where $p = 0$.

Then we prove I_g is continuous: Only the continuity at $\hbar = 0$ is non-trivial. By Plancherel formula,

$$I_g(\hbar) = \left(g(\hbar^{\frac{1}{2}} x), e^{-\frac{1}{2}B(x,x)}\right) = \hbar^{-\frac{d}{2}} (\det B)^{-\frac{1}{2}} (g^\vee(\hbar^{-\frac{1}{2}} p), e^{-\frac{1}{2}B^{-1}(p,p)}) = (\det B)^{-\frac{1}{2}} (g^\vee(p), e^{-\frac{\hbar}{2}B^{-1}(p,p)}).$$

But $e^{-\frac{\hbar}{2}B^{-1}(p,p)} \to 1$ in $\mathscr{S}'(V^*)$ as $\hbar \to 0$, so

$$\lim_{\hbar\to 0} I_g(\hbar) = (\det B)^{-\frac{1}{2}}(g^\vee(p),1) = (2\pi)^{\frac{d}{2}}(\det B)^{-\frac{1}{2}}g(0) = I_g(0).$$

To prove smoothness: If $\hbar > 0$, then by differentiation,

$$I_g^\backprime(h) = \frac{1}{2}\hbar^{-1}I_{Eg}(\hbar),$$

where $E = \sum_i e_i^*\partial_{e_i}$ is the Euler vector field on V(11.12.3.1). So by(11.11.2.24),

$$I_g^\backprime(\hbar) = I_{\frac{1}{2}\Delta_B g}(\hbar).$$

Then it suffices to prove that $I_g \in C^1([0,\infty))$ and use induction. For this, notice first that if C is a positive definite real form on V, then by(11.11.2.22),

$$I_{e^{-\frac{1}{2}C(x,x)}}(\hbar) = \int_V e^{-\frac{1}{2}(B+\hbar C)(x,x)}\mathrm{d}x = (2\pi)^{\frac{d}{2}}\det(B+\hbar C)^{-\frac{1}{2}}$$

is smooth. Thus by linearity, we may assume that $g(0) = 0$. Then it follows from Taylor expansion(11.3.3.15) that g is a linear combination of functions of the form lf, where $l \in V^*$ and $f \in \mathscr{S}(V)$. Thus we may assume $g = lf$, and then it follows from(11.11.2.24) that

$$\lim_{\hbar\to 0}\frac{I_g(\hbar) - I_g(0)}{\hbar} = I_{\varphi_B^{-1}(l)f}(\hbar),$$

which is just $I_{\frac{1}{2}\Delta_B g}(\hbar)$, because

$$\frac{1}{2}\Delta_B g(0) = \sum_j l(e_j)\partial_{\varphi_B^{-1}e_j^*}f(0) = \partial_{\varphi^{-1}(l)}f(0).$$

This proves that the assertion. $\square$

Lemma (11.11.2.24). For $f \in \mathscr{S}(V)$ and $l \in V^*$,

$$I_{lf}(\hbar) = \hbar I_{\varphi_B^{-1}(l)f}(\hbar).$$

⌟

Proof:

$$\begin{aligned} I_{lf}(\hbar) &= \hbar^{\frac{1}{2}}(l(x)f(\hbar^{\frac{1}{2}}x), e^{-\frac{1}{2}B(x,x)}) = \hbar^{\frac{1}{2}}(f(\hbar^{\frac{1}{2}}x), l(x)e^{-\frac{1}{2}B(x,x)}) \\ &= -\hbar^{\frac{1}{2}}(f(\hbar^{\frac{1}{2}}x), \partial_{\varphi_B^{-1}(l)}e^{-\frac{1}{2}B(x,x)}) = \hbar^{\frac{1}{2}}(\partial_{\varphi_B^{-1}(l)}f(\hbar^{\frac{1}{2}}x), e^{-\frac{1}{2}B(x,x)}) \\ &= \hbar((\partial_{\varphi_B^{-1}(l)}f)(\hbar^{\frac{1}{2}}x), e^{-\frac{1}{2}B(x,x)}) = \hbar I_{\varphi_B^{-1}(l)f}(\hbar) \end{aligned}$$

$\square$

Prop. (11.11.2.25) [Riemann Lemma]. Let $D \subset \mathbb{R}^n$ be a compact region with smooth boundary, and $f, g \in C^\infty(D)$ s.t. $g^{(n)}$ vanishes on the boundary for any $n \in \mathbb{N}$, and $\mathrm{d}f \neq 0$ on $\mathrm{Supp}(g)$, then the function

$$I(\hbar) = \int_D g(x)e^{\frac{\mathrm{i}f(x)}{\hbar}}\mathrm{d}x$$

extends to a smooth function on $[0,\infty)$, and has rapidly decaying derivatives of all orders as $\hbar \to 0$.
⌟

Proof: As $\operatorname{Supp} g$ is compact and $\mathrm{d}f \neq 0$ on $\operatorname{Supp} g$, we can cover D by f.m. charts s.t. $f(x) = x_1$. Then by using smooth partition of unity, we may reduce to the case that $f(x) = x_1$. Then we are reduced to the 1-dimensional case and $f(x) = x$. Then in this case, it suffices to notice that

$$\int_a^b g(x)e^{\mathrm{i}\,\frac{x}{\hbar}}\mathrm{d}x = \mathrm{i}\,\hbar\int_a^b g'(x)e^{\mathrm{i}\,\frac{x}{\hbar}}\mathrm{d}x,$$

and use induction. □

<u>**Steepest Descent and Stationary Phase Formulae**</u>

Thm. (11.11.2.26) [Steepest Descent Formula]. Let $D \subset \mathbb{R}^n$ be a compact region with smooth boundary and $f, g \in C^\infty(D)$. Assume that f attains a global minimal at a unique non-degenerate critical point $c \in D$ with $\operatorname{Hess} f(c)$ positive definite, then

$$\int_D g(x)e^{-f(x)/\hbar}\mathrm{d}x = \hbar^{\frac{d}{2}}e^{-f(c)/\hbar}I(\hbar)$$

where $I(x)$ extends to a smooth function on $[0, \infty)$ with

$$I(0) = (2\pi)^{\frac{d}{2}}\frac{g(c)}{\sqrt{\det \operatorname{Hess} f(c)}}.$$

Moreover, this generalizes to the case that f attains global minimums at multiple non-degenerate critical points. ⌟

Proof: WLOG, we may assume that c is the origin and $f(c) = 0$. By Morse lemma, there is a smooth coordinate near the origin that $f(x) = \frac{1}{2}\operatorname{Hess}(f)(x, x)$ on a nbhd of the origin. Then we can use smooth partition of function to reduce to the case g has support on a small nbhd of 0 or the case that g vanishes near 0. For the last case, it is clear by direct differentiation that $I(\hbar)$ is rapidly decaying as $\hbar \to 0$. And for the first case, by a change of variable,

$$I(\hbar) = \int_{\mathbb{R}^n} g'(\hbar y)e^{-\frac{1}{2}\operatorname{Hess} f y^2}\mathrm{d}y.$$

Then we finish by(11.11.2.23). □

Thm. (11.11.2.27) [Stationary Phase Formula]. Let $D \subset \mathbb{R}^n$ be a compact region with smooth boundary, and $f \in C^\infty(D), g \in C^\infty(D)$. Assume that f has a unique critical point $c \in D$ and f is non-degenerate at c, and $g^{(n)}$ vanishes on the boundary for any $n \in \mathbb{N}$, then

$$\int_D g(x)e^{\mathrm{i}\,f(x)/\hbar}\mathrm{d}x = \hbar^{\frac{d}{2}}e^{\mathrm{i}\,f(c)/\hbar}I(\hbar)$$

where $I(x)$ extends to a smooth function on $[0, \infty)$ with

$$I(0) = (2\pi)^{\frac{d}{2}}e^{\sigma\pi\,\mathrm{i}\,/4}\frac{g(c)}{\sqrt{|\det \operatorname{Hess} f(c)|}},$$

where σ is the signature of $\operatorname{Hess} f(c)$.

Moreover, this generalizes to the case that f has multiple non-degenerate critical points. ⌟

Proof: The proof is similar to that of(11.11.2.26). In particular, using the partition function to separate the near to 0 part of g. And the away-from-0 part of g is smooth and rapidly decaying by Riemann lemma(11.11.2.25). Then by Morse lemma, it reduces to the case that f is quadratic. Then the assertion follows from(11.11.2.23). □

3 Tauberian Theory

Thm. (11.11.3.1) [Wiener]. If Y is a closed translation-invariant space of $L^1(\mathbb{R}^n)$ s.t. $Z(Y) = \cap_{f\in Y}\{s \in \mathbb{R}^n : \widehat{f}(s) = 0\} = \varnothing$, then $Y = L^1(\mathbb{R}^n)$. ⌟

Proof: Cf.[Rud91]P228. □

Cor. (11.11.3.2). If $\varphi \in L^1(\mathbb{R}^n)$ and Y is the smallest closed translation-invariant subspace of $L^1(\mathbb{R}^n)$ containing φ, then $Y = L^1(\mathbb{R}^n)$ iff $\widehat{\varphi}(t) \neq 0$ for any $t \in \mathbb{R}^n$. ⌟

Proof: Notice $Z(Y) = \cap_{f\in Y}\{s \in \mathbb{R}^n : \widehat{f}(s) = 0\} = \{t \in \mathbb{R}^n : \widehat{\varphi}(t) = 0\}$. □

4 Sobolev Spaces

Def. (11.11.4.1) [Sobolev Spaces]. For $1 \leq p < \infty$, the **Sobolev space** $W^{m,p}(\Omega)$ is the space of functions u that $D^\alpha u \in L^p(\Omega)$ for every $|\alpha| \leq m$, with the norm $||u|| = \sum_{|\alpha|<m}\int_\Omega |D^\alpha u(x)|^2 dx$. The **Sobolev space** $W_0^{m,p}(\Omega)$ is the completion of the subspace $C_0^\infty(\Omega)$. ⌟

Prop. (11.11.4.2)[Meyers-Serrin]. The Sobolev space $W^{m,p}(\Omega)$ is the completion of $u \in C^\infty(\Omega)$ that $D^\alpha u \in L^p(\Omega)$ for every $|\alpha| \leq m$. ⌟

Proof: Choose a countable partition of unity ψ_k, then as in the proof of(11.3.8.11), we can choose δ_k small enough and $||\psi u - (\psi u)_{\delta_k}|| < \varepsilon/2^k$ and $\varphi = \sum(\psi u)_{\delta_k}$ is definable. □

Prop. (11.11.4.3). We denote $H^m(\Omega) = W^{m,2}(\Omega)$ and $H_0^m(\Omega) = W_0^{m,2}(\Omega)$ and $H^{-m}(\Omega) = (H_0^m(\Omega))^*$ when m is an integer. Notice derivative is not applicable for $H^{-m}(\Omega)$ unless $\Omega = \mathbb{R}^n$.

When $\Omega = \mathbb{R}^n$, $D(\mathbb{R}^n)$ is dense in $W^{m,p}$(11.3.8.11), thus $W_0^{m,p} = W^{m,p}$. Define the **Sobolev space**

$$H^s = \{u|(1+|y|^2)^{s/2}|\widehat{u}| \in L^2\}$$

H^s is a Hilbert space and $H^s \subset \mathcal{S}'$ for every s (use Holder to show $\widehat{u} \in \mathcal{S}'$). H^m coincides with previously defined H^m when m is a positive integer thus also negative-integer. A linear operator on $H = \cup H^s$ is said to have **order** t if it maps every H^s continuously into H^{s-t}.

⌟

Proof: By Plancherel,

$$||\varphi||'_m = (\sum_{|\alpha|\leq m} ||D_\alpha u||_2^2)^{1/2} \quad \text{and} \quad (\int (1+|x|^2)^m |\widehat{u}|^2)^{1/2}$$

are equivalence norms on H^m. □

Lemma (11.11.4.4) [Poincare Inequality]. For Ω bounded, on $C_0^m(\Omega)$ the $W^{m,p}$ norm is controlled by L^p norms of its mth order derivatives . ⌟

Proof: We may assume $\Omega \subset \prod_{i=1}^n [0,a]$, then for any $u \in W^{m,p}$, $u(x) = \int_0^{x_1} D^1 u(t, x_2, \ldots, x_n)dt$, so by Holder inequality,

$$|u(x)| \leq a^{1/q}(\int_0^a |D^1 u|^p dx_1)^{1/p}.$$

so

$$\int_\Omega |u(x)|^p dx \leq a^q \int_\Omega |D^1 u|^p dx_1.$$

Doing the same for all other derivatives, we can see the norm is controlled by the highest(m-th) order norms. □

Prop. (11.11.4.5). When $t < s$, $H^s \subset H^t$. And H^s are isometric to H^t by $\widehat{v} = (1+|y|^2)^{t/2}\widehat{u}$ and is of order t. D^α is of order $|\alpha|$. If $f \in \mathcal{S}$, then $u \to fu$ is an operator of order 0.

Every distribution of compact support is in some H^s(11.11.1.3), in particular $D(\Omega)$. ⌟

Proof: Cf.[Rudin P217]. □

Prop. (11.11.4.6)[Sobolev Embedding Theorem]. On a manifold of dimension n which is compact with Lipschitz boundary or complete of positive injective radius and bounded sectional curvature,

- if $k > l$ be integers and
$$\frac{1}{p} - \frac{k}{n} = \frac{1}{q} - \frac{l}{n}$$
then $W^{k,p}(\mathrm{int}(M)) \subset W^{l,q}(M)$ continuously.
- if
$$\frac{1}{p} - \frac{k}{n} = -\frac{r+\alpha}{n}$$
then $W^{k,p}(\mathrm{int}(M)) \subset C^{r,\alpha}(M)$ continuously.

⌟

Proof: Cf.[Evans P290]. □

Cor. (11.11.4.7)[Gagliardo–Nirenberg–Sobolev]. On a manifold of dimension n which is compact with Lipschitz boundary or a complete of positive injective radius and bounded sectional curvature, if $\frac{1}{p^*} = \frac{1}{p} - \frac{1}{n}$ (Sobolev conjugate), then $W^{1,p}(\mathrm{int}(M)) \subset L^{p^*}(M)$ continuously. ⌟

Cor. (11.11.4.8). On a manifold of dimension n which is compact with Lipschitz boundary or a complete of positive injective radius and bounded sectional curvature, if $m > n/2$, then $W^{m,2}(\mathrm{int}(M)) \subset C(\overline{\Omega})(M)$ continuously. And the functions in $W_0^{m,2}$ are continuous and vanish at the boundary, by C_0 approximation. ⌟

Proof: The $\mathbb{R}^n$ case can be directly proved: because we have the equivalent norm(11.11.4.3), $\widehat{u} \in L^2$ thus $u \in L^2$, and
$$\int |\widehat{u}| \leq (\int (1+|x|^2)^m |\widehat{u}|^2)^{1/2} \cdot \Big(\int 1/(1+|x|^2)^m\Big)^{1/2}.$$
We have $\widehat{u} \in L^1$, thus inversion formula applies that u is continuous and $||u||_\infty \leq ||\widehat{u}||_1 \leq C||u||_{H^m}$. □

Cor. (11.11.4.9). $\cap_s H^s = C^\infty(M)$. ⌟

Prop. (11.11.4.10) [Rellich-Kondrechov]. On a compact manifold with C^1 boundary of dimension n, if $k > l$ and
$$\frac{1}{p} - \frac{k}{n} < \frac{1}{q} - \frac{l}{n}$$
then $W^{k,p} \subset W^{l,q}$ completely continuously. ⌟

Proof: Cf.[Distributions and Operators P199], [Evans P290]. □

Cor. (11.11.4.11). On a bounded extension domain of $\mathbb{R}^n$, $W^{1,p} \subset L^p$ completely continuously. ⌟

Proof: We prove the $p=2$ case. For a sequence u_m in $W^{1,2}$, we have $||u_m-u_p||_2=||U_m-U_p||_2=||\widehat{U}_m-\widehat{U}_p||_2$. By(11.8.4.9), there is a subsequence that $\widehat{U}_m$ pointwise converge. Notice they are uniformly bounded, Now apply two region argument, for $|x|<r$, use Lebesgue dominant convergence, and for $|x|>r$, use $\int(1+|x|^2)|\widehat{U}_m-\widehat{U}_p|^2$ is bounded to conclude $||u_m-u_p||_2\to 0$. □

Prop. (11.11.4.12). $u\in D'(\Omega)$ is a locally H^s $\iff$ $\psi u\in H^s$ for every $\psi\in D(\Omega)$ $\iff$ $D_\alpha u$ is locally L^2 for every $|\alpha|\le s$.

Thus every smooth function is locally H^s for every s. ⌟

Proof: $1\to 2$ use partition of unity, $2\to 1$ easy, and $2,3$ are all equivalent to $D_\alpha(\psi u)\in L^2$ for every $\psi\in D(\Omega)$. by Leibniz+Plancherel or (11.11.4.5). □

Prop. (11.11.4.13). If $r>p+n/2$, then if a function f on Ω has all the distribution derivative $D_i^k f$ locally $L^2,=g_{is}$, for $0\le k\le r$, then $f\in C^p(\Omega)$ a.e. ⌟

Cor. (11.11.4.14). If $u\in D'(\Omega)$ is locally H^s, then $u\in C^{s-n/2}(\Omega)$. Thus $\cap$locally $H^s=C^\infty(\Omega)$. ⌟

Holder Space

Def. (11.11.4.15). Holder space $C^{k,\alpha}(\Omega)$ is the subspace of $C^k(\Omega)$ with the norm

$$||f||_{C^{k,\alpha}}=||f||_{C^k}+\max_{|\beta|=k}\sup_{x\neq y\in\Omega}\frac{|D^\beta f(x)-D^\beta f(y)|}{||x-y||^\alpha}.$$

⌟

5 Fourier Analysis on $\mathbb{T}^n$

Prop. (11.11.5.1). If f is a periodic function on $\mathbb{R}$ with period 2π and piecewise-differentiable, then the Fourier series of f converges to $\frac{1}{2}(f(x+)+f(x-))$ everywhere. ⌟

Proof: [武胜健 2, P264]. □

Prop. (11.11.5.2). If f is a periodic differentiable function on $\mathbb{R}$ with period 2π and f' is integrable at $[-\pi,\pi]$, then the Fourier series of f converges to f uniformly. ⌟

Proof: [武胜健 2, P281]. □

Prop. (11.11.5.3). If $f\in L^1(\mathbb{T})$ is absolutely continuous, then $\widehat{(f')}(n)=2\pi\,\mathrm{i}\,n\cdot\widehat{f}(n)$. ⌟

Prop. (11.11.5.4). $f\in L^1(\mathbb{T})$ is determined by its Fourier coefficients. ⌟

11.12 Differential Equations

1 ODE-Fundamentals

Prop. (11.12.1.1).

$$x^{(2)} = f(x)$$

It can be solved. ⌟

Proof:

$$x^{'}x^{(2)} = f(x)x^{'}$$
$$\frac{1}{2}(x^{'})^2 = \int^x f(t)dt$$

□

Prop. (11.12.1.2) [Wronsky]. ⌟

2 ODE-Theorems

Prop. (11.12.2.1) [Existence and Uniqueness of ODE of Lipschitz Type]. If $F(t,x)$ defined on $[-h,.h]\times[\eta-\delta,\eta+\delta]$ is a function that is locally Lipschitz: that is, $\exists\delta,L$, s.t. if $|t|\leq h, |x_i-\eta|\leq\delta$, then

$$|F(t,x_1)-F(t,x_2)|\leq L|x_1-x_2|.$$

Then the initial value problem:

$$(Tx)(t) = \eta + \int_0^t F(\tau,x(\tau))d\tau$$

has a unique solution on the interval $[-h,h]$ if $h<\min\{\delta/M,1/L\}$, where M is the maximum of F on $[-h,.h]\times[\eta-\delta,\eta+\delta]$. Because T is a contraction. ⌟

Prop. (11.12.2.2) [Existence of ODE of Continuous Type (Caratheodory)]. If $F(t,x)$ defined on $[-h,.h]\times[\eta-\delta,\eta+\delta]$ is a continuous function, then

$$(Tx)(t) = \eta + \int_0^t F(\tau,x(\tau))d\tau$$

has a unique solution on the interval $[-h,h]$ if $h<\delta/M$, where M is the maximum of F on $[-h,.h]\times[\eta-\delta,\eta+\delta]$. (Use Schauder fixed point theorem and Arzela-Ascali). ⌟

Prop. (11.12.2.3) [Existence Theorem for Complex Differential Equations]. Let $\Omega\subset\mathbb{C}^{n+1}$ be a domain, $f(z,\mathbf{w}):\Omega\to\mathbb{C}^n$, then the initial value problem

$$\mathbf{w}' = f(z,\mathbf{w}),\quad w(z_0)=w_0$$

has exactly on holomorphic solution locally (Thus on a simply connected domain). ⌟

Cor. (11.12.2.4). So a holomorphic high-order ODE for a complex variable can be solved. And luckily it can be solved even $\overline{z}$ appears (just regard it as a constant). ⌟

Proof: Cf.[Ordinary Differential Equations, P110]. □

Prop. (11.12.2.5). For the equation:

$$\frac{d\mathbf{y}}{d\mathbf{x}} = \mathbf{A}\mathbf{y},$$

One solution basis is:

$$\begin{cases} e^{\lambda_1 x}\mathbf{P}_1^{(1)}(x), \cdots, e^{\lambda_1 x}\mathbf{P}_{n_1}^{(1)}(x); \\ \cdots\cdots\cdots \\ e^{\lambda_s x}\mathbf{P}_1^{(d)}(x), \cdots, e^{\lambda_s x}\mathbf{P}_{n_s}^{(1)}(x); \end{cases}$$

Where

$$\mathbf{P}_j^{(i)}(x) = \mathbf{r}_{j0}^{(i)} + \frac{x}{1!}\mathbf{r}_{j1}^{(i)} + \cdots,$$

where $\mathbf{r}_{j0}^{(i)}$ is a basis of solution of $(\mathbf{A} - \lambda_i I)^n \mathbf{x} = 0$, and $\mathbf{r}_{k+1}^{(i)} = (\mathbf{A} - \lambda_i I)\mathbf{r}_k^{(i)}$. ⌟

Proof: Cf.[常微分方程丁同仁定理 6.6]. □

Cor. (11.12.2.6). For the equation:

$$y^{(n)} + a_1 y^{(n-1)} + \cdots + a_{n-1} y' + a_n y = 0,$$

If the characteristic equation has s different roots $\lambda_1, \ldots, \lambda_s$ and corresponding multiplicities $n_1, \ldots, n_s$, then:

$$\begin{cases} e^{\lambda_1 x}, xe^{\lambda_1 x}, \cdots, x^{n_1 - 1}e^{\lambda_1 x}; \\ \cdots\cdots\cdots \\ e^{\lambda_s x}, xe^{\lambda_s x}, \cdots, x^{n_s - 1}e^{\lambda_s x}; \end{cases}$$

is a solution basis. ⌟

Proof: Cf.[常微分方程丁同仁 P198]. □

Prop. (11.12.2.7)[Lyapunov]. Consider the Lyapunov stability of an autonomous system of the form:

$$\frac{\partial}{\partial t}x = Ax + o(|x|),$$

Then:

1. If A has a eigenvalue whose real part is positive, then the trivial solution is not weak stable.
2. If all eigenvalues of A has negative real part, then the trivial solution is strong stable.

⌟

Stum-Liouville

Prop. (11.12.2.8) [Stum-Liouville]. The eigenvalue BVP problem of L-S equation:

$$Lu = (pu')' + qu = \lambda u, \quad a_1 u(a) + a_2 u'(a) = 0, b_1 u(b) + b_2 u'(b) = 0, \sigma(x) > 0.$$

can be solved by the method of Green's function. For the function:

$$G(x,s) = \begin{cases} Cu_1(x)u_2(s), & x < s \\ Cu_2(x)u_1(s), & x > s \end{cases}$$

for some C, where u_1 is a solution of the L-S equation with boundary value at a, and u_2 with boundary value at b that are linear independent (This happens when the homogenous equation has no solution). It satisfies: $LG(x,s) = \delta(x-s)$ and satisfies the boundary conditions.

Because L is self-adjoint, we have:

$$Gf(x) = \int f(s)G(x,s)ds, LG = \mathrm{id}, GL = \mathrm{id}$$

thus the eigenvalues of L is the reciprocal of the eigenvalues of G, and G is a compact self-adjoint operator on $L^2(\sigma, \mathbb{R})$, so by spectral theorem, the eigenvectors are countable and form an orthonormal basis.

And when the homogenous problem do have a solution ϕ, then we have:$Lu = f$ has a solution iff $(f, \phi) = 0$. one way is simple and the other way is because we solve the initial problem of ODE and find that it automatically satisfies the boundary condition. Cf.[Stum Liouville Theory]. ⌟

Prop. (11.12.2.9). More generally, if there the boundary is mixed of $u(a), U'(a), u(b), u'(b)$, the solution of

$$Lu = (pu')' + qu = 0, B_1(u) = \alpha, B_2(u) = \beta.$$

has a unique solution for any α, β iff the homogenous equation has only non-trivial solution. (Because the solution space is of 2 dimensional. ⌟

Prop. (11.12.2.10) [Stum Seperation Theorem]. ⌟

Proof: □

Prop. (11.12.2.11) [Stum Comparison Theorem]. If $y" + K_i(x)y = 0$ are equations. If $y_i(0) = 0$ and $|y_1'(0)| = |y_2'(0)|$, then if $K_1(x) \geq K_2(x)$, then $y_1(x) \geq y_2(x)$ until $y_2(x)$ is zero. (directly from(12.3.4.10)). ⌟

Proof: □

3 Linear PDE

Linear Operators

Def. (11.12.3.1)[Euler Differential Operator]. For $V \in \mathcal{V}\mathrm{ect}/\mathbb{R}$, the **Euler differential** is the first order linear differential operator

$$E = \sum_i e_i^* \partial_{e_i},$$

where $\{e_i\}$ is any basis of V. ⌟

Proof: □

Def. (11.12.3.2) [Laplacians]. For $V \in \mathcal{V}\mathrm{ect}/\mathbb{R}$ and a non-degenerate bilinear form B on V, the **Laplacian operator** of B is defined to be the second order linear differential operator

$$\Delta_B = \sum_i \partial_{\varphi_B^{-1} e_i^*} \circ \partial_{e_i} : \mathscr{S}(V) \to \mathscr{S}(V)$$

⌟

Proof: □

<u>**Existence of Solutions**</u>

Def. (11.12.3.3) [Fundamental Solutions]. For a linear PDE with constant coefficients $P(D)u = v$, the **fundamental solution** is a distribution $E \in D'(\mathbb{R}^n)$ that $P(D)E = \delta$. This is important because if v is a distribution with compact support, $P(D)(E * v) = (P(D)E) * v = \delta * v = v$(11.11.1.10), so $u = E * v$ is a distribution solution. ⌟

Prop. (11.12.3.4). When $v \in D'(\mathbb{R}^n)$ has compact support, $P(D)u = v$ has a solution u with compact support iff $Pg = \widehat{v}$ has a solution g entire. In this case, $g = \widehat{u}$ for some distribution u, and u has support in the convex hull of the support of v. ⌟

Proof: Use(11.11.2.20), and some bound relation between g and Pg. Cf.[Rudin Functional Analysis P212]. □

Prop. (11.12.3.5). The fundamental solution always exist when for PDE of constant coefficients. ⌟

Proof: For a $\varphi \in D(\mathbb{R}^n)$, there is at most one ψ that $\psi = P(D)\varphi$ because $\widehat{\psi} = P\widehat{\varphi}$ and they are entire function. Thus the task is to verify the functional $u : P(D)\varphi \to \varphi(0)$ is continuous and extend to a distribution $u \in D'(\mathbb{R}^n)$. Cf.[Rudin Functional Analysis P215]. □

4 Differential Operators on Manifolds

Prop. (11.12.4.1) [Index Theorem P109]. has a nice definition of symbol of a differential operator on a manifold as a map form $\mathrm{Sym}^m T^*M \otimes \mathbb{C} \to \mathrm{Hom}(E, F)$. ⌟

5 Pseudo-Differential Operator

Def. (11.12.5.1)[Japanese Brackets]. Denote the **Japanese bracket** $[x] = (1+|x|^2)^{1/2} = \Theta(1+|x|)$.

Motivated by the formula $(P\cdot f^\vee)^\vee = P(D)f$ for $f \in \mathcal{S}$ and polynomial P of ξ with coefficients smooth functions of x**??** we define the **symbol class** $S^{\mu,\beta}$ as the space of smooth functions $a : \mathbb{R}^{2n} \to \mathbb{C}$ that

$$|D_{x,\alpha} D_{\xi,\beta} a(x,\xi)| \leq C_{\alpha,\beta}[x]^\mu [\xi]^{m-|\beta|}$$

and denote $S^m = S^{0,m}$.

We denote the **symbol class** $\mathcal{A}^v$ as the space of smooth functions $a : \mathbb{R}^{2n} \to C$ that $|D_\alpha a| \leq C_\alpha [x+\xi]^v$ for any α. So $S^{\mu,m} \subset \mathcal{A}^{|\mu|+|m|}$

And we define the **pseudo-differential operator of symbol** a:

$$(a(x,D)u)(x) = \int_\xi e^{ix\xi} a(x,\xi)\widehat{u}$$

Moreover, we can define the **amplitude function** $p(x,y,\xi)$ and define

$$Pu(x) = \int e^{i(x-y)\xi} p(x,y,\xi)u(y)dy.$$

⌟

Def. (11.12.5.2). We define the space S^d of **polyhomogenous symbols of degree** d as the set of all symbols in $S^d_{0,1}$ that there exists a set of p_{d-l} homogenous in ξ of degree $d-l$ that $p = \sum p_{d-l}$ modulo an operator in $S^{-\infty}$. Note that when p_{d-l} is homogenous of degree $d-l$, then it is automatically in $S^{d-l}_{0,1}$. ⌟

Def. (11.12.5.3). A ψdo operator a is called **elliptic** if $\sigma(a) \in S^m$ and $\sigma(a) \geq [\xi]^{-m}$ for ξ big enough. ⌟

Prop. (11.12.5.4) [Peetre's Inequality]. For all $v \in \mathbb{R}$, there is a constant C that

$$[X+Y]^v < C[X]^v[Y]^v.$$

⌟

Proof: For $v > 0$, just as normal. For $v < 0$, use $X = (X+Y) + (-Y)$ applied to $-v$. □

Prop. (11.12.5.5). The mapping $a(x,\xi) \times u(x) \mapsto a(x,D)u$ is continuous from $\mathcal{A}^v \times \mathcal{S} \to \mathcal{S}$, thus also continuous from $S^{\mu,m} \times \mathcal{S} \to \mathcal{S}$. Cf.[Pseudo Differential Operator P28]. ⌟

Lemma (11.12.5.6) [Schur Test]. For a function K on $\mathbb{R}^{2n}$ and $u \in L^p(\mathbb{R}^n)$, let $||K||_1 = \sup_x \int |K(x,y)|dy$ and $||K(x,y)||_2 = \sup_y \int |K(x,y)|dx$. Let $Au(x) = \int K(x,y)u(y)dy$, then

$$||Au||_{l^p} \leq ||K||_1^{1-1/p}||K||_2^{1/p}||u||_{L^p}.$$

by Holder. ⌟

Prop. (11.12.5.7) [Calderón-Vaillancourt]. There is a constant C, N_{CV} that for $u \in \mathcal{A}^0$ and $\varphi \in \mathcal{S}$,

$$||Op(u)\varphi||_{L^2} \leq C \max_{|\alpha|+|\beta| \leq N_{CV}} ||\partial_x^\alpha D_{\beta,\xi} u||_{L^\infty}||\varphi||_{L^2}.$$

This in particular applies to $u \in S^0$. ⌟

Proof: Cf.[Calderon-Vaillancourt]. □

Cor. (11.12.5.8). S^m maps H^s to H^{s-m}. Because by symbolic calculus(11.12.5.10), we have

$$Op([\xi]^{s-m})Op(u)Op([\xi]^{-s}) = Op(b) \in S^0,$$

thus $Op(u) = Op([\xi]^{m-s})Op(b)Op([\xi]^s)$ maps H^s into H^{s-m}. ⌟

Symbolic Calculus

Def. (11.12.5.9) [Semiclassical Operator]. For $a \in S^{\mu,m}$ and $h \in (0,1]$, we denote $a_h(x,\xi) = a(x,h\xi)$, it is also in $S^{\mu,m}$. ⌟

Prop. (11.12.5.10) [Composition]. If $a \in S^{\mu_1,m_1}$ and $b \in S^{\mu_2,m_2}$, there is a pseudo-differential operator $(a\#b)(h) \in S^{\mu_1+\mu_2,m_1+m_2}$ for every $h \in (0,1]$ that

$$Op(a_h)Op(b_h) = Op((a\#b)(h)_h)$$

and for all $J > 0$, $(a\#b)(h)$ can be written as

$$a\#b(h) = \sum_{j<J} h^j\Big(\sum_{|\alpha|=j}\frac{1}{\alpha!}\partial_\xi^\alpha a D_x^\alpha b\Big) + h^J r_J^\#(a,b,h)$$

where $r_J^\#(a,b,h) \in S^{\mu_1+\mu_2,m_1+m_2-J}$ and it is bilinear of a,b and equicontinuous independently of h. ⌟

Proof: Cf.[Pseudo Differential Operator P36]. □

Prop. (11.12.5.11) [Adjoint]. If $a \in S^{\mu,m}$ and $u, v \in \mathcal{S}$, there is a pseudo-differential operator $a * (h)$ for every $h \in (0,1]$ that

$$(u, Op(a_h)v) = (Op(a^*(h)_h)u, v)$$

in the L^2 norm and for all $J > 0$, $a^*(h)$ can be written as

$$a^*(h) = \sum_{j<J} h^j \Big(\sum_{|\alpha|=j} \frac{1}{\alpha!} \partial_\xi^\alpha D_x^\alpha \overline{a}\Big) + h^J r_J^*(a, h)$$

where $r_J^*(a, h) \in S^{\mu,m-J}$ and it is anti-linear of a and equicontinuous independently of h. ⌟

Proof: Cf.[Pseudo Differential Operator P30]. □

Def. (11.12.5.12). For $u \in \mathcal{S}'$, we define the action of $a(x,\xi)$ on u by

$$(Op(a_h)u)(\overline{\varphi}) = u(\overline{Op(a^*(h)_h)\varphi}).$$

This is compatible with the definition on $\mathcal{S}$. ⌟

6 General PDE

Cf.[Gilbarg, David; Trudinger, Neil S. Elliptic partial differential equations of second order. Reprint of the 1998 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2001. xiv+517 pp. ISBN: 3-540-41160-7].

Direct Solutions

Prop. (11.12.6.1) [Characteristic Line]. Consider a 1-dimensional parabolic equation:

$$p_t + c(p, x, t)p_x = r(p, x, t)$$

Let $P(t) = p(X(t), t)$, this equation is equivalent to

$$P_t = r(X(t), t, P(t)), \quad X_t = c(X(t), t).$$

an ODE equation. ⌟

Prop. (11.12.6.2). A set of equations:

$$\frac{\partial}{\partial x^i}\mu = A_i \mu$$

where μ is a n-vector. It has a solution iff

$$[A_i, A_j] = \frac{\partial}{\partial x^i} A_i - \frac{\partial}{\partial x^i} A_j.$$

⌟

Proof: □

Cor. (11.12.6.3). This seems to be able to derive Frobenius integrability theorem, but I cannot figure it out. ⌟

7 Analysis on Manifolds

Prop. (11.12.7.1) [Peetre's Theorem]. For a linear operator from $C^\infty(M)$ to $C^\infty(M)$ that $Supp(Lu) \subset Supp(u)$ where M is a compact manifold, then on every compact subset of a coordinate chart L looks like a differential operator of finite order. ⌟

Proof: The first thing is to prove on a chart Ω, L is continuous on $C_0^\infty(\Omega)$. In fact, it suffice to show it is continuous from $C_0^\infty(\Omega)$ to $C_0^0(\Omega)$ because we can apply to $D_\alpha L$. For this, Cf.[Pseudo Differential Operator P86].

Then we have $|Lu| \leq C\max_{|\alpha\leq m}\sup_K |D_\alpha\varphi|$ for every $\varphi \in C_0(K)$. And the functional $\varphi \to (L\varphi)(x)$ is a distribution supported on x, thus by(11.11.1.4), it is of the form

$$Lu(x) = \sum_{|\alpha|\leq m} a_\alpha(x) D_\alpha\varphi(x).$$

We need to show a_α is smooth, which we choose a bump function χ to show a_0 is smooth and then choose $x_i\chi$ applied to $L\varphi - a_0\varphi$ to show a_i is smooth, etc. □

Prop. (11.12.7.2). The property of ψdo of order d is preserved under diffeomorphism, Cf.[Distributions and Operators P195], giving us the possibility to define ψdo differential operator on manifolds, and the principal symbol variate in this way that it forms a function from the cotangent bundle to the $M_n(\mathbb{C})$. And the Sobolev space is defined by the property that all of its restrictions on a atlas are Sobolev, using the partition of unity. ⌟

Prop. (11.12.7.3). All the norms of different are commensurable up to constant factor w.r.t. each other, so it doesn't quite matter with different norms. ⌟

Prop. (11.12.7.4). The parametrix exists for an elliptic operator on manifolds. Cf.[Distributions and Operators P207]. ⌟

8 Elliptic Operators

Prop. (11.12.8.1). Elliptic operator is a Fredholm operator. And the kernel and cokernel are smooth functions, so it is also a Fredholm operator on $C^\infty(\Omega)$. ⌟

Proof: It suffice to find a left and right inverse modulo compact operators, and in fact we find it module $S^{-\infty}$. Since $S^{-\infty}$ are all compact operators, i.e. it has a parametrix. Cf.[Distributions and Operators, P184]. □

Prop. (11.12.8.2) [Garding Inequality]. For an elliptic operator of order d on $\Gamma(E)$,

$$||f||_{H^s} \leq C(||f||_{H^{s-d}} + ||Pf||_{H^{s-d}})$$

⌟

Proof: □

Cor. (11.12.8.3) [Elliptic Regularity Theorem]. The inverse image of a smooth function under an elliptic operator is a smooth function, because the intersection of $H^s(E)$ is $C^\infty(E)$. ⌟

Cor. (11.12.8.4) [Elliptic Regularity Theorem]. For $L = \sum_{|\alpha|\leq N} f_\alpha D_\alpha$, where $f_\alpha \in C^\infty(\Omega)$ and the equation $Lu = v$ for distributions u and $v \in D'(\Omega)$, when v is locally H^s, u is locally H^{s+N}. Thus if $v \in C^\infty(\Omega)$, then $u \in C^\infty(\Omega)$ by(11.11.4.12)(11.11.4.14). ⌟

Proof: We prove the case when L has leading coefficients constant. For every $\varphi \in D(\Omega)$ that is 1 on some open ball B, φu has compact support thus in some H^t< and then we use a sublemma that says if ψ is 1 on the support of φ, then if ψu is in H^t, where $t \le s+N-1$, then $\varphi u \in H^{t+1}$. In this way, we can shrink the nbhd to reach H^{s+N}. The proof of the lemma is in [Rudin Functional Analysis P220]. □

Prop. (11.12.8.5) [Analytic Ellipticity theorem]. Suppose L is an analytic elliptic differential operator on a domain $M \subset \mathbb{R}^n$, then every solution to $L\varphi = 0$ is analytic. ⌟

Proof: □

Prop. (11.12.8.6). The formal adjoint of an elliptic operator is an elliptic operator. ⌟

Proof: □

Cor. (11.12.8.7). The index of an elliptic operator, regarded as an operator form $L_s \to L_{s-d}$ doesn't depend on s, because all the kernel of P and P^* are smooth. ⌟

Prop. (11.12.8.8). For an elliptic operator, It has a inverse, the Green function which is a compact operator, so it has countable eigenfunctions consisting of smooth functions on L^2 with eigenvalues converging to ∞. Moreover, the eigenvalues satisfy $|\lambda_n| \ge Cn^\delta$ for some δ, C. ⌟

Proof: We prove for P self-adjoint. Use(11.12.8.1), $\ker P$ is all smooth, so there is a map $P(H^{-2d}) \to P(H^{-d})$ which is bijective thus an isomorphism by Banach. So the inverse of this isomorphism composed with the Sobolev embedding $H^{-d} \to L^2$ is a compact operator G. we notice that this map has the same eigenfunctions as P, thus the result from that of compact operators.

For the second assertion, if suffice to prove $\dim N(\lambda) \le C\lambda^M$. Using Garding inequality and Sobolev embedding, we have for $f \in N(\lambda)$, $||f||_{C^0} \le C(1+\lambda^l)||f||_{L^2}$ for large l. So if we choose an orthonormal basis f_i, then $|a_i f_i(x)| \le C(1+\lambda^l)|\sqrt{\sum |a_i|^2}$. Let $a_i = f_i(x)$ and integrate over M, we get the desired result. □

Cor. (11.12.8.9). For a self-adjoint elliptic operator P which is not a constant, $L^2(E)$ has a basis consisting of eigenfunctions of P. ⌟

Cor. (11.12.8.10) [Stum-Liouville]. This can be used to solve for example eigenvalue problem for Liouville's equation:

$$(pu')' + qu = \lambda\sigma u.$$

where p and σ are positive. Cf.(11.12.2.8). ⌟

Cor. (11.12.8.11). The Hermite functions $C_n e^{x^2/2}\frac{d^n}{dx^n}e^{-x^2}$, as the eigenvector of $\widehat{H} = x^2 - \frac{d^2}{dx^2}$, forms a complete basis for $L^2(\mathbb{R})$. Because it is e^{-x^2} times the solution of the operator $(e^{-x^2}F')' - e^{-x^2}F$. ⌟

Prop. (11.12.8.12). For a formally self-adjoint elliptic operator P of degree d on E, $\Gamma(E) = \operatorname{Im} P \oplus P(\Gamma(E))$. ⌟

Proof: We know that $L^2(E) = P(H^d E) \oplus \ker P$, and $\ker P$ are all smooth by(11.12.8.3), so $\Gamma(E) = \ker P \oplus P(H^d E) \cap \Gamma(E)$. Now use Garding's inequality(11.12.8.2), the intersection is just $P(\Gamma(E))$, thus the result. □

Prop. (11.12.8.13) [Asymptotic Heat Equation]. In this case we have the series

$$h_t(A^*A) = \sum_\lambda e^{-\lambda t} \dim \Gamma_\lambda(E)$$

converges and h_t has an asymptotic expansion

$$h_t = \sum_{k \geq -n} t^{k/2m} U_k(A^*A)$$

where $n = \dim M$ and $U_k = \int_M \mu_k$ for a differential form on M. Cf.[Heat Equation and the Index Theorem P297].

By the proposition above, the eigenspaces of eigenvalue non-zero neutralize, so Ind $A = h_t(A^*A) - h_t(AA^*)$, so

$$\text{Ind } A = U_0(A^*A) - U_0(AA^*) = \int_M \mu_0(A^*A) - \mu_0(AA^*).$$

The proof consists of the following propositions, ⌟

Prop. (11.12.8.14). Using the fact that an elliptic operator has a countable basis, for an elliptic operator P, when $t > 0$, we let $K(t, x, y) = \sum_n e^{-t\lambda_n} \Phi_n(x) \overline{\Phi}_n(y)$, then

$$e^{-tP} f(x) = \int K(t, x, y) f(y) dy.$$

$K(t, x, y)$ is smooth. and the trace of e^{-tA^*A} is exactly $h_t(A^*A)$ as in the last proposition. And the trace is just $\int_M K(t, x, x)$, as can be easily seen. ⌟

Proof: Use Garding inequality and(11.12.8.8), we can show $||K||_{C^k}$ is bounded. □

11.13 Calculus of Variations

1 Euclidean case

Def. (11.13.1.1) [Functionals on Function Spaces]. A **functional** on the space of finite curves in $\mathbb{R}^N$ is a real-valued function on the space of smooth curves in $\mathbb{R}^N$. ⌟

Def. (11.13.1.2) [Differentiable Functionals]. A **differentiable functional** on the space of finite curves in $\mathbb{R}^N$ is a functional on the space of curves s.t. for any $\gamma : I \to \mathbb{R}^N$ and $h \in C^\infty(I, \mathbb{R}^N)$,

$$\Phi(\gamma + h) - \Phi(\gamma) = F(h) + O(||h||^2 + ||h'||^2).$$

when $||h||^2 + ||h'||^2$ is small, where F is a linear functional $F : C^\infty(I, \mathbb{R}^N) \to \mathbb{R}$. Such a function F(necessarily unique) is called the **variation of the functional** Φ. ⌟

Def. (11.13.1.3) [Extremal Curves of a Functionals]. An **extremal curve** for a differentiable functional(11.13.1.2) is a finite curve $\gamma : [t_0, t_1] \to \mathbb{R}$ s.t. the variation $F(h) = 0$ for any $h \in C^\infty([t_0, t_1], \mathbb{R}^N)$ s.t. $h(t_0) = h(t_1) = 0$. ⌟

Prop. (11.13.1.4). If $L = L(a, b, c) \in C^\infty(\mathbb{R}^N \times \mathbb{R}^N \times \mathbb{R})$, then, the functional

$$\Phi(\gamma) = \int_{t_0}^{t_1} L(\gamma(t), \dot{\gamma}(t), t)\mathrm{d}t, \quad \gamma : [t_0, t_1] \to \mathbb{R}^N :$$

is differentiable, and its variation is given by

$$F(h) = \int_{t_0}^{t_1} \Big[\frac{\partial}{\partial\gamma}L - \frac{\partial}{\partial t}\frac{\partial}{\partial\dot{\gamma}}L\Big]h\mathrm{d}t + (h\frac{\partial}{\partial\dot{\gamma}}L)\Big|_{t_0}^{t_1}.$$

⌟

Proof:

$$\begin{aligned}\Phi(\gamma + h) - \Phi(\gamma) &= \int_{t_0}^{t_1} [L(\gamma + h, \dot{\gamma} + h', t) - L(\gamma, \dot{\gamma}, t)]\mathrm{d}t \\ &= \int_{t_0}^{t_1} \Big[\frac{\partial}{\partial\gamma}Lh + \frac{\partial}{\partial\dot{\gamma}}Lh'\Big]\mathrm{d}t + O(||h||^2 + ||h'||^2) \\ &= \int_{t_0}^{t_1} \Big[\frac{\partial}{\partial\gamma}L - \frac{\partial}{\partial t}\frac{\partial}{\partial\dot{\gamma}}L\Big]h\mathrm{d}t + (h\frac{\partial}{\partial\dot{\gamma}}L)\Big|_{t_0}^{t_1} + O(||h||^2 + ||h'||^2)\end{aligned}$$

The last assertion follows easily from(11.3.2.13). □

Cor. (11.13.1.5) [Euler-Lagrangian Equation]. γ is an extremal curve(11.13.1.3) for this functional(11.13.1.4) if

$$\frac{\partial}{\partial\gamma}L - \frac{\partial}{\partial t}\frac{\partial}{\partial\dot{\gamma}}L = 0$$

along the curve γ. This equation is called the **Euler-Lagrangian equation** for this functional. ⌟

Remark (11.13.1.6). In the higher dimensional case($L = L(\varphi_j, \partial_i\varphi_j, x_i) \in C^\infty((\mathbb{R}^N)^{2m} \times \mathbb{R}^m)$, the Euler-Lagrangian equation is given by

$$\frac{\partial}{\partial\gamma}L - \sum_i \partial_i \frac{\partial}{\partial(\partial_i\varphi)}L = 0.$$

⌟

2 Riemannian Manifold case

11.14 Micro-local Analysis

11.15 Scattering Theory

11.16 Operator Algebras

Cf.[Princeton Companion], [Folland], [Non-commutative Geometry, Connes]Chap5.
The theory of operator algebras is the non-commutative analogue of measure theory.

1 Basics

Def. (11.16.1.1) [von Neumann Algebra]. A **von Neumann Algebra** is a B^*-subalgebra of $L(\mathcal{H})$ that contains the identity and is closed in the weak operator topology(11.7.3.4). ⌟

Def. (11.16.1.2) [Bicommutant]. If $\mathcal{S}$ is a subset of $L(\mathcal{H})$, then we define the **commutator** $\Gamma(\mathcal{S})$ be the algebra of operators that commutes with $S \in \mathcal{S}$, then $\Gamma(\Gamma(\mathcal{S}))$ contains $\mathcal{S}$, it is called the **bicommutant** of $\mathcal{S}S$.

If $\mathcal{A}$ is a $*$-algebra in $L(\mathcal{H})$, then $\Gamma(\Gamma(A))$ is a von-Neumann algebra. ⌟

Proof: If $\mathcal{A}$ is a $*$-algebra, then $\Gamma(\Gamma(A))$ is clearly a $*$-algebra, and it is weakly-closed because if $SV_i = V_iS$ and $V_ix \to Vx$ for any x, then $SVx = VSx$ for any x. □

Prop. (11.16.1.3) [von Neumann Density Theorem]. Let $\mathcal{A}$ be a non-degenerate $*$-subalgebra of $L(\mathcal{H})$, then $\mathcal{A}$ is dense in $\Gamma(\Gamma(\mathcal{A}))$ in the strong operator topology. ⌟

Proof: For any $S \in \Gamma(\Gamma(\mathcal{A}))$ and any $x_1, \ldots, x_N \in \mathcal{H}$, $\varepsilon > 0$, we need to prove there exists $A \in \mathcal{A}$ that $\sum ||Sx_i - Ax_i|| \leq \varepsilon^2$.

For the case $N = 1$ and $x_1 = x$, consider the closure $\mathcal{X}$ of $\{Ax\}$, then the orthogonal projection P onto $\mathcal{X}$ is an operator in $\Gamma(\mathcal{A})$. This implies $A(1-P)x = (1-P)Ax = 0$, thus $x = Px$ because of non-degeneracy. Then because S commutes with P, $Sx = SPx = PSx \in \mathcal{X}$, thus there exists an $A \in \mathcal{A}$ that Ax is close to Sx.

For $N > 1$, we can just apply the result to $\mathcal{H}^N$. □

11.17 D-Modules

11.18 Dynamical Systems

References are [Dynamical System, Katok] and [B-S02].

1 Topological Dynamical Systems

Def. (11.18.1.1)[Topological Dynamic Systems]. A **topological dynamic system** is a topological space X and either a continuous map $f : X \to X$ or a continuous (semi)flow f^t on X. ⌟

Def. (11.18.1.2)[Conjugacies]. Let $(X, f), (Y, g)$ be topological dynamical systems, then a **semiconjugacy of dynamical systems** from (X, f) to (Y, g) is a surjection $\mathrm{pr} : X \to Y$ s.t. $g \circ \mathrm{pr} = \mathrm{pr} \circ f$. An invertible semiconjugacy is called a **conjugacy of dynamical systems**. ⌟

Def. (11.18.1.3) [Dynamical Notions]. Let $f : X \to X$ be a discrete topological dynamic system(11.18.1.1), then

- $x \in X$ is called a **periodic point** for f if $f^{(p)}(x) = x$ for some $p \in \mathbb{Z}_+$. And the minimal $p \in \mathbb{Z}_+$ s.t. $f^{(p)}(x) = x$ is called the **period** of f at x. $x \in X$ is called a **pre-periodic point** for f if $f^{(m)}(x) = f^{(n)}(x)$ for some $0 < m < n \in \mathbb{Z}_+$. The set of pre-periodic points of f is denoted by $\mathrm{PrePer}(f)$.
- A **periodic cycle** is a finite set $S \subset X$ s.t. $f|_S$ is a transitive permutation.
- $x \in X$ is called **almost periodic** if for any nbhd U of x, $\{i | f^i(x) \in U\}$ is relatively dense in $\mathbb{N}$, i.e. appear in every k consecutive integers for some k.
- A periodic point $x \in X$ for f with periodicity k is called **attracting** if there exists a precompact nbhd U of $x \in X$ s.t. $f(\overline{U}) \subset U$, and $\cap_{n\in\mathbb{N}} f^{(n)}(U) = \{x\}$. Similarly, x is called **repelling** if there exists a nbhd U of $x \in X$ s.t. $\overline{U} \subset f(U)$, and $\cap_{n\in\mathbb{N}} f^{(-n)}(U) = \{x\}$.
- For an attracting periodic point $x \in X$ for f, the **basin of attraction** of x is defined to be the set
$$BA(x) = \{y \in X | \exists j \in \mathbb{N}, \lim_{n\to\infty} f^{(n)}(y) = f^i(x)\}.$$
If U is a nbhd of $x \in X$ s.t. $f(\overline{U}) \subset U$, and $\cap_{n\in\mathbb{N}} f^{(n)}(U) = \{x\}$, then $BA(x) = \cup_{n\in\mathbb{Z}_+} f^{(-n)}(x)$, so it is open. The connected components $BA_0(x)$ of $BA(x)$ containing some $f^{(j)}(x)$ for $j \in \mathbb{N}$ is called the **intermediate basin of attraction** of x.
- For $x \in X$, its **ω-limit points** are defined to be
$$\omega(x) = \bigcap_{n\in\mathbb{N}} \overline{\bigcup_{i\geq n} f^i(x)}$$
- If f is invertible, for $x \in X$, its **α-limit points** are defined to be
$$\alpha(x) = \bigcap_{n\in\mathbb{N}} \overline{\bigcup_{i\leq n} f^i(x)}$$
- The set of **(positively)recurrent** points for f is defined to be $\mathcal{R}(f) = \{x \in X | x \in \omega(x)\}$.
- The set $NW(f)$ of **non-wandering points** are the points x that for any nbhd U of x, there is an $n > 0$ that $f^n(U) \cap U = \varnothing$.
- Denote the orbit sets $\mathcal{O}(x) = \bigcup_{n\in\mathbb{Z}} f^n(x), \quad \mathcal{O}^+(x) = \bigcup_{n\geq 0} f^n(x)$.

- Let X be compact, then a closed non-empty forward f-invariant $Y \subset X$ is called a **minimal set** for f if there is no smaller such set.

⌟

Prop. (11.18.1.4).

- $NW(f)$ is closed, f-invariant, and contains $\alpha(x), \omega(x)$ for all x.
- Every recurrent point is non-wandering, thus $\overline{\mathcal{R}(f)} \subset NW(f)$.
- Let X be compact Hausdorff, then $\overline{\mathcal{O}^+(x)}$ is minimal for f iff x is almost periodic.

⌟

Proof: item1 is easy, 2 follows from1 as $x \in \omega(x)$.

For3: suppose x is almost periodic and $y \in \overline{\mathcal{O}^+(x)}$, we need to show that $x \in \overline{\mathcal{O}^+(y)}$. For any nbhd $x \in U$, there is a small nbhd $x \in U' \subset U$ and a nbhd $\Delta \subset V \subset X \times X$, that if $x_1 \in U'$ and $(x_1, x_2) \in V$, then $x_2 \in U$. Since x is periodic, there is a K that for any $j \geq 0$, there is a $f^{j+k}(x) \in U'$ for some $0 \leq k \leq K$. Let $V' = \cap_{i=0}^K f^{-1}(V)$, then V' is open and contains the diagonal. Thus there is a nbhd W of y that $W \times W \subset V'$. Now choose $f^n(x) \in W$ by almost periodicity, and $f^{n+k}(x) \in U'$ for some $0 \leq k \leq K$, then we have $(f^{n+k}(x), f^k(x)) \in V$ by the definition of V' and W, and hence $f^k(x) \in U$. This shows $x \in \overline{\mathcal{O}^+(y)}$.

Conversely, if x is not almost periodic, then there is a nbhd U of x, that there is a sequence $\{a_i\} \in \mathbb{N}$, that $f^{a_i+j}(x) \notin U$ for $j \leq i$. By convergence theorem and passing to a subsequence, we assume y is a the limit of $f^{a_i}(x)$, and $f^j(y) \notin U$ for any $j > 0$, thus $x \notin \overline{\mathcal{O}^+(y)}$, showing $\overline{\mathcal{O}^+(x)}$ is not minimal. □

Prop. (11.18.1.5) [Minimal Set Exists on Compact Dynamic System]. If f is a topological dynamic system on a compact space, then there exists a minimal set. In particular, there exists an almost periodic point, in priori positively recurrent point, by(11.18.1.4). ⌟

Proof: Use Zorn's lemma and the finite intersection property. □

Def. (11.18.1.6) [Topologically Transitive]. A topological dynamic system $f : X \to X$ is called **topologically transitive** if there is a point x that $\overline{\mathcal{O}(x)} = X$. ⌟

Prop. (11.18.1.7). Let f be a continuous map of a locally compact Hausdorff second countable space X. Suppose that for any two non-empty open set U, V, there is $n > 0$ that $f^n(U) \cap V \neq \varnothing$, then f is topologically transitive. ⌟

Proof: For any open subset V, the hypothesis says $\cup_{n>0} f^{-n}(V)$ is dense in X. Let V_i be a countable basis for the topology of X, and $Y = \cap_i \cup_{n>0} f^{-n}(V_i)$, then it is non-empty, by Baire category theorem(4.4.9.2). Now the orbit of any $y \in Y$ enters every V_i, thus its orbit is dense in X. □

Prop. (11.18.1.8). Let $f : X \to X$ be a homeomorphism of a compact metric space, and suppose X has no isolated points, then if there is a dense orbit $\mathcal{O}(x)$, there will be a dense orbit $\mathcal{O}^+(x)$. ⌟

Proof: The hypothesis that X has no isolated points shows that $\mathcal{O}(x)$ meets every open subset U infinitely many times, thus we can choose $f^{n_k}(x) \in B(x, 1/k)$ that $|n_k| \to \infty$. Thus $f^{n_k+l}(x) \to f^l(x)$ for any l.

If there are infinitely many $n_k > 0$, then we have $\mathcal{O}(x) \subset \overline{\mathcal{O}^+(x)}$, hence $\mathcal{O}^+(x)$ is dense. If there are infinitely many $n_k < 0$, then $\mathcal{O}^-(x)$ is dense. Then for any open subset U, V, we can find $i < j < 0$ that $f^i(x) \in U, f^j(x) \in V$, thus $f^{j-i}(U) \cap V \neq \varnothing$. Hence we use(11.18.1.7) to conclude f is topologically transitive. □

Def. (11.18.1.9) [Topological Mixing]. A topological dynamic system $f : X \to X$ is called **topologically mixing** if for any two non-empty open subsets U, V, there is $N > 0$ that $f^n(U) \cap V \neq \varnothing$ for any $n \geq N$. ⌟

Def. (11.18.1.10). A homeomorphism $f : X \to X$ is called **expansive** if there is a $\delta > 0$ that for any two distinct points x, y, there is some $n \in \mathbb{Z}$ that $d(f^n(x), f^n(y)) \geq \delta$. Similarly, we can define **positively expansive** for a non-invertible continuous map $f : X \to X$. This constant δ is called a **expansiveness constant** of f. ⌟

Prop. (11.18.1.11) [Compact Metric Space not positively expansive]. If f be a continuous map of an infinite compact metric space X, then it is not positively expansive. ⌟

Proof: First assume f is invertible. Fix $\varepsilon > 0$, consider all m that there are points $x \neq y$ that

$$d(f^n(x), f^n(y)) < \varepsilon, \quad 0 < n \leq m, \quad d(x, y) \geq \varepsilon.$$

If these m are infinite, then we can use convergence point theorem to find a point x, y that $d(f^n(x), f^n(y)) < \varepsilon$ for any $n > 0$, thus f is not expansive.

If these m are finite, let M be a maximal, then by absolute convergence, there is a δ that if $d(x, y) \leq \delta$, then $d(f^n(x), f^n(y)) < \varepsilon$ for any $0 \leq n \leq m$. Then by definition of M, $d(f^{-1}(x), f^{-1}(y)) < \varepsilon$, and similarly $d(f^{-n}(x), f^{-n}(y)) < \varepsilon$ for any $n < 0$.

Now choose a finite $\delta/2$-net $\{x_i\}$ of M, then for each $j \in \mathbb{Z}$, there are two $f^j(x_s), f^j(x_t)$ in the same $B(\delta/2, x_j)$, thus $d(f^n(x_s), f^n(x_t)) < \varepsilon$ for $n \leq j$. Now there are only f.m. pairs of elements in M, there are some pair (x_α, x_β) appeared infinitely many times for different $j > 0$, thus we have $d(f^n(x_\alpha), f^n(x_\beta)) < \varepsilon$ for any $n \in \mathbb{Z}$.

For the non-invertible case, the proof is the same, noticing that f^{-1} is chosen wisely when it can be defined. □

Cor. (11.18.1.12). Let f be an expansive homeomorphism of an infinite compact metric space X, then there are distinct points x_0, y_0 that $\lim_{n\to\infty} d(f^n(x_0), f^n(y_0)) = 0$. ⌟

Proof: Let δ be an expansive constant of f, then by(11.18.1.11), there are $x_0 \neq y_0 \in X$ that $d(f^n(x_0), f^n(y_0)) \leq \delta$ for all $n > 0$. Suppose $d(f^n(x), f^n(y)) \nrightarrow 0$, then by compactness in $X \times X$, there is a subsequence $\{n_k\} \in \mathbb{N}$ that $f^{n_k}(x) \to x', f^{n_k}(y) \to y'$ with $x' \neq y'$. Then this will show that $d(f^m(x), f^m(y)) < \delta$ for any $m \in \mathbb{Z}$, contradicting expansiveness of f. □

Def. (11.18.1.13). Let $f : X \to X$ be a homeomorphism of compact Hausdorff space, then

- two points x, y are called **proximal** if the closure of orbits $\overline{\mathcal{O}((x, y))}$ under $f \times f$ intersect the diagonal $\Delta \subset X \times X$. It is called **distal** otherwise. f is called **distal** if every two distinct points x, y are distal.
- f is called **equicontinuous** if the family $\{f^n\}_{n\in\mathbb{Z}}$ is equicontinuous.

⌟

Prop. (11.18.1.14). A equicontinuous homeomorphism f of a compact metric space are distal. ⌟

Proof: Suppose f is not distal, then there is a proximal pair (x, y), thus there is a sequence $\{n_k\} \in \mathbb{Z}$ that $d(f^{n_k}(x), f^{n_k}(y)) \to 0$. let $d(x, y) = \varepsilon$, thus for any $\delta > 0$, there is some $d(f^{n_k}(x), f^{n_k}(y)) < \varepsilon$, thus contradicting the equicontinuity of f^{-n}. □

Def. (11.18.1.15) [Almost Periodic Set]. For a subset $A \subset X$ and a homeomorphism $f : X \to X$, denote by f_A the action of f on X^A. Then A is called **almost periodic** if every $z \in \mathrm{Mor}(A, A)$ is almost periodic for f_A. Equivalently, for any finite set of points $\{x_i\} \in A$, and nbhds $x_i \in U_i$, the set $\{k \in \mathbb{Z} | f^k(x_i) \in U_i\}$ is relatively dense in $\mathbb{Z}$. This is compatible with the previous definition of almost periodic point(11.18.1.3). ⌟

Def. (11.18.1.16). A homeomorphism of a compact Hausdorff space is called **pointwise almost periodic** if every point x is almost periodic. By(11.18.1.4), we can see that this is equivalent to X is a union of minimal sets. ⌟

Lemma (11.18.1.17). Every almost periodic set A is contained in a maximal almost periodic set in X. ⌟

Proof: It is because of the second definition of almost periodic set(11.18.1.15) that the sum of an ordered family of almost periodic sets is also almost periodic. □

Prop. (11.18.1.18). Let f be a homeomorphism of a compact Hausdorff space X, then every point $x \in X$ is proximal to an almost periodic point. ⌟

Proof: If x is almost periodic, then we are done. If not, consider a maximal almost periodic set $A \subset X$, then $x \notin A$. Then for $z \in X^A$ with range A, consider $(x, z) \in X \times X^A$, and find an almost periodic point (x_0, z_0) of $f \times f_A$ in $\overline{\mathcal{O}(x, z)}$, by(11.18.1.5). Because z is almost periodic, $z \in \overline{\mathcal{O}(z_0)}$, by(11.18.1.4). Thus we see $(x', z) \in \overline{\mathcal{O}(x_0, z_0)}$ for some x', by the compactness of X. Then (x', z) is also almost periodic, and we can forget about x_0, z_0.

Therefore, $\{x'\} \cup \mathrm{Im}(z) = \{x'\} \cup A$ is almost periodic for f, and since A is maximal, $x' \in A = \mathrm{Im}(z)$. This shows $(x', x') \in \overline{\mathcal{O}(x, x')}$, showing x is proximal to x'. □

Cor. (11.18.1.19)[Distal Homeomorphism is Pointwise Almost Periodic]. If f is a distal homeomorphism of a compact Hausdorff space, then f is pointwise almost periodic. ⌟

Prop. (11.18.1.20).

- A homeomorphism of a compact Hausdorff space is distal iff the product system $(X \times X, f \times f)$ is pointwise almost periodic.
- A factor system of a pointwise almost periodic homeomorphism is pointwise almost periodic.
- A factor system of a distal homeomorphism is distal.

⌟

Proof: 1: If f is distal, then so is $f \times f$, hence it is pointwise almost periodic, by(11.18.1.19). Conversely, if $f \times f$ is pointwise almost periodic, then if x, y is proximal, then $(z, z) \in \overline{\mathcal{O}(x, y)}$, but since $\overline{\mathcal{O}(x, y)}$ is minimal, by(11.18.1.4), $(x, y) \subset \overline{\mathcal{O}(z, z)} \subset \Delta$, hence $x = y$.

2: This is easy.

3: if f is a factor of g, then $f \times f$ is a factor of $g \times g$, but the latter is pointwise locally periodic, thus the first is also locally periodic, by2, and then f is distal, by1. □

Topological Entropy

Def. (11.18.1.21)[Definitions]. Let (X, d) be a compact metric space, and f a continuous map $X \to X$, we define

- for $x, y \in X$, $d_n(x, y) = \max_{0 \le k \le n-1} d(f^k(x), f^k(y))$.

- a subset $A \subset X$ is called (n,ε)**-spanning** if it is a ε-net in (X, d_n). Similarly, we can define (n,ε)**-separated** and $\mathrm{cov}(n,\varepsilon,f)$ the minimal number of covering of X of d_n-diameter$<\varepsilon$.

⌟

Lemma (11.18.1.22). $\mathrm{cov}(n, 2\varepsilon, f) \le \mathrm{span}(n,\varepsilon,f) \le \mathrm{sep}(n,\varepsilon,f) \le \mathrm{cov}(n,\varepsilon,f)$. ⌟

Proof: Easy. □

Prop. (11.18.1.23) [Topological Entropy]. The number

$$\lim_{n\to\infty} \frac{1}{n} \log(\mathrm{cov}(n,\varepsilon,f)) = h_\varepsilon(f)$$

is well-defined and finite. It is increasing as ε decreces, so $h(f) = \lim_{\varepsilon\to 0^+} h_\varepsilon(f)$ exists, which lies in $[0,\infty]$. It is called the **topological entropy** of f.

Notice the entropy can be calculated by either cov, span or sep, by(11.18.1.22). ⌟

Proof: For this, we need to notice if U has d_n-diameter$<\varepsilon$ and V has d_m-diameter$<\varepsilon$, then $U \cap f^{-m}(V)$ has d_{m+n}-diameter$<\varepsilon$. Hence

$$\mathrm{cov}(m+n,\varepsilon,f) \le \mathrm{cov}(m,\varepsilon,f)\cdot \mathrm{cov}(n,\varepsilon,f).$$

Thus we can use(2.6.1.1) to conclude. □

Prop. (11.18.1.24). The topological entropy doesn't depend on the metric generating the topology. ⌟

Proof: This is because d' is a continuous function on $(X\times X, d\times d)$, thus it is uniformly continuous as X is compact, so

$$\mathrm{cov}(n,\varepsilon,f) \le \mathrm{cov}(n,\delta(\varepsilon),f)$$

where $\delta(\varepsilon)\to 0$ when $\varepsilon\to 0$. This shows the topological entropies are the same. □

Cor. (11.18.1.25). Two conjugate dynamic systems have the same topological entropy. ⌟

Prop. (11.18.1.26) [Properties of Entropy]. Let $f : X \to X$ be a continuous map of a compact metric space X, $g : Y \to Y$ be a continuous map of a compact metric space Y, then

- $h(f^m) = m\cdot h(f)$ for $m > 0$.
- If f is invertible, then $h(f^{-1}) = h(f)$.
- Let A_i be a finite family closed forward f-invariant subsets of X whose union is X, then

$$h(f) = \max h(f|_{A_i}).$$

- $h(f\times g) = h(f) + h(g)$, and if f is an extension of g, then $h(f) \ge h(g)$.

⌟

Proof: 1: Use two inequalities:

$$\mathrm{span}(n,\varepsilon,f^m) \le \mathrm{span}(mn,\varepsilon,f), \quad \mathrm{span}(n,\delta(\varepsilon),f^m) \ge \mathrm{span}(mn,\varepsilon,f)$$

where $\delta(\varepsilon)\to 0$ if $\varepsilon\to 0$, and(11.18.1.22).

2: Because (n,ε)-separated sets for f and (n,ε)-separated sets for f^{-1} corresponds via f^n.

3: Use two inequalities:

$$\operatorname{span}(n,\varepsilon,f) \le \sum_{i=1}^{k} \operatorname{span}_i(n,\varepsilon,f) \le k \cdot \max \operatorname{span}_i(n,\varepsilon,f),$$

$$\operatorname{sep}(n,\varepsilon,f) \ge \max \operatorname{sep}(n,\varepsilon,f).$$

4: Noticing two inequalities:

$$\operatorname{cov}(n,\varepsilon,f\times g) \ge \operatorname{cov}(n,\varepsilon,f)\cdot \operatorname{cov}(n,\varepsilon,g),$$

$$\operatorname{sep}(n,\varepsilon,f\times g) \ge \operatorname{sep}(n,\varepsilon,f)\cdot \operatorname{sep}(n,\varepsilon,g).$$

and the proof of the last assertion is similar to that of(11.18.1.24). □

Prop. (11.18.1.27). Let $f : X \to X$ be an expansive homeomorphism of a compact metric space of expansiveness constant δ, then $h(f) = h_\varepsilon(f)$ for $\varepsilon < \delta$. ⌟

Proof: For $0 < \gamma < \varepsilon < \delta$, we show that $h_{2\gamma}(f) = h_\varepsilon(f)$. For this, it suffices to prove≤. By expansiveness, if $x \neq y$, then there is some $i \in \mathbb{Z}$ that $d(f^i(x), f^i(y)) \ge \delta > \varepsilon$. Since the set $\{(x,y) \in X \times X | d(x,y) \ge \gamma\}$ is compact, there is a $k = k(\gamma,\varepsilon)$ that if $d(x,y) \ge \gamma$, then $d(f^i(x), f^i(y)) > \varepsilon$ for some $|i| \le k$. Thus if A is a (n,γ)-separated set, then $f^{-k}(A)$ is a $(n+2k,\varepsilon)$-separated set. Hence by(11.18.1.22), $h_{2\gamma}(f) \le h_\varepsilon(f)$. □

Application to Ramsey Theory

Def. (11.18.1.28) [IP-System]. Let $\mathcal{F}$ be the collection of all finite non-empty subset of $\mathbb{N}$. For $\alpha,\beta \in \mathcal{F}$, write $\alpha < \beta$ if every element of α is smaller than that of β.

For a commutative group G, an **IP-system** in G is a map $T : \mathcal{F} \to G$ that $T_{i_1,\ldots,i_k} = T_{i_1} \cdot \ldots \cdot T_{i_k}$. ⌟

Prop. (11.18.1.29)[Furstenberg-Weiss]. Let G be a commutative group acting minimally on a compact topological space X, then for any open subset U of X, $n > 0$ and $\alpha \in \mathcal{F}$, and any IP-systems $T^1,\ldots,T^n$ on G(11.18.1.28), there is a $\beta \in \mathcal{F}$ that $\alpha < \beta$, and

$$U \cap T^1_\beta(U) \cap \ldots \cap T^n_\beta(U) \neq \varnothing.$$

⌟

Proof: Cf.[Dynamic System, P49]. □

Cor. (11.18.1.30). Let G be a commutative group acting homeomorphically on a compact metric space X and $T^1,\ldots T^n$ be IP-systems on G, then for any $\alpha \in \mathcal{F}$ and $\varepsilon > 0$, there are $x \in X$ and $\beta > \alpha$ that $d(x, T^i_\beta(x)) < \varepsilon$ for any i. ⌟

Proof: Just need to find a minimal closed subset of X for G, but this is easy by finite intersection theorem. □

Cor. (11.18.1.31) [Multiple Recurrence Property]. Let T be a homeomorphism of a compact metric space X, then for any $\varepsilon > 0$ and $q > 0$, there are $p > 0$ and $x \in X$ that $d(T^{jp}(x), x) < \varepsilon$ for $0 \le j \le q$. ⌟

Proof: This is a special case of(11.18.1.30), by taking $G = \{T^k\}$, and $T^i_\alpha = T^{i|\alpha|}$, where $|\alpha|$ is the sum of elements in α. □

Cor. (11.18.1.32)[Generalized van der Waerden Theorem]. For each finite partition $\mathbb{Z} = \cup_{i=1}^m S_k$, one of the the subset S_k contains arbitrarily long arithmetic progressions.

More generally, let A be a finite subset of $\mathbb{Z}^d$, then for each partition $\mathbb{Z}^d = \cup_{i=1}^m S_k$, there are some k, $z_0 \in \mathbb{Z}^d$ and $n > 0$ that $z_0 + na \in S_k$ for any $a \in A$. ⌟

Proof: Consider the product space $\Sigma_m = \{1, 2, \ldots, m\}^{\mathbb{Z}}$ with the 2-adic metric with shifting σ. Then a partition of $\mathbb{Z}$ can be viewed as an element ξ in $\{1, 2, \ldots, m\}^{\mathbb{Z}}$, with $\xi_i = k$ if $i \in S_k$. Let $X = \overline{\cup_{i=-\infty}^{\infty} \sigma^i(\xi)}$. Let $A_k = \{\omega \in X | \omega_0 = k\}$, then if $x \in A_k, y \in X$ with $d(x, y) < 1$, then $y \in A_k$ also. Thus for any $q > 0$, we can use(11.18.1.31) to show that there is an $\omega \in X$ that $d(\sigma^{ip}(\omega), \omega) < 1$ for $0 \leq i \leq q$, thus there is an $r \in \mathbb{Z}$ that $\xi_j = \omega_0$ for $j = r, r + k, \ldots, r + pq$. And this proves the theorem.

The proof of the general case is similar. □

2 Symbolic Dynamics

Shifts

Def. (11.18.2.1) [Subshifts]. A **subshift** is a closed subset $X \subset \Sigma_m$ that is invariant under the shift σ and σ^{-1}. A map between to subshifts of Σ_m is called a **code** if it commutes with σ. ⌟

Prop. (11.18.2.2). Let X be a subshift of Σ_m(11.18.2.1), let $W_n(X)$ be the set of words of length n that occurs in X, $\sigma|_X$ is clearly expansive of constant 1, thus we have

$$h(\sigma|_X) = \lim_{n\to\infty} \frac{1}{n} \log |W_n(X)|.$$

⌟

Proof: This is because every element in W_n appears in the first n term of some $\omega \in X$, and elements in a set of d_n-diameter< 1 has first n entries the same. For the other direction, notice a $(n, 1)$-separated set has the first n-entries not the same, thus contribute to different elements in $W_n(X)$, thus $\mathrm{sep}(n, 1, \sigma|_X) < W_n(X)$. □

Def. (11.18.2.3) [block code]. Let X be a subshift, $k, l \geq 0, n = k + l + 1$, and α be a map from $W_n(X)$ to $\{0, 1, \ldots, m' - 1\}$, then a (k, l)-block code is a morphism from X to $\Sigma_{m'}$ that maps x to the sequence $a_\alpha(x)$ that $a_\alpha(x)_i = \alpha((x_{i-k}, \ldots, x_{i+l}))$.

When $\{0, 1, \ldots, m' - 1\}$ is chosen to be $W_n(X)$ itself, then this is called a **higher block presentation** of X. ⌟

Prop. (11.18.2.4) [Every Code is a block code, Curtis–Lyndon–Hedlund]. Every code $c : X \to Y$ is a block code. ⌟

Proof: Let $\mathcal{A}$ be the symbol set of Y, define $\widehat{c} : X \to \mathcal{A} : x \mapsto c(x)_0$. This is a continuous map, and X is compact thus it is uniformly continuous, thus there is a $\delta > 0$ that $\widehat{c}(x) = \widehat{c}(y)$ if $d(x, y) < \delta$. Thus there is a large k that $\widehat{c}$ only depends on the first $2k + 1$ term, and it commutes with shifting, thus it is a block code. □

Def. (11.18.2.5) [SFT]. For $k \in \mathbb{Z}_+$, a **subshift of finite type** or SFT of k-step is a subshift X that are defined to be the elements in Σ_m that doesn't contain some set of words of length $k + 1$. When $k = 1$, this is also called a **topological Markov chain**. ⌟

Prop. (11.18.2.6). Every SFT is isomorphic to a vertex shift. ⌟

Proof: For this SFT X of step k, construct a graph, whose vertices are $W_k(X)$, and two element of $W_k(X)$ are connected by an edge if they adjoint to an element in $W_{k+1}(X)$. □

Cor. (11.18.2.7). Every SFT is isomorphic to an edge shift. This is because every vertex shift can be 2-block isomorphic to its edge shift. ⌟

Prop. (11.18.2.8) [Perron]. ⌟

Sofic Shifts and Data Transmission

Def. (11.18.2.9) [Sofic Shifts]. A subshift $X \subset \Sigma_m$ is called **sofic** if it is a factor of a subshift of finite type. ⌟

Prop. (11.18.2.10). A subshift $X \subset \Sigma_m$ is sofic iff it is isomorphic to an infinite path shift for some directed graph Γ(Notice that different edge in Γ can be labeled the same). ⌟

Proof: Clearly such a path shift is a factor of the edge shift of Γ, thus it is sofic. Conversely, A sofic shift is a factor of some edge shift $c : \Sigma^e_A \to X$, by(11.18.2.7), and c is a block code, by(11.18.2.3). Composing with the higher block code presentation, we may assume c is a $(0, 1)$-block code, □

3 Ergodic Theory

Prop. (11.18.3.1) [Poincaré's Recurrence Theorem]. Let T be a measure-preserving transformation of a finite measure space X, if A is a measurable set, then for a.e. $x \in A$, there is some $n > 0$ that $T^n(x) \in A$. ⌟

Proof: Let B be the set of points contradicting this property, $B = A \setminus \cup_{k>0} T^{-k}A$, thus all the preimages $T^{-k}B$ are disjoint, measurable and have the same measure as B, thus it must has measure 0 as X has finite measure. □

Cor. (11.18.3.2) [Derivarive Transformation]. Given a finite measurable space and a measure-preserving map $T : X \to X$ and a measurable subset A of finite measure, then the **derivative transformation** $T_A : A \to A : x \mapsto T^k(x)$, where $k > 0$ is the first integer that $T^k(x) \in A$. By Poincaré's Recurrence theorem, the derivative transformation is defined on a subset of full measure. ⌟

Prop. (11.18.3.3). Let X be a second countable metric space and μ a Borel probability measure on X, and $f : X \to X$ is a measure preserving continuous map, then a.e. point $x \in X$ is recurrent, i.e. $\operatorname{Supp} \mu \subset \mathcal{R}(f)$. ⌟

Proof: There is a countable family of basis $\{U_i\}$ of nbhds of X, and for each U_i, elements in U_i returns to U_i except for a set X_i of measure0. Then $\mathcal{R}(f) = X \setminus \bigcup_i X_i$ has full measure. □

Def. (11.18.3.4) [Ergodicity]. A measure-preserving transformation T of a measure space X is called **ergodic** if any essentially T-invariant measurable subset has measure 0 or full measure. ⌟

Prop. (11.18.3.5). Let T be a measure-preserving transformation on a finite measure space X and $p \in (0, \infty]$, then T is ergodic iff every essentially T-invariant function $f \in L^p(X, \mu)$ is constant. ⌟

Proof:

□

Prop. (11.18.3.6). Let X be a measure space and f is an essentially invariant function for a measure-preserving map or flow Ton X, then there is a strictly invariant measurable function $\widehat{f}$ that $f=\widehat{f}$ a.e.. ⌟

Proof: [Dynamic System P74]. □

Def. (11.18.3.7). A measure-preserving transformation or flow on a probability space X is called **mixing** if

$$\lim_{t\to\infty}\mu(T^{-t}A\cap B)=\mu(A)\mu(B).$$

It is called **weak mixing** if

$$\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n}|\mu(T^{-i}A\cap B)-\mu(A)\mu(B)|=0.$$

or

$$\lim_{t\to\infty}\frac{1}{t}\int_0^t|\mu(T^{-t}A\cap B)-\mu(A)\mu(B)|=0.$$

⌟

Prop. (11.18.3.8). Mixing transformation is weak mixing, and weak mixing is ergodic. ⌟

Proof: For a weak mixing transformation, if A is essentially invariant, then $\mu(A)=\mu(A)^2$, thus $\mu(A)=1$ or 0. □

Prop. (11.18.3.9)[Mixing and Topological Mixing]. Let X be a compact metric space, $T:X\to X$ be a continuous map and μ a T-invariant Borel measure on X, then

- If T is ergodic, then the orbit of a.e. point $x\in X$ is dense in $\operatorname{Supp}\mu$.
- If T is mixing, then T is topologically mixing on $\operatorname{Supp}\mu$.

⌟

Proof: 1: Let U be an open subset intersecting $\operatorname{Supp}\mu$, then the T-invariant subset $\cup_{k>0}T^{-k}U$ has full measure, thus the forward orbit of a.e. x intersect U. Then take a countable open basis of X, thus the forward orbit of a.e. x is dense in $\operatorname{Supp}\mu$.

2: Because $\lim_{t\to\infty}T^{-t}(A)\cap B\to\mu(A)\mu(B)>0$, so does $\lim_{t\to\infty}A\cap T^t(B)$. □

Ergodic Theorems

Prop. (11.18.3.10) [von Neumann Ergodic Theorem]. If $U\in L(H)$ is unitary and $x\in H$, then the average $A_nx=\frac{1}{n}(x+Ux+\ldots+U^{n-1}x)$ converges to some Px, where P is the projection to the fixed space of U. ⌟

Proof: Define $a_n=\frac{1}{n}(1+\lambda+\ldots+\lambda^{n-1})$ on the unit circle, and $b(1)=\chi_{\{1\}}$, then if $y=b(U)x=P(x)$, then $||y-A_nx||^2=\int_{\sigma(U)}|b-a_n|^2dE_{x,x}(\lambda)$. But this integral converges to 0 by dominated convergence theorem. □

Prop. (11.18.3.11) [Birkhoff Ergodic Theorem]. If T is a measure-preserving transformation of a finite measure space (X,μ), and let $f\in L^1(X,\mu)$, then the limit

$$\overline{f}(x)=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}f(T^k(x))$$

exists for a.e. x and is μ-integrable and T-invariant, and satisfies

$$\int_X \overline{f}(x)d\mu = \int_X f(x)d\mu$$

In addition, if $f \in L^2(X,\mu)$, then $\overline{f}$ is just the projection of f to the subspace of T-invariant measures.

The same thing is true for a measure-preserving flow. ⌟

Proof: Let

$$A = \{x \in X | f(x) + f(T(x)) + \ldots + f(T^k(x)) \geq 0, \quad \exists k \geq 0\}.$$

Then firstly we have $\int_A f(x)d\mu \geq 0$: Cf.[Dynamic System, P82].**?** □

Cor. (11.18.3.12). A measure-preserving map $T: X \to X$ in a finite measure space (X,μ) is ergodic iff for each $f \in L^1(X,\mu)$,

$$\lim_{n\to\infty} \frac{1}{n}\sum_{i=0}^{n-1} f(T^i(x)) = \frac{1}{\mu(X)}\int_X f(x)d\mu, a.e.x.$$

I.e., the time average equals the space average for any L^1-function. ⌟

Proof: If T is ergodic, then the function $\overline{f}$ defined in(11.18.3.11) is a constant, thus the equation. Conversely, if this equation holds, then if f is T-invariant, the RHS is constant. □

Cor. (11.18.3.13). Taking a dense subset of $L^2(X,\mu)$ in the above corollary, we see that a measure-preserving map $T: X \to X$ is ergodic iff for any measurable subset A and a.e. $x \in X$,

$$\lim_{n\to\infty} \frac{1}{n}\sum_{i=0}^{n-1} \chi_A(T^i(x)) = \frac{\mu(A)}{\mu(X)}.$$

⌟

Invariant Measure for a Transformation

4 Hyperbolic Dynamics

11.19 Complex Dynamical Systems

See [Milnor, John Dynamics in one complex variable], [Complex Dynamics and Renormalization, McMullen] and [C-G93].

1 Local Behaviors

Notation (11.19.1.1).
- For $d \in \mathbb{Z}_{\geq 2}$, denote Rat_d the set of non-constant rational maps $f : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ of degree d. And denote $\mathrm{Rat} = \bigcup_{d\in\mathbb{Z}_{\geq 2}} \mathrm{Rat}_d$.

⌟

Def. (11.19.1.2) [Attracting and Repelling]. For a Riemann surface Ω and $f : \Omega \to \Omega$, suppose $x \in \Omega$ is a periodic point for f of periodicity k, the **Multiplier** of f at x is defined to be $\lambda_f(x) = (f^{(k)})'(x) \in \mathbb{C}$. Then x is called
- an **anattracting point** for f iff $|\lambda_f(x)| < 1$.
- a **repelling pint** for f iff $|\lambda_f(x)| > 1$.
- a **superattracting point** if $\lambda_f(x) = 0$.
- called a **rationally neutral point** if $\lambda_f(x) \in \mu(\mathbb{C})$.
- called an **irrationally neutral point** if $|\lambda_f(x)| = 1$ but $\lambda_f(x) \notin \mu(\mathbb{C})$.

Hyperbolic points and irrationally neutral points are all called **neutral points** of f. ⌟

Def. (11.19.1.3) [Stable Points]. For a Riemann surface Ω and $f : \Omega \to \Omega$, suppose $x \in \Omega$ is a fixed point of f, then x is called a **stable point** if there exists $0 \leq r_0, r \leq R$ s.t. $f^{\circ n}(z) \in \mathbb{D}(z_0, r)$ for any $z \in \mathbb{D}(z_0, r_0), n \in \mathbb{Z}_+$.

Later it will be clear that a fixed point z_0 is stable iff $z_0 \in \mathrm{Fat}(f)$(11.19.3.1). ⌟

Prop. (11.19.1.4) [Attracting Fixed Points, Koenigs]. Suppose $f \in \mathcal{O}(\mathbb{C})$ has an attracting fixed point $z_0 \in \mathbb{C}$ with $\lambda = f'(z_0) \in B(0, (0, 1))$. Then there is a unique conformal mapping φ from a nbhd of z_0 to a nbhd of 0 that conjugates f to the linear function $g(\zeta) = \lambda\zeta$, and $\varphi'(z_0) = 1$. ⌟

Proof: The uniqueness is clear. For the existence, suppose $z_0 = 0$. For $n \in \mathbb{Z}_+$, let $\varphi_n = \lambda^{-n} f^{(n)}$, then φ_n satisfies $\varphi_n \circ f = \lambda\varphi_{n+1}$. If there exists $\varphi \in \Omega(\mathbb{C})$ s.t. $\varphi_n \to \varphi$ pointwise, then $\varphi \circ f = \lambda\varphi$.

Notice for $\delta \in \mathbb{R}_+$ small, $|f(z)-\lambda z| \leq C|z|^2$ for any $|z| \leq \delta$. So $|f(z)| \leq |\lambda z|+C|z|^2 \leq (|\lambda|+C\delta)|z|$. So when δ is small s.t. $|\lambda| + C\delta < 1$,

$$|f^{(n)}(z)| \leq (|\lambda| + C\delta)^n|z|, \quad \forall |z| \leq \delta.$$

If δ is small s.t. $\rho = (|\lambda| + C\delta)^2/|\lambda| < 1$, then

$$|\varphi_{n+1}(z) - \varphi_n(z)| = |\frac{f(f^{(n)}(z)) - \lambda f^{(n)}(z)}{\lambda^{n+1}}| \leq \frac{C|f^{(n)}(z)|^2}{|\lambda|^{n+1}} \leq \frac{\rho^n C|z|^2}{|\lambda|}.$$

So φ_n converges uniformly for $|z| \leq \delta$, to some holomorphic function φ. □

Cor. (11.19.1.5) [Repelling Fixed Points]. The same applies to repelling fixed points, because we can consider $f^{(-1)}$ instead. The corresponding Schröder's equation for $h = \varphi^{(-1)}$ is $h(\lambda\zeta) = f(h(\zeta))$. Then it can be verified that h can be extended to an entire function of finite order. ⌟

Prop. (11.19.1.6) [Superattracting Fixed Points, Boettcher]. Suppose $f \in \mathcal{O}(\mathbb{C})$ has a superattracting fixed point $z_0 \in \mathbb{C}$ of order $p \geq 2$ s.t. $f(z) = z_0 + a_p(z - z_0)^p + \ldots$, then there exists a conformal mapping φ of some nbhd of z_0 to a nbhd of 0 that conjugates f to the mapping $g(\zeta) = \zeta^p$. And the conjugation is unique up to multiplication by a $(p-1)$-th roots of unity. ⌟

Proof: Suppose $z_0 = 0$. If we change variables $w = cz$ with $c^{p-1} = 1/a_p$, then $f(w) = w^p + \ldots$. Let $\varphi_n = (f^{(n)})^{p^{-n}}$, then $\varphi_{n-1} \circ f = (f^{(n-1)} \circ f)^{p^{-n+1}} = \varphi_n^p$. If there exists $\varphi \in \Omega(\mathbb{C})$ s.t. $\varphi_n \to \varphi$ pointwise, then $\varphi \circ f = \varphi^p$.

Notice for $\delta \in \mathbb{R}_+$ small, $|f(z)| \leq C|z|^p$ for some $C \in \mathbb{R}_{\geq 1}$. So $|f^{(n)}(z)| \leq (C|z|)^{p^n}$. Thus

$$\frac{\varphi_{n+1}}{\varphi_n} = (\frac{\varphi_1 \circ f^{(n)}}{f^{(n)}})^{p^{-n}} = (1 + O(|f^{(n)}|))^{p^{-n}} = 1 + O(p^{-n}(C|z|)^{p^n}) = 1 + O(p^{-n}),$$

when $|z| \leq 1/C$. So $\prod_n \frac{\varphi_{n+1}}{\varphi_n}$ is uniformly bounded for $|z| \leq 1/C$, so φ_{n+1} converges to some holomorphic function φ. □

Prop. (11.19.1.7) [Neutral Fixed Points]. Suppose $f \in \mathcal{O}(\mathbb{C})$ has a neutral fixed point $z_0 \in \mathbb{C}$ with $f'(z_0) = \lambda$. We may find a local conformally mapping λ from a nbhd of z_0 to a nbhd of 0 that conjugates f to a linear function $g(\zeta) = \lambda\zeta$. If $h = \varphi^{(-1)}$, then h must satisfy the Schröder's equation

$$h(\lambda\zeta) = f(h(\zeta)).$$

Then this equation is solvable iff z_0 is a stable points for f(11.19.1.3) ⌟

Proof: Suppose z_0 is stable, let $\Omega = \cup_{n \in \mathbb{Z}_+} f(\mathbb{D}(z_0, r_0))$, then $\Omega \subset \mathbb{D}(0, r)$ and is connected. Suppose $\varphi : \mathbb{D} \to \Omega$ is a covering map that $\varphi(0) = 0$(11.4.7.10), then the map $f : \Omega \mapsto \Omega$ lifts to a map $F : \mathbb{D} \to \mathbb{D}$, thus by Schwartz lemma(11.5.1.3), $F(z) = \lambda z$, and the Schröder's equation has a solution φ.

Conversely, it is clear if the Schröder's equation has a solution φ, then z_0 is stable. □

Cor. (11.19.1.8). Situation as in(11.19.1.7), f is topologically conjugate to $g(\zeta) = \lambda\zeta$ near z_0 iff f is conformally conjugate to $g(\zeta) = \lambda\zeta$ near z_0. ⌟

Def. (11.19.1.9) [Siegel Disks]. A **Siegel disk** is a simply-connected f-fixed region $\Omega \subset \mathbb{C}$ s.t. the action of f on it is conjugate to a rotation.

By(11.19.1.7), if f has a fixed point z_0, then a nbhd of z_0 that is a Siegel disk iff z_0 is a stable point for f. ⌟

Thm. (11.19.1.10) [Siegel]. Situation as in(11.19.1.7),

- If $\lambda^n = 1$ for some $n \in \mathbb{Z}_+$, then z_0 is stable for f iff $f^{(m)}(z_0) = z_0$ for some $m \in \mathbb{Z}_+$. And if this is the case, then $f^{(n)} = 1$.
- If $\lambda = e^{2\pi i \omega}$ where ω is a Diophantine number(15.2.4.5), then z_0 is a stable point for $f(z)$.
- There exists a case $\lambda = e^{2\pi i \theta}$ s.t. the Schröder's equation is unsolvable.

⌟

Proof: 1: If $z = 0$ is stable, then $f^{\circ n}(z) = z$ by(11.19.1.7). Conversely, if $f^{\circ m}(z) = z$, then clearly $z = 0$ is stable.

3: Take $f(z) = \lambda z + \ldots + z^d$, and suppose there is a solution h to the Schröder's equation that covers a nbhd $\mathbb{D}(z_0, \delta)$ of z_0, then $f^{(n)}(z) = z$ has only one zero in $\mathbb{D}(0, \delta)$. But

$$f^{(n)}(z) - z = z^{d^n} + \ldots + (\lambda^n - 1)z,$$

so all the zeros except for $z =$ are outside $\mathbb{D}(0, \delta)$. Thus

$$\delta^{d^n} \leq \prod |z_j| = |\lambda^n - 1|.$$

But if we take $\lambda = e^{2\pi \mathrm{i}\, \theta}$ and $\theta = \sum_{k \in \mathbb{Z}} 2^{-q_k}$ where $q_1 < q_2 < \ldots$ is an sequences of integers increasing rapidly, then the above inequality is not possible.

2:(See also [C-G93]P43**?**) Use(11.19.1.7), the Schröder functional equation writes:

$$\sum_{k=2}^{\infty} c_k (a_1^k - a_1) \zeta^k = \sum_{l=2}^{\infty} a_l (\zeta + \sum_{r=2}^{\infty} c_r \zeta^r)^l.$$

Thus it is clear that $c_2 = a_2/a_1(a_1 - 1)$, and c_k is determined by c_2 inductively by

$$c_k = \frac{1}{a_1^k - a_1} \sum_{l_1 + \ldots + l_r = k} c_{l_1} \cdots c_{l_r}.$$

So φ is formally determined by f. Moreover, the modulus of c_k are bounded by the solution of the functional equation

$$\sum_{k=2}^{\infty} c_k |a_1^{k-1} - 1| \zeta^k = \sum_{l=2}^{\infty} |a_l| (\zeta + \sum_{r=2}^{\infty} c_r \zeta^r)^l,$$

and the bound depends positively on $|a_l|$ and negatively on $|a_1^{k-1} - 1|$.

We have $\overline{\lim} |a_n|^{\frac{1}{n}} = 1/R$, so we have $|a_n| \geq a^{n-1}$ for some $a \in \mathbb{R}_+$ and any $n \geq 2$. Notice that the Schröder functional remains true under the transformation $f(z) \mapsto af(z/a), \varphi(\zeta) \mapsto a\varphi(\zeta/a)$, so we may assume that $|a_n| \leq 1$ for $n \geq 2$. Then it suffices to show the solution $\varphi(\zeta) = \zeta + \sum_{k=2}^{\infty} \tau_k \zeta^k$ of the functional equation

$$\sum_{k=2}^{\infty} c_k |a_1^{k-1} - 1| \zeta^k = \sum_{l=2}^{\infty} (\zeta + \sum_{r=2}^{\infty} c_r \zeta^r)^l$$

has positive radius of convergence. We also denote the solution of the functional equation

$$\sum_{k=2}^{\infty} c_k \zeta^k = \sum_{l=2}^{\infty} (\zeta + \sum_{r=2}^{\infty} c_r \zeta^r)^l$$

by $\psi(\zeta) = \zeta + \sum_{k=2}^{\infty} \sigma_k \zeta^k$. Then

$$\psi(\zeta) - \zeta = \psi(\zeta)^2/(1 - \psi(\zeta)),$$

thus

$$4\psi(\zeta) = \zeta + 1 - \sqrt{1 - 6\zeta + \zeta^2}$$

has radius of convergence $R = 2 - 2\sqrt{2}$. And we can prove inductively that

$$\sigma_k \leq \delta_k \tau_k,$$

where δ_k are defined as follows:

$$\delta_1 = 1, \quad \delta_k = |a_1^{k-1} - 1| \cdot \max_{l_1 + \ldots + l_r \leq k} \delta_{l_1} \cdots \delta_{l_r}.$$

But then by(11.19.1.11), $\sigma_k < k^{-2\nu} 2^{(5\nu+1)(k-1)} \tau_k$. So $\varphi(\zeta)$ has radius of convergence$\geq (3 - 2\sqrt{2}) 2^{-5\nu - 1}$. □

Lemma (11.19.1.11). Situation as in(11.19.1.10), suppose $|a_1^n - 1| \leq (2n)^\nu$ for $\nu \in \mathbb{R}_+$ and any $n \in \mathbb{Z}_+$, then

$$\delta_k \leq k^{-2\nu} 2^{(5\nu+1)(k-1)}.$$

⌟

Proof: Cf.[Sie42]Lemma3.**?** □

Cor. (11.19.1.12). Let $f(z) = z + \sum_{k\geq 2} a_k z^k$ be a power series with positive radius of convergence, then $z = 0$ is a stable point iff $f(z) = z$. ⌟

Prop. (11.19.1.13)[Rationally Neutral Fixed Points]. Suppose $f \in \mathcal{O}(\mathbb{C})$ has a neutral fixed point $z_0 \in \mathbb{C}$ with $f(z) = \lambda z + az^{p+1} + \ldots, a \in \mathbb{C}^\times, p \in \mathbb{Z}_+$, then there is a conformally mapping φ from a "half nbhd" of z_0 to a nbhd of $\infty \in \mathscr{H} \cup \{\infty\}$ with $g(\zeta) = \zeta + 1$. ⌟

Proof: □

2 Rational Dynamics

Prop. (11.19.2.1). Any $f \in \mathrm{Rat}$ has infinitely many periodic points. ⌟

Proof: Notice the degree of $f^{(n)}(z) - z$ tends to infinity as $n \to \infty$, so if there are only f.m. periodic points $\{x_1, \ldots, x_r\}$, the multiplicity of one of these points as a period point of $f^{(n)}(z) - z$ must be large when n is large. But suppose $f^{(n)}(\xi) - \xi = 0$ and ξ has multiplicity $m \geq 2$ for $f^{(n)}$, then near ξ,

$$f^{(n)}(z) = z + (z - \xi)^m + \ldots,$$

thus for $k \in \mathbb{Z}_+$, by induction,

$$f^{(nk)}(z) = z + k(z - \xi)^m + \ldots,$$

so ξ has multiplicity m for $f^{(nk)}$. Thus we can argue that for all sufficiently divisible N, $f^{(N)}(z) - z$ has only f.m. solutions(counting multiplicity), contradiction. □

Thm. (11.19.2.2)[Shishikuka87]. For $f \in \mathrm{Rat}$, there are at most $2d-2$ attracting or neutral periodic points for f. ⌟

Proof: **?** □

Cor. (11.19.2.3). Any $f \in \mathrm{Rat}$ contains infinitely many repelling periodic points, by(11.19.2.1). ⌟

3 Julia Sets

Def. (11.19.3.1) [Fatou Sets and Julia Sets]. For any $f \in \mathrm{Rat}$, the **Fatou set** $\mathrm{Fat}(f)$ is defined to be the set of points $z \in \mathbb{P}^1(\mathbb{C})$ s.t. the family $\{f^{(n)}\}_{n\in\mathbb{Z}_+}$ is Montel-normal at z. And the **Julia set** $\mathrm{Jul}(f)$ is defined to be $\mathrm{Jul}(f) = \mathbb{P}^1(\mathbb{C}) \setminus \mathrm{Fat}(f)$. Each component of $\mathrm{Fat}(f)$ is called a **Fatou component** of f. By(11.19.2.3) and(11.19.3.6), $\mathrm{Jul}(f) \neq \varnothing$. ⌟

Prop. (11.19.3.2). For $f \in \mathrm{Rat}$ and $k \in \mathbb{Z}_+$, $\mathrm{Jul}(f) = \mathrm{Jul}(f^{(k)})$, by(11.5.1.10). ⌟

Thm. (11.19.3.3) [Complete Invariance of Julia Sets]. For any $f \in \mathrm{Rat}$, $\mathrm{Jul}(f)$ and $\mathrm{Fat}(f)$ are both completely invariance under f, i.e. $f(\mathrm{Jul}(f)) = f^{-1}(\mathrm{Jul}(f)) = \mathrm{Jul}(f)$, and $f(\mathrm{Fat}(f)) = f^{-1}(\mathrm{Fat}(f)) = \mathrm{Fat}(f)$. ⌟

Proof: If $\{f^{(n)}\}$ is Montel-normal at $f(x)$, then it is Montel-normal at x because f is continuous. Conversely, if $\{f^{(n)}\}$ is Montel-normal at x, suppose f is Montel-normal on a nbhd U of $x \in X$, and let V be a nbhd of x s.t. $x \in V \subset \overline{V} \subset U$. Then because f is open, we can show that $\{f^{(n)}\}$ is Montel-normal on $f(V)$. □

Prop. (11.19.3.4). For $f \in \mathrm{Rat}$, $\mathrm{Jul}(f)$ is either $\mathbb{P}^1(\mathbb{C})$ or has no interior. ⌟

Proof: Suppose U is open and $U \subset \mathrm{Jul}(f)$, then $\{f^{(n)}\}$ is not Montel-normal on U. Then by(11.5.1.9), $\cup_{n\in\mathbb{N}} f^{(n)}(U) \subset \mathbb{P}^1(\mathbb{C})$ omits at most 2 points. As $\mathrm{Jul}(f)$ is f-invariant and closed, this implies $\mathrm{Jul}(f) = \mathbb{P}^1(\mathbb{C})$. □

Prop. (11.19.3.5) [Julia Sets and Periodic Points]. For $f \in \mathrm{Rat}$, $\mathrm{Jul}(f)$ contains all repelling periodic points and unstable neutral periodic points(not corresponding to Siegel disks); and $\mathrm{Fat}(f)$ contains all attracting periodic points and all stable neutral periodic points(corresponding to Siegel disks). ⌟

Proof: This follows from(11.19.1.9) and the definition of stable points(11.19.1.3). □

Prop. (11.19.3.6). For $f \in \mathrm{Rat}$, if x is an attracting point for f, then $BA(x) \subset \mathrm{Fat}(f)$. And if x is a repelling periodic point, then $x \in \mathrm{Jul}(f)$. ⌟

Proof: If x is attracting, then $\{f^{(n)}\}$ is eventually uniformly bounded on each compact subset of $BA(x)$, thus Montel-normal. If x is repelling, then $|f'(z)| > 1$, so $|(f^{(n)})'(z)|$ tends to infinity as $n \to \infty$. Then it is clear that $\{f^{(n)}\}$ is not Montel-normal at x. □

Prop. (11.19.3.7) [Exceptional Sets]. For $f \in \mathrm{Rat}$ and $z \in \mathrm{Jul}(f)$, the **exceptional set** E_z of f at z is defined to be

$$E_z = \cup_{z\in U}\mathbb{P}^1(\mathbb{C}) \setminus \Big(\cup_{n\in\mathbb{Z}_+} f^{(n)}(U)\Big).$$

Then $\#E_z \leq 2$, and it is in fact independent of $z \in \mathrm{Jul}(f)$.

- If $\#E = 1$, then it can be conjugated to ∞, and then f is a polynomial.
- If $\#E = 2$, then it can be conjugated to $\{0, \infty\}$, and then $f(z) = Cz^d, d \in \mathbb{Z} \setminus \{0, \pm 1\}$.

In particular, $E \subset \mathrm{Fat}(f)$. ⌟

Proof: $\#E_z \leq 2$ by(11.5.1.9). By definition, $f^{-1}(E_z) \subset E_z$, so if $\#E_z = 2$ for some z, it can be conjugated to the form as above, and then it can be verified that $E_z = \{0, \infty\}$ for any $z \in \mathrm{Jul}(f)$. If $\#E_z = 1$ for some z, then it can be conjugated to the form as above, and $\#E_z \geq 1$ for any $z \in \mathrm{Jul}(f)$. But we also know from the above argument that $\#E_{z'} = 2$ cannot happen for any $z' \in \mathrm{Jul}(f)$, so $E_z = \{\infty\}$ for any $z \in \mathrm{Jul}(f)$. □

Cor. (11.19.3.8). Suppose $f \in \mathrm{Rat}$, and $z \in \mathrm{Jul}(f)$, then $\cup_{n\in\mathbb{Z}_+} f^{(-n)}(z)$ is dense in $\mathrm{Jul}(f)$. In particular, any completely invariant subset of $\mathrm{Jul}(f)$ is dense in $\mathrm{Jul}(f)$. ⌟

Proof: By the definition of E, if $z \notin E$, then for any open subset $U \subset \mathbb{P}^1(\mathbb{C})$ s.t. $U \cap \mathrm{Jul}(f) \neq \varnothing$, there exists $n \in \mathbb{Z}_+$ s.t. $z \in f^{(n)}(U)$. In particular, $U \cap \Big(\cup_{n\in\mathbb{Z}_+} f^{(-n)}(z)\Big) \neq \varnothing$. As $E \subset \mathrm{Fat}(f)$, any $z \in \mathrm{Jul}(f)$ suffices. □

Thm. (11.19.3.9) [Mañé-Rocha]. For $f \in \mathrm{Rat}$, $\mathrm{Jul}(f)$ is perfect and uniformly perfect(11.5.5.2) subset. ⌟

Proof: Cf.[C-G93]P57, 64. □

Prop. (11.19.3.10) [Repelling Periodic Points are Dense]. For $f \in \mathrm{Rat}$, $\mathrm{Jul}(f)$ is the closure of repelling periodic points of f. ⌟

Proof: As f has only f.m. attracting or neutral periodic points(11.19.2.2), and $\mathrm{Jul}(f)$ is perfect(11.19.3.9), so if the assertion is wrong, we will get a non-empty open subset $U \subset \mathbb{C}$ that intersect $\mathrm{Jul}(f)$, and contains no periodic points, poles and critical points of f. Since $\deg(f) > 1$, there are two different branches h_1, h_2 of $f^{(-1)}$ on U, and $h_1(z) \neq f^{(n)}(z), h_2(z) \neq f^{(n)}(z)$ for any $z \in \mathbb{U}$ and $n \in \mathbb{N}$. But then the family of functions

$$h_n(z) = \frac{f^{(n)}(z) - h_1(z)}{f^{(n)}(z) - h_2(z)} \cdot \frac{z - h_2(z)}{z - h_1(z)}$$

doesn't take values $0, 1, \infty$, thus is a Montel-normal family(11.5.1.9). And then also $\{f^{(n)}\}$ is a Montel-normal family on U, contradicting the definition of $\mathrm{Jul}(f)$. □

Prop. (11.19.3.11) [Self-Similarity of Julia Sets]. For $f \in \mathrm{Rat}$, if U is an open subset of $\mathbb{P}^1(\mathbb{C})$ s.t. $U \cap \mathrm{Jul}(f) \neq \varnothing <$ then there exists some $N \in \mathbb{Z}_+$ s.t. $f^N(U \cap \mathrm{Jul}(f)) = \mathrm{Jul}(f)$. ⌟

Proof: By(11.19.3.10), choose $z \in U \cap \mathrm{Jul}(f)$ a repelling periodic point with period n. Then choose a nbhd V of $z \in \mathbb{P}^1(\mathbb{C})$ s.t. $V \subset f^{(n)}(V)$, so $f^{(n(j-1))}(V) \subset f^{(nj)}(V)$ for any $j \in \mathbb{Z}_+$. By(11.19.3.7),

$$\mathrm{Jul}(f) \subset \mathbb{P}^1(\mathbb{C}) \setminus E \subset \bigcup_{j \in \mathbb{Z}_+} f^{(nj)}(V),$$

so by compactness of $\mathrm{Jul}(f)$, $\mathrm{Jul}(f) \subset f^{(nj)}(V)$ for some j. □

4 Fatou Components

Prop. (11.19.4.1). For $f \in \mathrm{Rat}$ and a Fatou component U of f, $f(U)$ is also a Fatou component of f, and the map $f : U \to f(U)$ is proper of degree$\leq \deg(f)$. And $f^{-1}(U)$ is a disjoint union of at most d Fatou components. ⌟

Proof: By(11.19.3.3), this is true for any analytic covering map. □

Prop. (11.19.4.2). For $f \in \mathrm{Rat}$, if U is a completely invariant Fatou component for f, then $\partial U = \mathrm{Jul}(f)$, and every other Fatou components is simply-connected. There are at most two completely invariant Fatou components for f. ⌟

Proof: Cf.[C-G93]P70.?
$\partial U = \mathrm{Jul}(f)$ by(11.19.3.8). □

Prop. (11.19.4.3). For $f \in \mathrm{Rat}$, there can only be $0, 1, 2$ or infinitely many Fatou components. ⌟

Proof: Suppose there are only f.m. Fatou components of f. Let U be a Fatou component, and suppose $U_0 = U$, and $f(U_{k+1}) = U_k$ for $k \in \mathbb{N}$. then there are some $U_m = U_n$ for $n \neq m$. In this case, we see that U is periodic. And then there exists $N \in \mathbb{Z}_+$ s.t. $f^{(N)}(U) = U$ for any Fatou component U of f. Then each component U is totally invariant under $f^{(N)}$, which implies that there are at most 2 Fatou components by(11.19.4.2). □

Thm. (11.19.4.4) [No-Wandering-Domain Theorem, Sullivan1985]. For $f \in \mathrm{Rat}$, every Fatou component U of f is eventually periodic under permutation by f, i.e. there exists $0 < n < m \in \mathbb{Z}_+$ s.t. $f^{(n)}(U) = f^{(m)}(U)$. ⌟

Proof: If there is a contradictory Fatou component U, call it a wandering domain. Then we have:

Lemma (11.19.4.5) [Baker]. If U is a wandering domain, then $f^{(n)}(U)$ is simply-connected for n sufficiently large. ⌟

Proof: □

Lemma (11.19.4.6). $B(U)$ contains a infinitely-dimensional subspace $N(U)$ of compactly-supported Beltrami differentials with the following property: If $\mu \in N(U)$ satisfies $\mu = \overline{\partial} v$ for some quasi-conformal vector field v and $v|_{\partial U} = 0$, then $\mu = 0$. ⌟

Proof:

□

? □

Thm. (11.19.4.7). If $f \in \mathrm{Rat}$, and $A \subset \mathrm{Jul}(f)$ is a stable point that intersect any equivalent class of f(where $x \sim y \iff f^{(n)}(x) = f^{(n)}(y)$ for some $n \in \mathbb{N}$) in at most one point, then $\mu(A) = 0$. ⌟

Proof: □

Def. (11.19.4.8) [Parabolic Components]. For $f \in \mathrm{Rat}$, a **parabolic component** for f is a Fatou component U of f of period n with a neutral fixed point ζ for $f^{(n)}$ on its boundary with multiplier 1, and that all points of U converges to ζ under iterations by $f^{(n)}$. ⌟

Def. (11.19.4.9) [Herman Rings]. For $f \in \mathrm{Rat}$, a **Herman ring** for f is a doubly-connected Fatou component of f of period n s.t. the action of $f^{(n)}$ is conjugate to either a isometry of an annulus. ⌟

Thm. (11.19.4.10)[Classifying Periodic Fatou Components]. For $f \in \mathrm{Rat}$, each Fatou component U for f is exactly one of the following:

- U contains an attracting periodic point
- U is parabolic(11.19.4.8).
- U is a Sigel disk(11.19.1.9).
- U is a Herman ring(11.19.4.9).

⌟

Proof: Cf.[C-G93]P74. □

Thm. (11.19.4.11) [Sullivan]. For $f \in \mathrm{Rat}$, if $\mathrm{Fat}(f)$ has two components and f is hyperbolic on $\mathrm{Jul}(f)$, then $\mathrm{Jul}(f)$ is a quasi-circle(11.5.5.7). ⌟

Proof: Cf.[C-G93]P102. □

Prop. (11.19.4.12) [Woff-Denjoy]. ⌟

5 Conjectures

Conj. (11.19.5.1) [Density of Hyperbolicy]. The set of hyperbolic rational maps is dense and open in the set Rat_d of rational maps on $\mathbb{P}^1(\mathbb{C})$ of dimension d. ⌟

Proof: □

Conj. (11.19.5.2) [No Invariant Line Fields]. For $f \in C(z)$, there are no invariant fields on $\mathrm{Jul}(f)$, unless f is double covered by an integral torus endomorphism. ⌟

6 Polynomial Iterates

Prop. (11.19.6.1) [Julia Sets and Critical Points]. For $P \in \mathcal{P}\mathrm{oly}(z)$,

- $\mathrm{Jul}(P)$ is connected iff there are no finite critical points in $AB(\infty)$, i.e. the forward orbits of any finite critical point of f is bounded.
- $\mathrm{Jul}(P)$ is totally disconnected if for any finite critical point q, $P^{(n)}(q) \to \infty$ as $n \to \infty$.

⌟

Proof: Cf.[C-G93]P66, 67. □

7 Quadratic Maps

Prop. (11.19.7.1). Since any polynomial $f \in \mathcal{P}\mathrm{oly}(z)$ of degree 2 can be conjugated via maps $z \mapsto z+A$ to a map of the form $z \mapsto z^2 + c$, to study quadratic polynomial maps, it suffices to study maps of the form $f(z) = z^2 + c$.

By(11.19.6.1), $\mathrm{Jul}(f)$ is either connected or totally disconnected(Notice if $\{f^{(n)}(0)\}$ is unbounded, then it tends to ∞. ⌟

Def. (11.19.7.2) [Mandelbrot Set]. The **Mandelbrot set Man** is define to be the set of $c \in \mathbb{C}$ s.t. $\{f_c^{(n)}(0)\}$ is bounded, where $f_c(z) = z^2 + c$. ⌟

Prop. (11.19.7.3). $\mathbf{Man} \subset \overline{\mathbb{D}(0,2)}$. ⌟

Proof: This is because we can show by induction that $|f^{(n)}(0)| \geq |a|(|a|-1)^{n-1}$ for $n \in \mathbb{Z}$. □

Prop. (11.19.7.4) [Douady–Hubbard1982]. The Mandelbrot set $\mathbf{Man} = \{a \in \mathbb{C} | (z^2+a)^{(n)}(0) \leq 2, \forall n \in \mathbb{N}\}$, and it is compact, connected and $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{Man}$ is connected. ⌟

Proof: Let $f_a(z) = z^2 + a$. If $|a| > 2$, then $a \notin \mathbf{Man}$. If $|a| \leq 2$, $f_a^{(n)}(0) = 2 + \alpha$ for some $\alpha \in \mathbb{R}_+$, then it can be shown by induction that $f_a^{(n+k)}(0) \geq 2 + 4^k \alpha$ for any $k \in \mathbb{N}$, so $a \notin M$. This implies $\mathbf{Man} = \{a \in \mathbb{C} | (z^2+a)^{(n)}(0) \leq 2, \forall n \in \mathbb{N}\}$. In particular, it is closed.

For the last assertion, suppose Ω is a connected component of $\mathbb{C} \setminus M$. Then $\max_{a \in \overline{\Omega}} |f_a^{(n)}(0)| > 2$. If Ω is bounded, then by maximum principle, $f_a^{(n)}(0)| \geq 2$ for some $a \in \partial\Omega \subset \mathbf{Man}$, which contradict the first assertion. So any connected component of $\mathbb{C} \setminus \mathbf{Man}$ is unbounded, thus $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{Man}$ is connected.

To show that **Man** is connected, denote $P_n(c) = f_c^n(0)$, let $R \in (2, \infty)$, then

$$\mathbf{Man} = \bigcap_{n \in \mathbb{Z}_+} P_n^{-1}(\overline{D(0,R)})$$

is a nested intersection of compact sets. We may choose R s.t. $\partial\mathbb{D}(0,R)$ contains no critical points of any P_n. Thus by(4.4.6.2), it suffices to show that each $P_n^{-1}(\overline{D(0,R)})$ is connected. Suppose U is a connected component of $P_n^{-1}(D(0,R))$ s.t. $0 \notin \overline{U}$, and this n is minimum. Then we show that $0 \notin P_k(\overline{U})$ for all $1 \leq k \leq n$. To show this, use induction on k: $k = 1$ case follows from the hypothesis, suppose that this is true for $k \leq k_0 < n$, then for $k = k_0$,

$$f_c^{k+1}(0) \neq c, \quad c \in \overline{U}.$$

Notice for $c \in \partial U$,

- $f_c^{k+1-n}(\partial D(0,R))$ is a Jordan curve, which varies smoothly in c: By the minimality of n, $P_{n-k-1}^{-1}(\mathbb{D}(0,R))$ is connected, so for any $c \in \overline{U}$, $f_c^{k+1-n}(\partial\mathbb{D}(0,R))$ is a smooth Jordan curve(because f_c^{k+1-n} has a critical point if $|f_c^m(0)| = R$ for some $m < n$, which contradicts the fact $|f_c^n(0)| \leq R$), and

$$F : \{(c,z) : c \in \overline{U}, f_c^m(z) \in \partial\mathbb{D}(0,R)\} \to U \times \partial\mathbb{D}(0,R)$$

is a smooth covering map. Notice U is simply-connected so there is a map $\partial U \times I \to \overline{U}$. Thus the pullback of F just induces a smooth isomorphism of this family of Jordan curves with the trivial family, so it depends smoothly on c.
- $f_c^{k+1}(0) \in f_c^{k+1-n}(C_R)$, .because $|f_c^{n-1}(c)| = R$
- $0, c \in f_c^{k+1-n}(\mathbb{D}(0,R))$, because $|f_c^{n-1}(c)| = R$.

So $n(\partial U, c \mapsto f_c^{(k+1)}(0) - c) = n(\partial U, c \mapsto f_c^{(k+1)}(0) - 0)$ by**??**. Thus

$$f_c^{k+1}(0) \neq 0, \quad c \in \overline{U},$$

by argument principle. Then the induction process is finished.

Finally, notice $P_n : U \to D(0,R)$ is a branched covering, so $0 \in D(0,R) = P_n(U)$, contradiction.

For another proof, Cf.[Mandelbrot set is connected].**?** □

Conj. (11.19.7.5) [Locally-Connectedness]. The Mandelbrot set **Man** is locally connected. ⌟

Proof: □

Prop. (11.19.7.6) [Main Cardioid]. Man contains the **main cardioid** which is given by

$$\{a \in \mathbb{C} : |1 + \sqrt{1-4a}| < 1\} \cup \{a \in \mathbb{C} : |1 - \sqrt{1-4a}| < 1\} = \{\frac{\mu(2-\mu)}{4} | \mu \in \mathbb{D}\}.$$

⌟

Proof: The main cardioid is just the set $a \in \mathbb{C}$ s.t. $f_a(z) = z^2 + a$ has a attracting fixed point. And in this case, it can be shown that $\mathbb{D}(0, \frac{1}{2}) \subset BA(\frac{1+\sqrt{1-4a}}{2})$. Thus $a \in$ **Man**. □

Prop. (11.19.7.7). Man $\cap \mathbb{R} = [-2, \frac{1}{4}]$. ⌟

Proof: For $a \in \mathbb{R}$, if $a > 1/4$, then $z^2 + a > z + (a - \frac{1}{4})$, so $a \notin$ **Man**. If $a < -2$, then $a \notin$ **Man** by(11.19.7.3).

And for $a \in [0, 1/4], f^{(n)}(0) \in [0, 1/2]$, so $a \in$ **Man**. Finally, for $a \in [-2, 0]$, $|f^{(n)}(0)| \leq a$, so $a \in$ **Man**. □

Prop. (11.19.7.8). Any point in ∂**Man** is an accumulation point of the set of values $a \in \mathbb{C}$ s.t. $f_a(z) = z^2 + a$ has a supper-attracting point other than ∞(i.e. 0 is periodic for f_a). ⌟

Proof: Let U be an small open set of $\mathbb{C}$ intersecting ∂**Man** and $0 \notin U$. Suppose $f_a(z)$ doesn't has a supper-attracting point other than ∞, then $f_a^{(n)}(0) \neq 0$ for any $n \in \mathbb{Z}_+$. In particular, $f_a^{(n)}(0) \neq \sqrt{a}$, where $\sqrt{a}$ is a branch of square root. Consider the family of functions $\{g_n(a) = f_a^{(n)}(z)/\sqrt{a}\}$ on a, then $g_n(a) \neq \{0, 1, \infty\}$ for any $a \in D$. So by(11.5.1.9), $\{g_n\}$ is normal on D. As $D \cap$ **Man** $\neq \varnothing$, there exists $a \in D$ s.t. $\{g_n(a)\}$ is bounded. But $D \setminus$ **Man** $\neq \varnothing$, so there exists $\xi \in D$ and a sequence $(g_n^{(n_i)}(\xi))$ that tends to infinity. So $\{g_n\}$ is normal on D cannot be normal on D, contradiction. □

Conj. (11.19.7.9) [Hyperbolicity]. Every component of the interior of the Mandelbrot set is hyperbolic. Equivalently, the set of $c \in \mathbb{C}$ s.t. $f_c(z) = z^2 + c$ is hyperbolic is an open dense subset of $\mathbb{C}$. ⌟

Proof: □

Thm. (11.19.7.10) [Yoccoz]. If $f \in \mathbb{C}[z]$ is a quadratic polynomial, and there is an invariant line field on $\mathrm{Jul}(f)$, then f is infinitely renormalizable. ⌟

Proof:

□

Thm. (11.19.7.11) [Robust Rigidity]. If $f \in \mathbb{C}[z]$ is a robust infinitely renormalizable quadratic polynomial, then there are no invariant line fields on $\mathrm{Jul}(f)$. ⌟

Proof: Cf.[McMullen] □

Cor. (11.19.7.12). If $f \in \mathbb{C}[z]$ is a real quadratic polynomial, then then there are no invariant line fields on $\mathrm{Jul}(f)$. ⌟

Proof: □

12 Differential Geometry

12.1 Smooth Manifolds

References are [Lee13], [G-P74](Good) and [Geometric Analysis Jost].

Notation (12.1.0.1).
- All manifolds in this section is assumed to be smooth over $\mathbb{R}$(12.1.1.1) or analytic over $\mathbb{C}$.

⌟

1 Local Properties

Def. (12.1.1.1) [Smooth manifolds]. ?. The category of smooth manifolds is denoted by $\mathcal{D}\mathrm{iff}$. ⌟

Prop. (12.1.1.2) [Collar Neighborhood Theorem]. If X is a smooth paracompact manifold with boundary, then there is a nbhd of ∂X in X which is diffeomorphic to the product $\partial X \times [0,1]$. ⌟

Proof: □

Prop. (12.1.1.3) [Rank Theorem]. Let $M \in \mathcal{D}\mathrm{iff}^m, N \in \mathcal{D}\mathrm{iff}^n$ and $F : M \to N$ be a smooth map with constant rank r. Then for any $p \in M$, there exists smooth charts centered at $p, F(p)$ that the coordinate representation of F is

$$F(x_1, \ldots, x_r, x_{r+1}, \ldots, x_m) \mapsto (x_1, \ldots, x_r, 0, \ldots, 0).$$

⌟

Proof: Cf.[Lee13]P81. □

Def. (12.1.1.4) [Immersion]. A **smooth immersion** of manifolds $f : M \to N$ is a smooth map that $\mathrm{d}f(x) : T_x(M) \to T_{f(x)}(N)$ is injective for any $x \in M$.

A **smooth submersion** of manifolds $f : M \to N$ is a smooth map that $\mathrm{d}f(x) : T_x(M) \to T_{f(x)}(N)$ is surjective for any $x \in M$. ⌟

Def. (12.1.1.5) [Local Diffeomorphism]. A **local diffeomorphism** $f : M \to N$ is a smooth map that for any $p \in M$, there exists an open subset U that $U \to f(U)$ is a diffeomorphism. ⌟

Prop. (12.1.1.6) [Local Section Theorem]. Let $F : M \to N$ be a smooth map between smooth manifolds, then π is a smooth submersion iff each point of M is in the image of a local section of F. ⌟

Proof: If each point of M is in the image of a local section of F, the differential is surjective at every point. Conversely, use the rank theorem(12.1.1.3). □

Prop. (12.1.1.7). A smooth submersion $F : M \to N$ is an open map, and a surjective smooth submersion is a quotient map. ⌟

Proof: Let $W \subset M$, and $q = \pi(p)$ where $p \in W$, then there is a local section $\sigma : U \to M$ that $\sigma(q) = p$(12.1.1.6), thus $\sigma^{-1}(W)$ is open in N. But for any $y \in \sigma^{-1}(W)$, $y = \pi(\sigma(y)) \subset \pi(W)$. So $p \in \sigma^{-1}(W) \subset \pi(U)$, which means $\pi(W)$ is open, and π is an open map. t The last assertion follows as any open surjective map is a quotient map(4.4.1.10). □

Prop. (12.1.1.8)[Characteristic Property of Surjective Smooth Submersions]. Let $\pi : M \to N$ be a smooth submersion of manifolds, P another smooth manifold, then

- Any map $F : N \to P$ is smooth iff $F \circ \pi$ is smooth.
- Any smooth map $\widetilde{F} : M \to P$ that is constant on the fibers of π induces a smooth map $F : N \to P$ that $\widetilde{F} = F \circ \pi$.

⌟

Proof: 1: Use local section theorem(12.1.1.6).

2: There is a constant map $F : N \to P$ that $\widetilde{F} = F \circ \pi$ by(12.1.1.7) and universal property of quotient maps, and it is smooth by item1. □

Def. (12.1.1.9) [Smooth Covering Space]. A **smooth covering space** of a smooth manifold X is a space $\widetilde{X}$ together with a smooth map $\pi : \widetilde{X} \to X$ that there is a covering U_α of X that for each α, $\pi^{-1}(U_\alpha)$ is a disjoint union of open subsets of $\widetilde{X}$, each of which is mapped diffeomorphically onto U_α. ⌟

Prop. (12.1.1.10) [Proper Free Action]. Let $\pi : E \to M$ be a smooth covering map, then with the discrete topology, $\mathrm{Aut}_\pi(E)$ is a discrete Lie group acting smoothly, freely and properly on E.

Conversely, suppose M is a smooth manifold and Γ is discrete group acting smoothly, freely and properly on a manifold, then the quotient space M/Γ is a topological manifold, and it has a unique smooth structure that the quotient map $\pi : M \to M/G$ is a smooth normal covering map. ⌟

Proof: If $\pi : E \to M$ is a smooth covering map, then the action is continuously, freely and properly by(4.15.1.28). Smoothness can be seen by applying(12.1.1.8). $\mathrm{Aut}_\pi(E)$ is a Lie group because it is countable: Let $q \in M$, and U an evenly covered nbhd of q, then $\pi^{-1}(U)$ is a union of open subsets each containing one element of $\pi^{-1}(q)$. so $|\pi^{-1}(q)|$ is countable, and because $\mathrm{Aut}_\pi(E)$ acts freely, it is also countable.

Because this action is a covering map action by(4.12.1.19), (4.15.1.31) shows this is a normal covering map. The quotient space is locally Euclidean, and also Hausdorff by(4.12.1.12)(4.12.1.10), so it is a topological manifold. The smooth structure is clear. □

Def. (12.1.1.11)[Smooth Embedding]. A **smooth embedding** of manifolds $f : M \to N$ is a smooth immersion that is also a homeomorphism onto its image. ⌟

Prop. (12.1.1.12) [Global Rank Theorem]. Let $F : M \to N$ be a smooth map of manifolds of constant tank, then:

- if it is an injection, then it is a submersion.
- if it is an surjection, then it is a submersion.

- if it is a bijection, then it is an diffeomorphism.

⌟

Proof: Cf.[Lee Smooth Manifold P83]. □

Prop. (12.1.1.13)[Local Embedding Theorem]. If $F : M \to N$ is a smooth morphism of manifolds, then it is a smooth immersion if it is locally a smooth embedding on the source. ⌟

Proof: Let $p \in M$, then there exists a nbhd U_1 of $p \in M$ that F is injective. Now choose another precompact nbhd U of p that $\overline{U} \subset V$, then $F|_{\overline{U}}$ is an injective map with compact domain, so it is a topological embedding by(4.4.2.11). Thus $F|_U$ is a smooth embedding. □

Submanifolds

Def. (12.1.1.14) [Submanifolds]. For a smooth manifold M, an **embedded submanifold** $S \subset M$ is a subset S that is a manifold in the induced topology together with a smooth structure that the inclusion is a smooth embedding of manifolds(12.1.1.11).

An **immersed submanifold** $S \subset M$ is a subset endowed with a topology and a smooth manifold structure that the inclusion is a smooth immersion(12.1.1.4).

An **weakly embedded submanifold** $S \subset M$ is an immersed submanifold that any smooth map $F : N \to M$ from some space N that has image in S is smooth as a map from N to S. ⌟

Remark (12.1.1.15). Examples of immersed submanifolds that is not an embedded submanifolds are the 8-figure and the dense curve in a torus. However, an immerse submanifold is locally embedded on the source, by(12.1.1.13). ⌟

Def. (12.1.1.16) [Slice Charts]. Let $U \subset \mathbb{R}^n$, then a k-slice of U is the set $S = \{(x^1, \ldots, x^n) \in U | x^{k+1} = \ldots = x^n = 0\}$.

Let M be a manifold, a **slice chart** of a subset $S \subset M$ is a smooth char (U, φ) that $\varphi(U \cap S)$ is a k-slice of $\varphi(U)$ for some k. ⌟

Prop. (12.1.1.17) [Local Slice Criterion for Embedded Submanifolds]. Let M be a smooth n-manifold and S an embedded k-submanifold, then each point of S is contained in the domain of a slice chart. Conversely, if $S \subset M$ is a subset that each point of S is contained in the domain of a slice chart, then the induced topology makes S a topological manifold, and there is a smooth structure on S that makes it an embedded submanifold of M. ⌟

Proof: Suppose S is an embedded submanifold, then the rank theorem(12.1.1.3) shows there exists coordinates that the image of $i(S)$ is contained in a k-slice of M. Shrinking the open subset a little bit, we get a slice chart of S.

Conversely, if each point of S is contained in the domain of a slice chart, then we can use these smooth charts to get an atlas for S, which makes S an embedded topological submanifold of M. The transition maps are also smooth because they are restrictions of the corresponding transition map of M, so S is an embedded submanifold of M. □

Prop. (12.1.1.18). If M is a compact manifold, then any injective immersion $f : M \hookrightarrow M$ is an embedding of submanifolds. ⌟

Proof: The topology of M is equivalent to the induced topology by(4.4.2.10). □

Prop. (12.1.1.19) [Immersed Submanifolds are Locally Embedded]. If $S \subset M$ is an immersed submanifold, then for any $p \in S$, there is a nbhd U of $p \in S$ that $U \subset M$ is an embedded submanifold. ⌟

Proof: This follows immediately from(12.1.1.13). Notice that the topology on U must be the induced topology, because it is a smooth embedding thus a homeomorphism onto its image(12.1.1.11). □

Lemma (12.1.1.20). If $i : S \hookrightarrow M$ is an immersed submanifold, if $F : N \to M$ is a smooth morphism of manifolds that has image in S, if $F : N \to S$ is continuous, then $N \to S$ is smooth. ⌟

Proof: Let $p \in N$ mapping to $q = F(p)$. By(12.1.1.19), there is a nbhd V of $q \in S$ that $i|_V$ is an smooth embedding. Thus there is a slice chart(12.1.1.17) (W, ψ) of M that $(V_0, \widetilde{\psi})$ is a smooth chart for V, where $V_0 = W \cap V$ and $\widetilde{\psi} = \pi \circ \psi$, where π is the projection $\mathbb{R}^n \to \mathbb{R}^k$ onto the first k coordinates, and also a smooth chart for S.

Let $U = F^{-1}(V_0)$ be open in F, then there is a smooth chart of N contained in U. Now the coordinate representation of F in the slice chart of S is just the representation of $F : N \to M$ composed with the projection π, so it is smooth. □

Remark (12.1.1.21). $N \to S$ being continuous is a necessary condition, otherwise consider the figure 8. ⌟

Prop. (12.1.1.22) [Restricting Codomain of Smooth Morphism]. If S is an embedded submanifold in M, if if $N \to M$ is a smooth that has image in S, then $N \to S$ is smooth. ⌟

Proof: Because in this case, S has the induced topology, so it is easily seen that $N \to S$ is continuous. □

<u>**Sard's Theorem**</u>

Lemma (12.1.1.23) [Invariance of Measure Zero Sets]. If $S \in \mathbb{R}^n$ has measure zero, then for any smooth map $g : \mathbb{R}^n \to \mathbb{R}^m$, $g(S)$ has measure zero.

Thus the notion of measure zero is definable for arbitrary smooth manifolds. ⌟

Lemma (12.1.1.24). Cf.[Pollack Appendix A]. ⌟

Def. (12.1.1.25). For a map of schemes $f : X \to Y$, a point $y \in Y$ is called **critical** iff df_x is not surjective, for some $x \in f^{-1}(y)$, otherwise it is called a **regular value**. ⌟

Prop. (12.1.1.26) [Regular Value Theorem]. If y is a regular value for a map $f : X \to Y$, then $f^{-1}(Y)$ has a natural submanifold structure. ⌟

Proof: □

Prop. (12.1.1.27) [Stack of Records Theorem]. If y is regular value of a map $f : X \to Y$, where X is compact and $\dim X = \dim Y$, then f is a covering map locally on $f^{-1}(U)$ for some nbhd U of y. ⌟

Proof:

□

Thm. (12.1.1.28) [Sard]. For a map $X \to Y$ of smooth manifolds, the set of critical values is of measure zero Y. ⌟

Proof: Cf.[Pollack Appendix A]. □

Prop. (12.1.1.29) [Whitney Embedding Theorem]. For any $k \in \mathbb{Z}_+$ and $M \in \mathcal{D}\mathrm{iff}^3$, M can be embedded into $\mathbb{R}^{2k}$. ⌟

Proof: Cf.[Pollack P51]. □

Cor. (12.1.1.30) [Whitney Immersion Theorem]. Any smooth manifold M of dimension k can be immersed into $\mathbb{R}^{2k}$. ⌟

Proof: □

1-dimensional Smooth Manifold with Boundaries

Prop. (12.1.1.31). Any smooth manifold of dimension 1 with boundary is isomorphic to $[0,1]$ or S^1. ⌟

Proof: Cf.[Pollack Appendix]. □

Cor. (12.1.1.32). The boundary of any smooth manifold of dimension 1 consists of points of even number. ⌟

Simplifications

Prop. (12.1.1.33). For every vector field X and every point $X(p) \neq 0$, there exists a coordinate nbhd $(x_1, \ldots, x_{n-1}, t)$ such that $X = \frac{\partial}{\partial t}$. ⌟

2 Smooth Vector Bundles

Def. (12.1.2.1) [Smooth Vector Bundle]. A **smooth vector bundle** over a smooth manifold is a vector bundle over X that the trivialization maps are all smooth. ⌟

Def. (12.1.2.2) [Smooth Fiber Bundle]. ⌟

Tangent and Cotangent Bundles

Lemma (12.1.2.3) [Differential in Coordinates]. Let $F : U \to V$ be a smooth map where $U \subset \mathbb{R}^n$ and $V \subset R^n$, with corresponding coordinates (x^i) and (y^i), then

$$dF_p(\frac{\partial}{\partial x^i}|_p) = \sum_j \frac{\partial F^j}{\partial x^i}(p)\frac{\partial}{\partial y^j}|_{F(p)}.$$

⌟

Proof: for any smooth function f,

$$dF_p(\frac{\partial}{\partial x^i}|_p)(f) = \frac{\partial}{\partial x^i}|_p(f \circ F) = \sum \frac{\partial f}{\partial y^j}(F(p))\frac{\partial F^j}{\partial x^i}(p) = (\sum_j \frac{\partial F^j}{\partial x^i}(p)\frac{\partial}{\partial y^j}|_{F(p)})(f).$$

□

Lemma (12.1.2.4) [Change of Coordinates]. Suppose $(U,\varphi),(V,\psi)$ be two smooth charts of a smooth manifold, and the transition function on $U\cap V$ is denoted by

$$\psi\circ\varphi^{-1}(x)=(\widetilde{x}^1(x),\ldots,\widetilde{x}^n(x)),$$

then(12.1.2.3) shows

$$\begin{aligned}\frac{\partial}{\partial x^i}|_p&=d(\varphi^{-1})_{\varphi(p)}(\frac{\partial}{\partial x^i}|_{\varphi(p)})=d(\psi^{-1})_{\psi(p)}\cdot d(\psi\cdot\varphi^{-1})|_{\varphi(p)}(\frac{\partial}{\partial x^i}|_{\varphi(p)})\\&=d(\psi^{-1})_{\psi(p)}(\sum_j\frac{\partial\widetilde{x}^j}{\partial x^i}(\varphi(p))\frac{\partial}{\partial\widetilde{x}^j}|_{\psi(p)})=\sum_j\frac{\partial\widetilde{x}^j}{\partial x^i}(\varphi(p))\frac{\partial}{\partial\widetilde{x}^j}|_p\end{aligned}$$

⌟

Def. (12.1.2.5) [Tangent Vectors]. Let M be a smooth manifolds, then a **tangent vector** at a point p is a linear maps $v:C^\infty(M)\to\mathbb{R}$ satisfying:

$$v(fg)=f(p)v(g)+g(p)v(f).$$

The set of tangent vectors at p is a vector space, denoted by T_pM. ⌟

Def. (12.1.2.6) [Tangent Bundle]. Let M be a n-dimensional smooth manifold, the tangent bundle of M is defined to be the set $TM=\coprod T_pM$. It has a smooth manifold structure that makes it into a $2n$-dimensional manifold, and the projection $\pi:TM\to M$ is smooth. And it is a n-dimensional vector bundle over M. ⌟

Proof: Let (U,φ) be a smooth chart of M, with coordinate functions $\varphi^1,\ldots,\varphi^n$, then we define a map $\widetilde{\varphi}:\pi^{-1}(U)\to\mathbb{R}^{2n}$ by

$$\widetilde{\varphi}(\sum v^i\frac{\partial}{\partial x^i}|_p)=(x^1(p),\ldots,x^n(p),v^1,\ldots,v^n).$$

Then for two different open subset U,V, the transition map is

$$\widetilde{\psi}\cdot\widetilde{\varphi}^{-1}(x^1,\ldots,x^n,v^1,\ldots,v^n)=(\widetilde{x}^1(x),\ldots,\widetilde{x}^n(x),\sum_j\frac{\partial\widetilde{x}^1}{\partial x^j}(x)v^j,\ldots,\sum_j\frac{\partial\widetilde{x}^n}{\partial x^j}(x)v^j)$$

which is clearly smooth. So this defines a smooth vector bundle over M, called the **tangent bundle** of M. □

Def. (12.1.2.7) [Cotangent Bundle]. The **cotangent bundle** T^*M of a smooth manifold M is the dual of the tangent bundle TM. ⌟

Def. (12.1.2.8) [Parallelizable manifold]. A manifold is called **parallelizable** iff the tangent bundle is trivial. ⌟

Vector Fields

Def. (12.1.2.9) [Smooth Vector Field]. A **smooth vector field** on a smooth manifold is a smooth global section of the tangent bundle $TM\to M$(12.1.2.6). ⌟

Prop. (12.1.2.10) [Check Smoothness]. Let M be a smooth manifold and X be a section of the vector bundle $TM\to M$, then X is a smooth vector field iff for any $f\in C^\infty(M)$, $Xf\in C^\infty(M)$. ⌟

Proof: If for any $f \in C^\infty(M)$, $Xf \in C^\infty(M)$, let U be a trivializing nbhd of M with coordinate functions x^i, then near any point $p \in U$, we can use bump function to extend x^i to a smooth function on M. Then $X(x^i) = X^i$ near p, thus the coordinates of X in this trivialization are all smooth, so X is smooth near p, thus smooth everywhere.

Conversely, for any $f \in C^\infty(M)$, in a trivializing nbhd U of M, $Xf(x) = (\sum X^i(x) \frac{\partial}{\partial x^i}|_x)(f) = \sum X^i(x) \frac{\partial f}{\partial x^i}(x)$ is smooth. □

Def. (12.1.2.11) [Pushforward of Vector Fields]. Let $F : M \to N$ be a diffeomorphism, then for any $X \in \mathfrak{X}(M)$, there exists a $Y \in \mathfrak{X}(N)$ that $dF_p(X_p) = Y_{F(p)}$. ⌟

Proof: We just define $Y_q = dF_{F^{-1}(q)}(X_{F^{-1}(q)})$, it suffices to show this a smooth vector field. But $Y : N \to TN$ is the composition

$$N \xrightarrow{F^{-1}} M \xrightarrow{X} TM \xrightarrow{TF} TN,$$

so it is smooth. □

Def. (12.1.2.12) [Lie Bracket of Vector Fields]. Cf.[Lee13]P185. ⌟

Prop. (12.1.2.13)[Pushforward of Lie Bracket]. Let $F : M \to N$ be a diffeomorphism and $X_1, X_2 \in \mathfrak{X}(M)$, then $F_*[X_1, X_2] = [F_*X_1, F_*X_2]$(12.1.2.11). ⌟

Proof: For any $f \in C^\infty(N)$, $F_*X_i = Y_i$, then

$$[X_1, X_2](f \circ F) = X_1X_2(f \circ F) - X_2X_1(f \circ F) = X_1((Y_2(f) \circ F) - X_2((Y_1(f) \circ F) = (Y_1Y_2(f) - Y_2Y_1(f)) \circ F,$$

which means exactly $F_*[X_1, X_2] = [Y_1, Y_2]$. □

Tensor Fields

Def. (12.1.2.14) [Lie Derivatives of Tensor Fields]. Cf.[Lee13]P321. ⌟

3 Differential Forms

Prop. (12.1.3.1)[Frobenius Theorem]. If X is an involutive distribution on a manifold M, then there is a unique maximal integration manifold passing through it. Where a distribution is involutive if it is closed under Lie bracket. ⌟

Proof: The key to the proof is to prove that involutive is equivalent to integrable, i.e. flat locally as $\{\frac{\partial}{\partial x_i}\}$ for some local coordinate. Cf.[李群讲义 项武义 P226] □

Cor. (12.1.3.2). X, Y in a Lie algebra commute iff their corresponding vector fields commute. ⌟

Interior and Exterior Derivatives

Lie Derivatives

Def. (12.1.3.3). The **Lie bracket** of two vector fields X, Y is defined to be $[X, Y](f) = (XY - YX)f$, then if $X = \sum a_i \partial/\partial x_i$, $Y = \sum b_i \partial/\partial x_i$, then $[X, Y] = \sum (X(b_i) - Y(a_i))\partial/\partial x_i$. ⌟

Lemma (12.1.3.4). $[X, Y] = \frac{\partial}{\partial t}(d(\phi_{-t})Y)|_{t=0}$. ⌟

Proof: For any function f,set $g(t,q) = \frac{f(\phi_t(q))-f(q)}{t}$,$g(0,q) = Xf(q)$. Then g is differentiable (because $g(t,q) = \int_0^1 Xf(\phi_{ts}(p))ds$, and:

$$\begin{aligned}\lim_{t\to 0} d(\phi_{-t})Yf(p) &= \lim \frac{Yf(p) - Y(f\phi_{-t})(\phi_t(p))}{t} \\ &= \lim \frac{Yf(p) - Yf(\phi_t p) - Y(tg(-t,\phi_t(p))}{t} \\ &= ((XY - YX)f)(p) \\ &= [X,Y]f(p)\end{aligned}$$

□

Prop. (12.1.3.5). $[fu,v] = f[u,v] - df(u)v$. ⌟

Proof: Direct from the definition(12.1.3.3). □

Prop. (12.1.3.6) [Derivative formula].

$$d\omega(X,Y) = X\omega(Y) - Y\omega(X) - \omega([X,Y]).$$

⌟

Proof: □

Prop. (12.1.3.7) [Cartan's magic formula].

$$L_X\omega = \iota_X(d\omega) + d(\iota_X\omega)$$

$$\iota([X,Y]) = [L_X, \iota_Y]$$

⌟

Proof: Notice that four of them are derivatives (check because $\iota_X(w\wedge v) = \iota_X w\wedge v + (-1)^{|w|} w\wedge \iota_X v$). So by induction, we only has to verify them on dimension 0 and 1. □

Prop. (12.1.3.8) [Stoke's theorem].

$$\oint_\Omega d\omega = \oint_{\partial\Omega} i^*\omega.$$

In a 3-dimensional Riemanian manifold, If we set:

$$df = \omega^1_{\mathrm{grad}f}, \quad d\omega^1_A = \omega^2_{\mathrm{curl}A}, \quad d\omega^2_A = (\nabla A)\omega^3,$$

Then:

$$f(y) - f(x) = \int_l \mathrm{grad} f\cdot dl.$$

$$\int_l A\cdot dl = \oint_S \mathrm{curl} A\cdot dn.$$

$$\oint_U \nabla\cdot F dV = \oint_{\partial U} F\cdot n dS.$$

⌟

Proof: □

Hodge Star

Def. (12.1.3.9) [Hodge Star Operator]. given a volume-form ω on a vector space, the Hodge star operator $*-$ is an operator from $\bigwedge^k V \to \bigwedge^{n-k} V$ such that:

$$\alpha \wedge (*\beta) = \langle \alpha, \beta \rangle \omega.$$

On a closed oriented Riemannian manifold, given a volume form ω, the star operator satisfies:

$$(\alpha, \beta) = \int_M \langle \alpha, \beta \rangle \omega = \int_M \alpha \wedge *\beta.$$

And $** = (-1)^{p(n-p)}$ on $\Omega^p M$. ⌟

Def. (12.1.3.10). For a operator d on $\Omega^* M$, we define the adjoint $d^* = (-1)^{n(p+1)+1} * d*$ on Ω^p, which satisfies the adjoint property by calculation:

$$(d^* \alpha, \beta) = (\alpha, d\beta).$$

The laplacian $\Delta = d^* d + dd^*$. It can be verified that Δ commutes with $*$ and d. ⌟

4 Differential Topology

References are [J. W. Milnor, Topology from the differentiable viewpoint. Based on notes by David W. Weaver University Press of Virginia, Charlottesville, Va. 1965 ix+65 pp.].

Transversality

Def. (12.1.4.1) [Transversality]. ⌟

Prop. (12.1.4.2) [Transversal Stable under Pertabations]. The property of transversal for a map $f : X \to Y$ for a compact manifold X to a fixed submanifold Z of Y is stable under smooth deformation. ⌟

Proof: We can assume the submanifold is defined by a slice, so the transversality is in fact equivalent to locally submersion in the vertical direction. Thus it is clearly stable under deformation. □

Prop. (12.1.4.3). If a smooth map $f : X \to Y$ is transversal to a submanifold $Z \subset Y$ of codimension r, then the preimage $f^{-1}(Z)$ is a submanifold of X of codimension r. ⌟

Proof: Cf.[Pollack P28]. □

Cor. (12.1.4.4). If two submanifolds are transversal at every point is again a submanifold, and the codimension is the sum of them. ⌟

Prop. (12.1.4.5) [Parametric Transversality Theorem]. Suppose N and M are smooth manifolds, $X \subset M$ is an embedded submanifold, and F_s is a smooth family of maps from N to M. If the map $F : N \times S \to M$ is transverse to X, then for a.e. s, the map $F_s : N \to M$ is transverse to X. ⌟

Proof: Cf.[Smooth Manifold Lee T6.35]. □

Prop. (12.1.4.6) [Transversality Homotopy Theorem]. Suppose N and M are smooth manifolds and $X \subset M$ is an embedded submanifold. Every smooth map $f : N \to M$ is homotopic to a smooth map $g : N \to M$ that is transverse to X. ⌟

Proof: Embed M into an R^k and take a tubular neighbourhood, then we can construct a $N \times D^k$ transversal to M. Cf.[Smooth Manifold Lee T6.36]. □

Prop. (12.1.4.7) [Transversality Extension Theorem]. Let X is a manifold with boundary and $C \subset X$ is a closed subscheme, Z is a closed submanifold of Y. If $f: X \to Y$ is a smooth map that is transversal to Z on C and transversal to Z on $C \cap \partial X$, then there is a map $g: X \to Y$ that is homotopic to f, and $g = f$ on a nbhd of C. ⌟

Proof: Cf.[Pollack P72]. □

Intersection Numbers Modulo 2

Prop. (12.1.4.8) [Intersection Number Modulo 2]. Let X be a compact manifold, and Z is an closed submanifold of Y, where $\dim X + \dim Z = \dim Y$, then for any smooth map $f: X \to Y$ transversal to Z, define $I_2(f, Z)$ as the number of points of $f^{-1}(Z)$ modulo 2. ⌟

Prop. (12.1.4.9) [Boundary Theorem]. If X is the boundary of a smooth manifold W, Z is a closed subscheme of Y that $\dim X + \dim Z = \dim Y$. If $g: X \to Y$ is a map of smooth manifolds that can be extended to $W \to Y$, then $I_2(g, Z) = 0$. ⌟

Proof: Use extension theorem(12.1.4.7), (12.1.4.3) and(12.1.1.32). □

Cor. (12.1.4.10). Let X be a compact manifold, and Z is an closed submanifold of Y, where $\dim X + \dim Z = \dim Y$, then for any smooth maps $f, g: X \to Y$ transversal to Z. If f is homotopic to g, then $I_2(f, Z) = I_2(g, Z)$. ⌟

Proof: Immediate from boundary theorem(12.1.4.9). □

Prop. (12.1.4.11) [Mod 2 Degree of Maps]. If X, Y are manifolds of the same dimension and X is compact, then $I_2(f, \{y\})$ is the same for each $y \in Y$, called the **mod 2 degree of** f. This number is 0 for the boundary of a map, by(12.1.4.9). ⌟

Proof: Cf.[Pollack P80]. □

Orientable Intersection Numbers

Prop. (12.1.4.12) [Preimage Orientation]. Let X, Y is orientable and Z is an orientable closed subscheme in Y. If $f: X \to Y$ is transversal to Z, then the orientation of Z, Y, Z defines canonically an orientation on $f^{-1}(Z)$, called the **preimage orientation** of $f^{-1}(Z)$. ⌟

Def. (12.1.4.13) [Intersection Number]. If X is an orientable smooth manifold, Z is an orientable closed subscheme of an orientable manifold Y that $\dim X + \dim Z = \dim Y$. If $g: X \to Y$ is a map of smooth manifolds that is transversal to Z, then we defined the $I(g, Z)$ to be the sum of the orientations of $f^{-1}(Z)$. ⌟

Lemma (12.1.4.14) [Boundary Theorem]. If X is the boundary of an orientable compact smooth manifold W, Z is an orientable closed subscheme of an orientable manifold Y that $\dim X + \dim Z = \dim Y$. If $g: X \to Y$ is a map of smooth manifolds that is transversal to Z and can be extended to $W \to Y$, then $I(g, Z) = 0$. ⌟

Proof: The same as the proof of(12.1.4.9). □

Prop. (12.1.4.15). Homotopic transversal maps always have the same intersection number w.r.t Z. ⌟

Prop. (12.1.4.16) [Degree of Maps]. If X, Y are orientable manifolds of the same dimension and X is compact, then $I_2(f, \{y\})$ is the same for each $y \in Y$, called the **degree of** f. This number is 0 for a boundary map, by(12.1.4.14). ⌟

Proof: The same as that of(12.1.4.11). □

Cor. (12.1.4.17). The only finite group G that can act freely on S^{2n} is $\mathbb{Z}/2\mathbb{Z}$ or 1. ⌟

Proof: Consider the degree map, then it is a homomorphism from G to $\mathbb{Z}$, thus the image is just ± 1. Now it is by Lefschetz fixed point theorem that $\deg(g) = -1$ for $g \neq 1$, thus it is injective to $\pm$. □

Prop. (12.1.4.18) [General Intersection Number]. The intersection number can be generalized to the case that $g : Z \to Y$ is an arbitrary map of the complementary dimension, and we can define $I(f, g)$. Then:

- f, g are transversal iff $f \times g$ are transversal to Δ_Y.
- $I(f, g) = (-1)^{\dim Z}(f \times g, \Delta_Y)$.

⌟

Proof: This a simple local tangent vector calculation. □

Cor. (12.1.4.19). If $f' \sim f, g' \sim g$, then $I(f, g) = I(f', g')$ if they are definable. This is because $f \times g \sim f' \times g'$. ⌟

Prop. (12.1.4.20). $I(f, g) = (-1)^{\dim X \cdot \dim Z} I(g, f)$. This is obvious from the definition. ⌟

Cor. (12.1.4.21). This shows that the intersection number of a odd-dimensional orientable submanifold of an orientable submanifold with itself is 0. If this fails, then the ambient space is not orientable, for example the Möbius band with the central circle. ⌟

Prop. (12.1.4.22). The Euler character of an orientable compact manifold Y equals the intersection of the diagonals $I(\Delta, \Delta)$. ⌟

Proof: For this, we use the Poincare-Hopf theorem(12.1.4.24). It is clear that on a triangulation, we can place a source on the center of each face/edge/..., thus producing a smooth vector fields, thus it is clear the sum of their indices equals both the combinatorial Euler character and the defined character. □

Cor. (12.1.4.23). The Euler character of an odd dimensional compact manifold Y is 0. ⌟

Prop. (12.1.4.24) [Poincare-Hopf Index theorem]. In a compact manifold M, any vector field V with isolated zeros has sum of its index equal to $\chi(M)$. Where the index of a singularity is the mapping degree of V on a surrounding sphere. ⌟

Proof: Should use Euler character defined in(12.1.4.22), Cf.[Pollack]. □

5 Flow

Def. (12.1.5.1)[Integral Curves]. Let V be a vector field over a smooth manifold M, then an **integral curve** of V is a smooth curve $\gamma : J \to M$ that $\gamma'(t) = V_{\gamma(t)}$ for any $t \in J$. ⌟

Def. (12.1.5.2) [Flow]. Let M be a manifold, then a **flow** on M is a continuous map $\theta : D \to M$, where

- $D \in \mathbb{R} \times M$ is an open subset.
- for any $p \in M, D^p = \{t|(t,p) \in D\}$ is an open interval containing 0.
- When it is defined, $\theta(s, \theta(t,p)) = \theta(s+t,p)$.

If θ is a flow, we define $\theta_t(p) = \theta^{(p)}(t) = \theta(t,p)$.

If θ is smooth, then we can define the **infinitesimal generator** of θ to be the vector field $V_p = \theta^{(p)\prime}(0)$. ⌟

Def. (12.1.5.3)[Complete Vector Fields]. A complete vector field on a smooth manifold is a vector field that generates a global flow. ⌟

Prop. (12.1.5.4). If $\theta : D \to M$ is a smooth flow, then the infinitesimal generator V of θ is a smooth vector field, and each $\theta^{(p)}$ is an integral curve of V. ⌟

Proof: Cf.[Lee13]P212. □

Prop. (12.1.5.5)[Isotopy Extension Theorem]. Let M be a manifold and A be a compact subset. Then an isotopy $F : A \times I \to M$ can be extended to an diffeotopy of M. ⌟

Proof: Consider $F(A \times I) \subset M \times I$ is a compact set, and $TM \times I \to M \times I$ is a vector bundle. The time lines generate a section $F(A \times I) \to TM \times I$, so **??** guarantees an extension $M \times I \to TM \times I$, and because manifolds are locally compact, this section can be chosen to be compactly supported, then the flow it generates is a diffeotopy. □

6 Distributions and Foliations

Cf.[Lee13]Chap19.

7 Smooth Isotopies

Def. (12.1.7.1)[Smooth Isotopies]. For $V, M \in \mathcal{D}\mathrm{iff}$, a **smooth isotopy** is an isotopy $F : V \times I \to M$ that is smooth.

If $V = M$, $F_0 = \mathrm{id}_M$, and each F_t is a diffeomorphism of M, then this is called a **diffeotopy**. ⌟

Thm. (12.1.7.2) [Isotopy Extension Theorem]. Let $V \subset M$ be a compact submanifold and $F : V \times I \to M$ be an isotopy of V, then F extends to a diffeotopy of M with compact support. ⌟

Proof: [Hirch, Differential Topology]P180. □

Thm. (12.1.7.3)[Isotopy Extension Theorem]. let $M \in \mathcal{D}\mathrm{iff}$, $U \subset M$ be an open subset and $A \subset U$ a compact set. Let $F : U \times I \to M$ be an isotopy s.t. $\widehat{F}(U \times I) \subset M \times I$ is open, then there is a diffeotopy of M with compact support, which agrees with F on a nbhd of $A \times I$. ⌟

Proof: [Hirch, Differential Topology]P180. □

8 Morse Theory(Milnor)

Main references are [Mil63] and [Supersymmetry and Morse Theory, Witten].

Def. (12.1.8.1) [Non-Degenerate Critical Point]. For $X \in \mathfrak{Diff}, f \in C^\infty(X)$, a critical point of f is called a **non-degenerate critical point** iff the Hessian matrix is non-singular at x.

The notion of non-degenerate critical is independent of the coordinate chosen. ⌟

Proof: Cf.[Pollack P42]. □

Prop. (12.1.8.2) [Non-Degeneracy is Generic]. Non-degenerate critical points are the general situation in the following sense: For a manifold $M \subset \mathbb{R}^n$, for any smooth function f on M, consider the functions $f_a = f + \sum a_i x_i$, then for almost all (a_i), all critical points of f_a is non-degenerate. ⌟

Proof: Cf.[Pollack P43] □

Prop. (12.1.8.3) [Morse Lemma]. In a non-degenerate critical point of f, there is a coordinate that

$$f = f(p) + x_1^2 + \cdots + x_{n-\lambda}^2 - y_1^2 - \cdots - y_\lambda^2.$$

⌟

Proof: By induction on n, it suffices to show the following: If f is a smooth function on $\mathbb{R}^n$ s.t. $f(0) = 0$ and the origin is a non-degenerate critical point of f, then there is a local coordinate system near 0 s.t. $f(x_1, \ldots, x_n) = \pm x_1^2 + f(0, x_2, \ldots, x_n)$.

By linear algebra, after a linear change of variable, we may assume that the quadratic part of f is of the form $\pm x_1^2 + Q(x_2, \ldots, x_n)$. Then consider the function $g(x) = \frac{\partial}{\partial x_1} f(x)$, then the linear part of g at the origin is $\pm 2x_1$. So by implicit function theorem(11.3.4.1), $\{g(x) = 0\}$ is a smooth hypersurface near the origin with the tangent plane at the origin given by the equation $x_1 = 0$. Then by Taylor's expansion, for any $y = (x_2, \ldots, x_n)$,

$$f(u, y) = f(0, y) + \frac{\partial}{\partial u} f(0, y)x_1 + h(x_1, y)x_1^2 = f(0, y) + h(x_1, y)x_1^2,$$

where h is a smooth function near the origin with $h(0, 0) = \pm 1$. Thus with a change of variable $\widetilde{x}_1 = \sqrt{|h(x_1, y)|}x_1$ and y unchanged, we may assume that $h = \pm 1$. So $f(x_1, y) = \pm u^2 + f(0, y)$, as desired. □

Prop. (12.1.8.4). If $M \in \mathfrak{Diff}, f \in C^\infty(M)$ s.t. $f^{-1}([a, b])$ is compact and with no critical points of f, then $F^{-1}(a)$ is a deformation retracts of $f^{-1}(b)$ using the flow $\operatorname{grad} f / |\operatorname{grad} f|^2$. ⌟

Proof: □

Prop. (12.1.8.5) [Morse Main Lemma]. If f is a smooth function with p a non-degenerate critical point and λ downward pointing direction. If for some $f^{-1}([c - \epsilon, c + \epsilon])$ is compact, then $M^{c+\epsilon}$ is homotopic to $M^{c-\epsilon}$ gluing a λ dimensional cell. ⌟

Proof: Cf.[Milnor Prop3.2]. □

Prop. (12.1.8.6). For an embedded manifold and almost all point p, the distance to p is a morse function. (Use Sard theorem and degenerate $\iff$ p is a focal point. ⌟

Cor. (12.1.8.7). smooth manifold has CW type; on a compact manifold any vector field with discrete singular points has its index sum equal to $\chi(M)$ (Hopf-Rinow), and there exists one. ⌟

Prop. (12.1.8.8). for $\Omega(p,q)^c$ the path space of energy $< c$, the piecewise geodesic path space B (piece fixed), the energy function is smooth and B^a is compact and is the deformation contraction of $\mathrm{int}\Omega^a$ for $a < c$. E has the same critical point and same index and nullity on B and Ω^c. (Just geodesicrize any path in Ω.

So for two point not conjugate in B^a, Ω^a has a finite CW complex type and a λ-dimensional cell for every geodesic of index λ in B^a. ⌟

Prop. (12.1.8.9) [Morse Main Theorem]. If p and q are not conjugate along any geodesic, then $\Omega(p,q)$ has a countable CW complex type and has a λ-cell for every geodesic of index λ.

If M has nonnegative Ricci curvature, then M has only finite cell for every dimension. ⌟

Proof: Cf.[Mil63]Prop17.3. □

Cor. (12.1.8.10). The path space homotopy type only depend on the homotopy type of M (use the two homotopy to id to get a composition of homotopy of the two path space), so one can get the information of path space of M by looking at the homotopy type of M. ⌟

Prop. (12.1.8.11) [Minimal Geodesics]. If p, q in a complete manifold M has distance $\sqrt{d}$ and the minimal geodesics form a topological manifold, and if all non-minimal geodesic has index $\geq \lambda$, then for $0 \leq i < \lambda$, $\pi_i(\Omega, \Omega^d) = 0$. ⌟

Lemma (12.1.8.12). In $SU(2m)$, the minimal geodesic from I to $-I$ is homeomorphic to Grassmannian $G_m(\mathbb{C}^{2m})$ and and non-minimal geodesic has index $\geq 2m+2$.

Similarly, The space of minimal geodesic from I to $-I$ in $O(2m)$ is homeomorphic to the space of complex structures in $\mathbb{R}^{2m}$, and any non-minimal geodesic has index $\geq 2m-2$. ⌟

Proof: Cf.[Milnor Morse Theory Lemma23.1 Lemma24.4]. □

Lemma (12.1.8.13). Ω_{k+1} is homotopic to the space of minimal geodesics in Ω_k from J to $-J$. (The same way, calculate the index of geodesics from J to $-J$ and use (12.1.8.11)). Cf.[Milnor Morse Theory Prop24.5] for definition of Ω_{k+1}. ⌟

9 Others

Real Algebraic Geometry

Prop. (12.1.9.1). Any compact smooth manifolds in $\mathbb{R}^n$ can be approximated by a real algebraic variety. ⌟

Proof: Cf.[Nash's work on Algebraic Geometry]. □

Prop. (12.1.9.2). Let Y be a projective variety over $\mathbb{R}$ and $Z \subset Y$ a closed subvariety, then there exists a triangulation of the pair $(Y(\mathbb{R}), Z(\mathbb{R}))$. ⌟

Proof: Cf.[Hironaka1975, Triangulations of Algebraic Sets] and [Lojasiewicz1964, Triangulation of semi-analytic sets]. □

12.2 Geometric Analysis II

1 Spin Structures

Prop. (12.2.1.1) [Spin Structure Obstruction]. For a oriented real bundle, its transformation map can be chosen to be in $SO(n)$, and constitute a Cech Cohomology $H^1(X, SO(n))$, and by exact sequence of

$$0 \to \pm 1 \to \mathrm{Spin}(n) \to SO(n),$$

this can be lifted to a $H^1(X, \mathrm{Spin}(n))$ iff its image w in $H^2(X, \mathbb{Z}/2\mathbb{Z})$ is 0. and then its inverse image will be parametrized by $H^1(X, \mathbb{Z}/2\mathbb{Z})$ (By the non-commutative spectral sequence of Čech).

We have $w = w_2$, the Whitney class, (Just need to reduce to $sk_2 X$ and in this case, check they both equivalent to the bundle can be lifted). Cf.[XieYi 几何学专题]. Or we can use the Postnikov system of $BO(n)$(4.14.5.2). ⌟

Proof: First prove that if $E \oplus R^n$ is spin, then E is spin, and then pull $H^2(X, \mathbb{Z}/2\mathbb{Z})$ into $H^2(\mathrm{sk}_2(X), \mathbb{Z}/2\mathbb{Z})$, this in a injection, and the homology is natural, so we only have to prove this for $\mathrm{sk}_2(X)$. But E on $\mathrm{sk}_2(X)$ can decompose into a E' of dimension on more than 2, and for this, we see E is Spin iff it is the square of another bundle, so w and w_2 are the same. □

Prop. (12.2.1.2). For a Spin bundle E, the Spin-principal bundle with the Spinor representation(12.12.1.2) will generate a bundle S called the **Spinor bundle**. And the Ad action of $\mathrm{Spin}(n)$ on $Cl_{n,0}$ will generate a **Clifford bundle** $Cl(E)$. The $\mathrm{Spin}(n)$ actions are compatible, so the Clifford bundle can act on the spinor bundle. bundle. The act of the chirality operator on the Spinor bundle will generate two half spinor bundles $S^{\pm}$. Then TM will maps $S^{\pm} \to S^{\mp}$ for n even,(because of anti-commutative with Γ). ⌟

Prop. (12.2.1.3) [Spin^c-structure]. The group Spin^c is the covering space of $SO(n) \times S^1$ (n>2) that corresponds to the group of elements mod 0 mod 2 in $\mathbb{Z}_2 \times \mathbb{Z}$, i.e. $\mathrm{Spin}(n) \times S^1/\{\pm 1\}$.

For example, $\mathrm{Spin}^c(4) = \{(A_1, A_2) \in U(2) \times U(2) | \det A_1 = \det A_2\}$, and $\mathrm{Spin}^C(3) = U(2)$.

Then a $SO(n)$ bundle can be lift to be a Spin^c-bundle if the line bundle determined by S^1 is determine the same w_2 as it, i.e. $w_2 = c_1(L)$ mod 2, This is equivalent to w_2 is in the image of $H^2(X, \mathbb{Z})$, and this is equivalent to the Bockstein image of it is zero.

Use a variant of Wu's formula: $w_2(TM)[\alpha] = \alpha \cdot \alpha (\mathrm{mod}\ 2)$ for M orientable of dimension 4, we have any orientable manifold of dimension 4 has a Spin^c-structure. Cf.[XieYi 几何学专题 Homework3]. ⌟

There is a connection on the Clifford bundle and on the Spinor bundle induced by the Levi-Civita connection of M(12.3.3.2). This is compatible with the Clifford action. and it is also metric because the connection 1-form is in $\mathfrak{so}(n)$ because the action of $SO(n)$ preserves metric.

2 Young-Mills Euqation & Seiberg-Witten Equation

[Atiyah, M. F.; Bott, R. The Yang-Mills equations over Riemann surfaces. Philos. Trans. Roy. Soc. London Ser. A 308 (1983), no. 1505, 523–615.].

Def. (12.2.2.1) [Young-Mills]. The Young-Mills functional on connections A on a bundle E on a compact oriented space:

$$YM(A)^2 = ||F_A||^2 = -\int_X \mathrm{tr}(F_A \wedge *F_A)$$

it is a critical point when $d_A \star F_A = 0$ and $d_A F_A = 0$. ⌟

Prop. (12.2.2.2) [2-dim Case]. $\star F \in \Omega^0(su(E))$ is parallel thus its characteristic spaces is orthogonal and a stable under parallel transport. So an irreducible YM $SU(2)$-connection must by flat, thus correspond to irreducible $SU(2)$ representation of $\pi_1(X)$. ⌟

Prop. (12.2.2.3) [4-dim Case]. $** = (-1)^{2*2} = \mathrm{id}$ on $\Omega^2(E)$ on E a $SU(n)$-bundle, so $\Omega^2(E) = \Omega^+ \oplus \Omega^-$. We have

$$||F_A^+||^2 + ||F_A^-||^2 \geq ||F_A^-||^2 - ||F_A^+||^2 = \int_X \mathrm{tr}(F_A \wedge F_A) = 8\pi^2 c_2(E)$$

Cf.[谢毅 Lecture5]. So it attains minimum at the connection that $*F_A = \pm F_A$ and $d_A F_A = 0$.((Anti)self-dual((anti)instanton)) depending on the sign of $c_2(E)$. ⌟

Prop. (12.2.2.4) [Anti-Instanton Connection on Complex Line Bundle]. For a $U(1)$-bundle, $d_A F_A = dF_A$, so F_A is harmonic, thus $c_1(L) = [\frac{-1}{2\pi i} F_A] \in H^2(X, \mathbb{Z}) \cap \mathcal{H}^2_-(X, \mathbb{R})$, In fact, this is equivalent to the existence of a anti-self-dual connection on this bundle.

If this is the case, then we have the ASD-connections module Gauge equivalence is isomorphic to $H^1(X, \mathbb{R})/H^1(X, \mathbb{Z}) = T^{b_1(X)}$. ⌟

Proof: Because a gauge is just a $X \to S^1$, and its connected component thus equals $[X, S^1] = H^1(X, \mathbb{Z})$ (MacLane space), and its identity is just the map that is homotopic to id. and $d(gA) = dA - g^{-1}dg = dA - idu$, for $g = exp(iu)$, so $\Omega^1/\mathcal{G} = H^1(X, \mathbb{R}/H^!(X, \mathbb{Z}) = T^{b_1(X)}$. □

Lemma (12.2.2.5) [Weizenbock Formula]. On a Riemannian manifold M, the Laplace operator has the form:

$$\Delta = -\nabla^2_{e_i e_i} - \xi^i \wedge \iota(e_j) R(e_i, e_j)$$

where $\nabla^2_{X,Y} = \nabla_X \nabla_Y - \nabla_{\nabla_X Y}$.

$$\int |\mathcal{D}_A \varphi|^2 = \int |\nabla_A \varphi|^2 + \frac{1}{4} R |\varphi|^2 + \frac{1}{2} \langle F_A^+ \varphi, \varphi \rangle.$$

If M is a spin manifold, then the Dirac operator D satisfies:

$$D^2 = -\nabla^2_{e_i e_i} + \frac{1}{4} R$$

where R is the scalar curvature form on M. If M is a $Spin^c$ manifold with a $Spin^c$ connection ∇_A, then the Dirac operator satisfies

$$D_A^2 = -\nabla^2_{A, e_i e_i} + \frac{1}{4} R + \frac{1}{2} F_A$$

Cf.[Geometric Analysis Jost P143,153]. ⌟

Prop. (12.2.2.6) [Seiberg-Witten]. The Seiberg-Witten equation functional for a unitary connection A on the determinant bundle of a Spin^c structure of M and a section of $\mathcal{S}^+$ is:

$$\begin{aligned} SW(\varphi, A) &= \int \Big(|\nabla_A \varphi|^2 + |F_A^+|^2 + \frac{R}{4} |\varphi|^2 + \frac{1}{8} |\varphi|^2 \Big) Vol. \\ &= \int \Big(|\mathcal{D}_A \varphi|^2 + |F_A^+ - \frac{1}{4} \langle e_j e_k \varphi, \varphi \rangle e^j \wedge e^k|^2 \Big) Vol \end{aligned}$$

So the Seiberg-Witten equation is the lowest topological possible value of the Seiberg-Witten functional. It writes:

$$\mathcal{D}_A \varphi = 0, \quad F_A^+ = \frac{1}{4} \langle e_j e_k \varphi, \varphi \rangle e^j \wedge e^k.$$

Cf.[Jost Chapter 7]. ⌟

Cor. (12.2.2.7). If a compact oriented Spin^c manifold M has nonnegative scalar curvature, then the only possible solution is $\varphi = F_A^+ = 0$. (See from the equivalence of forms of Seiberg-Witten functional.) ⌟

3 Chern-Weil Theory

Prop. (12.2.3.1) [Chern-Weil]. An **Invariant polynomial** of a the entries of $M_n(k)$ is one that is invariant under the conjugation action(3.3.4.5).

For any connection on E, the **Chern-Weil** map CW from invariant polynomial ring to $H^*(X) : P \mapsto [P(\Omega)]$ is a ring homomorphism independent on the connection A.

There are relations between c_i and $\mathrm{tr}(\Omega^k)$, they can be derived formally by considering diagonal elements. ⌟

Proof: To prove $P(\Omega)$ is closed, notice by(3.3.4.5), it suffice to show $\mathrm{tr}(\Omega^k)$ is closed. By(12.3.3.7), $d\,\mathrm{tr}(\Omega^k) = \mathrm{tr}(\omega \wedge \Omega^k - \Omega^k \wedge \omega) = 0$, which is zero because Ω is of even dimension.

For the independence of connections, use(4.14.3.28). For two connection ∇_i, $\nabla = t\nabla_0 + (1-t)\nabla_1$(you can smooth it) is a connection on the vector bundle $\pi^* E$ on $M \times I$, and the section 0 and 1 induces the connection ∇_0 and ∇_1. Thus s_0^* and s_1^* are the same map, thus $CW_M(p) = s_i^* CW_{M\times I}(p)$ are all the same map. □

Cor. (12.2.3.2). For a complex line bundle of degree r over a complex manifold,

$$\det(1 - \frac{1}{2\pi i} F_A) = 1 + c_1 + \ldots + c_r$$

gives out the **Chern class**, because it satisfies the axioms of Chern class (4.15.4.16). In other words, $c_k = \mathrm{tr}((-\frac{1}{2\pi i} F_A)^k)$.

For a real line bundle of degree r,

$$\det(1 - \frac{1}{2\pi i} F_A) = 1 + p_1 + \ldots + p_{\lfloor \frac{r}{2} \rfloor}$$

gives out the **Pontryagin class**, where $p_k \in H^{4k}(X)$. (Notice the ω thus Ω can be chosen to be skew-symmetric, thus for odd k the classes $\mathrm{tr}(\Omega^k) \in H^{2k}(X)$ vanish).

For an oriented real bundle of degree $2r$, the ω and thus Ω can be chosen to be skew-symmetric and the transformation matrix in $SO(2r)$, then

$$\mathrm{Pf}(\frac{1}{2\pi}\Omega) \in H^{2r}(X)$$

is well-defined and closed and gives the **Euler class** $e(E)$ (recall $e(E)^2 = p_r(E)$). (Use $\mathrm{Pf}^2 = \det$ to get that $[\frac{\partial \mathrm{Pf}}{\partial \Omega_{ij}}]^t$ commutes with Ω, then calculate $d\mathrm{Pf}(\Omega) = 0$). ⌟

Proof: In fact, the construction is natural w.r.t the connection because connection can be pulled back and summed. Then the only task is the normality, which is direct calculation on $\mathbb{CP}^1$. □

Cor. (12.2.3.3).

$$c_1(E) = c_1(\wedge^{\dim E} E).$$

Direct from the formula. ⌟

Cor. (12.2.3.4) [Whitney Product Formula].

$$c(E\oplus F)=c(E)c(F),\quad p(E\oplus F)=p(E)p(F)$$

Directly form the product connection on $E\oplus F$. ⌟

Prop. (12.2.3.5) [Chern Character]. The Chern character

$$ch(E)=[\operatorname{tr}\operatorname{expo}(\frac{i}{2\pi}F_A)]$$

satisfies $ch(E\oplus F)=ch(E)+ch(F)$ and $ch(E\otimes F)=ch(E)ch(F)$ by simple calculation. So it defines a ring homomorphism from $K(X)$ to $H^*(X)$. ⌟

Prop. (12.2.3.6) [Chern-Gauss-Bonnet]. For a $2n$-dimensional orientable manifold M,

$$\int_M e(TM)=\chi(M).$$

⌟

Prop. (12.2.3.7). For a vector bundle and a flat connection d_A on a manifold, i.e. $d_A^2=0$, we have a deRham like cohomology, and there is a sheaf of flat sections.

$$H^*(X,A)=H^*(X,E).$$

⌟

4 Index Theorems(Atiyah-Singer)

References are [Heat equation and the Index Theorem Atiyah] and [Index Theorem].

Prop. (12.2.4.1) [Gilkey]. For a natural transformation ω from the functor $p: M\to$ the Riemannian structure on M to the functor $q: M\to k$-forms on M, if it is homogenous of weight 0 w.r.t to metric g(i.e. $\omega(\lambda^2 g)=\omega(g)$) and in local coordinates it has the coefficients of $\omega(g)$ generated by g_{ij} and $\det g^{-1}$ and their derivatives , then is is a polynomial of Pontryagin classes of the given dimension. (not only up to homology). ⌟

Proof: Cf.[Heat equation and the Index Theorem Atiyah P284]. □

Prop. (12.2.4.2) [Gilkey Generalized]. For a natural transformation ω from the functor $p: M\to$ Riemannian structures on M with a Hermitian bundle E with a Hermitian connection and the functor $q: M\to k$-forms on M, if it is homogenous of weight $(0,0)$ w.r.t to metric g,h and the Hermitian structure(i.e. $\omega(\lambda^2 g,\mu^2\xi)=\omega(g,\xi)$) and in local coordinates it has the coefficients of $\omega(g,\xi)$ generated by $g_{ij},h_{ij},\det h^{-1},\det g^{-1}$ and Γ_k^{ij}(the connection form) and their derivatives, then is is a polynomial of Pontryagin classes and Chern classes of E of the given dimension. (not only up to homology). ⌟

Proof: Cf.[Heat equation and the Index Theorem Atiyah P290]. □

Cor. (12.2.4.3). For a natural transformation ω from the functor $p: M\to$ Hermitian bundle E on M with a Hermitian connection and the functor $q: M\to k$-forms on M, if it is homogenous of weight 0 w.r.t to metric h and the Hermitian structure(i.e. $\omega(\mu^2\xi)=\omega(\xi)$) and in local coordinates it has the form $\omega(g,\xi)$ generated by $h_{ij},\det h^{-1}$ and Γ_k^{ij}(the connection form) and their derivatives, then is is a polynomial of Chern classes of E of the given dimension. Because when composed with the forgetful functor, it gives a transformation as above. And it is obviously independent of g. ⌟

Prop. (12.2.4.4) [Hodge]. For any differential operator A from a vector bundle E to a vector bundle F, we form two operators AA^* and A^*A, then they are both self adjoint elliptic operators, let these corresponding eigenspace be $\Gamma_\lambda(E)$ and $\Gamma_\lambda(F)$, then A and A^* define an isomorphism between $\Gamma_\lambda(E)$ and $\Gamma_\lambda(F)$. ⌟

Proof: □

Prop. (12.2.4.5) [Hirzebruch Signature Formula]. On a $4n$-dimensional orientable manifold M, the Poincare duality defines a bilinear pairing $H^{2n}(M)\times H^{2n}(M)\to\mathbb{R}$, its signature $\sigma(M)$ is given by:

$$\sigma(M)=\int_M L_n(p_1,\ldots,p_n).$$

Where L_n is the degree n part of the Taylor expansion of $\prod_{i=1}^r\dfrac{\sqrt{x_i}}{\tanh\sqrt{x_i}}$ in terms of the symmetric polynomial. ⌟

Proof: We consider the operator $\tau:\alpha\mapsto i^{l+p(p-1)}*\alpha$, $\tau^2=1$, thus Γ^* is decomposed into two eigenspaces of τ. We define the **signature operator** A as the restriction of $\Delta=d-\tau d\tau$ to Γ_+. Δ anti commutes with τ thus maps Ω_+ to Ω_-, then we have $\ker A=\ker\Delta\cap\Omega_+$, which is the positive harmonic forms H_+. So

$$\mathrm{Ind}A=\dim H_+-\dim H_-.$$

And we notice the positive and negative harmonic forms neutralize each other unless on the $2n$-forms, so only need to consider them. In fact, if we consider $4n+2$ manifolds, then τ is pure imaginary and the conjugation neutralize even the $2n+1$ forms, so there are no signature.

Now the inner product $\alpha\to\int\alpha\wedge*\alpha$ is positive definite for a real form α, so this index of A is just the signature of the intersection form defined by cup product. □

Cor. (12.2.4.6). For a $4n$-dimensional M which is a boundary of a manifold, its signature is 0. ⌟

Proof: By Stokes theorem, if M is a boundary of a manifold, then all its Pontryagin numbers, i.e. $\int_M\prod p_i^{n_i},\sum n_i=n$, vanish. □

Prop. (12.2.4.7) [Generalized Hirzebruch Signature Formula]. Let M be a $2l$ dimensional smooth manifold and E be a Hermitian bundle over M, then The index of the generalized signature operator is giving by

$$\mathrm{Ind}A_\eta=2^l\cdot ch(E)L(p_1,\ldots,p_l).$$

where $L(M)(p_i)=\prod\dfrac{x_i/2}{\tanh x_i/2}$. ⌟

Prop. (12.2.4.8) [Hirzebruch-Riemann-Roch]. For a n-dimensional complex line bundle L over a compact Kähler manifold M,

$$\chi(M,L)=\int_M[\mathrm{ch}(E)\mathrm{td}(T^{1,0}M)]_n.$$

Where $\chi(M,L)=\sum_{q=0}^n(-1)^q\dim H^q(M,E)$, ch is the Chern character(12.2.3.5) and $\mathrm{td}(T^{1,0}M)$ is the Todd polynomial, i.e. Taylor expansion of $\prod_{i=1}^r\dfrac{t_i}{1-e^{-t_i}}$ in terms of the symmetric polynomial, applied to $c_i(T^{1,0}M)$. ⌟

Cor. (12.2.4.9) [Riemann-Roch]. For a n-dimensional complex vector bundle E over a Riemann Surface M, let $\deg E = \int_M c_1(E)$, then

$$\chi(M,E) = H^0(M,E) - \dim H^1(M,E) = \deg E + \mathrm{rk}(E)(1-g).$$

Cf.[Index Theorem P115]. ⌟

Hodge Theory

Prop. (12.2.4.10) [Hodge]. By(11.12.8.12), if we investigate the Laplace operator Δ_d on a compact orientable Riemannian manifold, we get that

$$\Omega^i = \mathcal{H}^i \oplus \mathrm{Im}\,\Delta_d = \mathcal{H}^i \oplus \mathrm{Im}\,d \oplus \mathrm{Im}\,d^*.$$

Thus H^i can be uniquely represented by elements of $\mathcal{H}^i$. ⌟

Proof: It suffice to prove Δ_d is self-adjoint elliptic.

$\mathrm{Im}\,\Delta_d \subset \mathrm{Im}\,d \oplus \mathrm{Im}\,d^*$, and the result follows if we show $\mathcal{H}^i, \mathrm{Im}\,d, \mathrm{Im}\,d^*$ are orthogonal. In fact, let ω be harmonic, then $(\omega, d^*\xi) = (d\omega,\xi) = 0$, $(\omega, d\eta) = (d^*\omega,\eta) = 0$, $(d\eta, d^*\xi) = (dd\eta,\xi) = 0$. □

Cor. (12.2.4.11) [Poincare Duality for deRham Cohomology]. If M is a n-dimensional compact orientable Riemannian manifold, then

$$H^p_{dR}(M) \cong H^{n-p}_{dR}(M)$$

Induced by $*$, because $** = \pm 1$ and $*$ commutes with Δ_d(12.1.3.10), so it induce an isomorphism $\mathcal{H}^p \cong \mathcal{H}^{n-p}$.

Moreover, $*$ in fact induces a perfect pairing:

$$H^k_{dR}(M) \times H^{n-k}(M) \to \mathbb{R}$$

induced by the map

$$* : \mathcal{H}^k(M) \times \mathcal{H}^{n-k}(M) \to \mathbb{R} : (\alpha,\beta) \mapsto \int_M \alpha \wedge *\beta$$

As $\int_M \alpha \wedge *\alpha = ||\alpha||^2 \neq 0$. ⌟

Prop. (12.2.4.12). On a compact complex manifold, the formal adjoint of $\overline{\partial}$ is $*\partial *$. (By direct calculation). Also $d^* = (-1)^{n(p+1)+1} * d* = - * d*$. ⌟

Prop. (12.2.4.13) [Hodge]. Given a compact Hermitian complex manifold (X,J,g) and a holomorphic line bundle E over it, there is a Hermitian metric on $A^{p,q}E$, and an operator $\overline{\partial}$ on it. Then $\overline{\partial}$ has a formal adjoint $\overline{\partial}^*$, and $\Delta_{\overline{\partial}_E}$ can be defined. Let $\mathcal{H}^{p,q}_E$ be the kernel of $\Delta_{\overline{\partial}}$ on $A^{p,q}E$, called the **E-valued (p,q)-forms**, then there is a orthonormal decomposition

$$A^{p,q}E = \mathcal{H}^{p,q}_E \oplus \mathrm{Im}\,\Delta_{\overline{\partial}_E} = \mathcal{H}^{p,q}_E \oplus \mathrm{Im}\,\overline{\partial}_E \oplus \mathrm{Im}\,\overline{\partial}^*_E$$

And thus $\mathcal{H}^{p,q}(X,E) \cong H^{p,q}_{\overline{\partial}}(X,E)$. ⌟

Proof: It suffice to prove $\Delta_{\overline{\partial}_E}$ is self-adjoint elliptic. The rest is verbatim as the proof of(12.2.4.10). □

Cor. (12.2.4.14) [Hodge]. In case $E = \mathcal{O}_X$, $\mathcal{H}^{p,q}(X) \cong H^{p,q}_{\overline{\partial}}(X)$. ⌟

Cor. (12.2.4.15) [Kodaira-Serre Duality]. For a Hermitian line bundle over a compact Hermitian complex manifold X, from Hodge theorem and(12.8.5.2), we get

$$H^p(X,\Omega^q(E)) \cong H^{n-p}(X,\Omega^{n-q}(E^*))$$

induced by $\overline{*}_E$ and $\overline{*}_{E^*}$. ⌟

12.3 Riemannian Geometry

??.

Basic references are [Riemannian Geometry Do Carmo], [Geometric Analysis Jost] and [Differentia Geometry Loring Tu].

1 $\mathbb{R}^3$-Geometry

Different Coordinates

Prop. (12.3.1.1). In a polar coordinate,

$$g_{11} = 1, g_{12} = 0, g_{22} = |\frac{\partial}{\partial\theta} f|^2, \quad K = -\frac{(\sqrt{g_{22}})_{\rho\rho}}{\sqrt{g_{22}}}$$

And $\sqrt{g_{22}} \sim \rho$. (Use the formula relating Jacobi Field with curvature) ⌟

Moving Frame Method

Thm. (12.3.1.2) [Theorema Egregium, Gauss1827].

$$R_{1212} = K(g_{11}g_{22} - g_{12}^2)$$

Which is a special case of the definition of curvature. ⌟

Proof: □

Prop. (12.3.1.3) [Gauss-Bonnet]. Let M be a compact oriented 2-dimensional Riemannian manifold, then

$$\chi(M) = \frac{1}{2\pi}\int_M K \text{ Vol}.$$

⌟

Proof: Should be an direct corollary of(12.2.3.6). □

Topology and Geometry

Prop. (12.3.1.4). Every compact orientable surface of genus $p > 1$ can be provided with a metric of constant negative curvature. ⌟

Proof: □

Remark (12.3.1.5) [Hilbert Theorem]. There exist complete surfaces with $K \leq 0$ in $\mathbb{R}^3$, but the hyperbolic surface cannot be immersed into $\mathbb{R}^3$. ⌟

2 Basics

Prop. (12.3.2.1). If the metric tensor on the tangent space is g in a coordinate, then it is g^{-1} in the cotangent space. (Follows from**??**). ⌟

3 Connections

Def. (12.3.3.1) [Affine Connection]. An **affine connection** on a vector bundle E is a map $D : \Gamma(E) \to \Gamma(E) \otimes \Gamma(T^*M)$ that satisfies differential-like properties, it can be written as $D = d + \omega$, with $\omega \in \Omega^1(\mathrm{End}(E))$. ⌟

Prop. (12.3.3.2) [Transformation Law]. In two coordinates $\overline{e} = ea$ for $a : U \to GL(r, \mathbb{R})$, $d_A = d + \omega, d + \overline{\omega}$, then $\overline{\omega} = a^{-1}\omega a + a^{-1}da$.

Moreover, giving any locally compatible $d + \omega$,$\omega \in \Omega^1(\mathfrak{g})$ in the sense above, then for any G-associated bundle E, where G has lie algebra $\mathfrak{g}$, there is a connection that locally looks like $d + \omega$, (where $\mathfrak{g}$ embeds into $\mathfrak{gl}(E)$). ⌟

Cor. (12.3.3.3) [Local Nature of Connection]. From the description of connection given above, it's easy to say if the is a local connection that satisfies these transformation laws, then it generate a global connection. So by partition of unity(4.4.7.9), connection exists in any vector bundle over a manifold. ⌟

Cor. (12.3.3.4) [Simplification]. $d_{gA}(s) = gd_A(g^{-1}(s))$, So for any connection d_A and any point x_0, there is a gauge transformation that makes $d_A = d$ at x_0. ⌟

Proof: Just need to have $s(x_0) = \mathrm{id}$, $ds(x_0) = -A(x_0)$. this is possible because $A \in \Omega^1(\mathrm{Ad}E)$ which is the fiber of the frame bundle, use exp. □

Prop. (12.3.3.5) [Induced connections]. The connection action $d_A = d + \omega$ on a vector bundle E induces connection on many relevant bundles. the action on dual bundle is by

$$d_A(s^*) = ds^* - \omega^t(s^*) = ds^* - s^* \circ \omega.$$

And the connection on $\mathrm{End}\, E$ by

$$d_A(\alpha) = d\alpha + [\omega, \alpha] = [\nabla, \alpha]$$

And they act on $\Omega^*(E)$ by Leibniz rule thus the formula looks the same. (Note that the convention is section write on the left of the differential forms, so for example, $[\omega, \omega] = 2\omega \wedge \omega$). ⌟

Proof: Cf.[Jost P110]. □

Cor. (12.3.3.6). For a line bundle L, for a connection on it with curvature Ω, the induced on the dual line bundle L^* has connection $-\Omega$. (because $\Omega = d\omega$ and $\omega' = -\omega$). ⌟

Prop. (12.3.3.7) [Second Bianchi's Identity]. A affine connection on E looks locally like $d_A = d + \omega$, where $\omega \in \Omega^1(\mathrm{End}\, E)$. And $F_A = d_A \circ d_A \in \Omega^2(\mathrm{End}(E))$ satisfies

$$d_A F_A = dF_A + [\omega, F_A] = 0.$$

⌟

Proof: Notice $dF_A = dd\omega + d(\omega \wedge \omega) = d\omega \wedge \omega - \omega \wedge d\omega$, and $\omega(d\omega + \omega \wedge \omega) - (d\omega + \omega \wedge \omega)\omega = \omega \wedge d\omega - d\omega \wedge \omega$. □

Def. (12.3.3.8) [Christoffel Symbol]. The **Christoffel symbol** of a connection is defined by the equations: $\nabla_{X_i} X_j = \sum_k \Gamma_{ij}^k X_k$.

The **geodesic equations** is $\dfrac{D}{dt}(\dfrac{d\gamma}{dt}) = \ddot{x}_k + \sum_{i,j} \Gamma_{ij}^k \dot{x}_i \dot{x}_j = 0 \quad \forall k$. ⌟

Def. (12.3.3.9). The **torsion tensor** of a connection ∇ on TM is defined as $T(X,Y)=\nabla_X Y-\nabla_Y X-[X,Y]$. The connection is called **torsion-free** if $T=0$. This is equivalent to $\Gamma^k_{i,j}=\Gamma^k_{j,i}$.

A connection is called **metric** if it preserves metric. i.e. $\nabla g=0$. ⌟

Proof: T is a tensor because it is skew-symmetric, and

$$T(fX,Y)=f\nabla_X Y-f\nabla_Y X-df(Y)X-(f[X,Y]-df(Y)X)=fT(X,Y),$$

where(12.1.3.5) is used. □

Prop. (12.3.3.10). If ∇ is torsion-free connection on TM, then its induced connection on T^*M satisfies

$$(d\alpha)(v_1,\ldots,v_k)=\sum(-1)^i(D_{v_i}\alpha)(v_1,\ldots,\widehat{v_i},\ldots,v_k).$$

⌟

Proof: □

Def. (12.3.3.11) [Curvature Tensor]. The **curvature** of a (affine) connection d_A is $F_A=d_A\circ d_A\in\Omega^2(\mathrm{End}(E))$. The curvature tensor it induced is

$$F_A(Z)(X,Y)=R(X,Y)Z=D_YD_XZ-D_XD_YZ+D_{[X,Y]}Z.$$

In particular, the curvature depends only on the point, and locally $F_A=d\omega+\omega\wedge\omega$

In two coordinates $\overline{e}=ea$ for $a:U\to GL(r,\mathbb{R})$,$\overline{F_A}=a^{-1}F_Aa$.

The connection is called **flat** if $F_A=0$.

⌟

Proof: To verify the equation, check first the left side is pointwise, and the third component of the right side assures it is pointwise, too, thus we can check for a local coordinate vector field($[X_i,X_j]=0$), then because $\nabla s=\sum_i\nabla_i s dx_i$,

$$\nabla^2 s=\nabla(\sum_i\nabla_i s dx_i)=\sum_{ij}\nabla_j\nabla_i s dx_j dx_i=\sum_{i<j}(\nabla_i\nabla_j-\nabla_j\nabla_i)s dx_i\wedge dx_j$$

□

Prop. (12.3.3.12)[Flat coordinate]. A connection on TM assumes near every point a flat coordinate, i.e. $\nabla(\partial/\partial x^i)=0$, iff it is flat and torsion-free. ⌟

Proof: One side is easy because its Christoffels vanish. On the other side, use integrability theorems (11.12.6.2). Cf.[Jost P115]. □

Prop. (12.3.3.13).

$$\Delta\langle\varphi,\varphi\rangle=2(\langle D^*D\varphi,\varphi\rangle-\langle D\varphi,D\varphi\rangle).$$

⌟

Proof: Cf.[Jost P118]. □

Prop. (12.3.3.14). For a flat connection, there is a bundle isomorphism (Gauge transform) that transforms d_A into natural d. ⌟

Proof: Because $d_{gA}(s) = g d_A(g^{-1}(s))$,$d_{gA} = d - dg \cdot g^{-1} + g \cdot \omega \cdot g^{-1}$. Solve this PDE direvtly. (Cf.[Topics in Geometry Xie Yi week3]). □

Cor. (12.3.3.15). For a flat connection, by(12.3.3.14), the parallel transportation only depends on the homotopy type of the loop, thus gives an action of $\pi(X)$ on $SO(T_p(X))$ (or $SU(T_p(X))$. (because it is locally constant).

In this way, connections module gauge equivalence (preserving matric) equals representation of $\pi(X)$ module conjugations. The reverse map is giving by principal bundle. ⌟

Proof: □

Levi-Civita Connection

Def. (12.3.3.16)[Levi-Civita Connection]. The Levi-Civita connection is the unique connection on M that is metric and torsion-free:

$$X\langle Y, Z\rangle = \langle \nabla_X Y, Z\rangle + \langle Y, \nabla_X Z\rangle, \qquad \nabla_X Y - \nabla_Y X = [X, Y].$$

It satisfies:

$$\langle Z, \nabla_Y X\rangle = 1/2\{X\langle Y, Z\rangle + Y\langle Z, X\rangle - Z\langle X, Y\rangle - \langle [X, Z], Y\rangle - \langle [Y, Z], X\rangle - \langle [X, Y], Z\rangle\}.$$

Then

$$\Gamma_{ij}^m = 1/2 \sum_k \Big\{g_{jk,i} + g_{ki,j} - g_{ij,k}\Big\} g^{km}$$

Thus geodesic is a solution that only depends on the metric(12.3.3.8), so a local isometry preserves geodesics. ⌟

Prop. (12.3.3.17). Now the Lie derivative has the form:

$$L_X(S)(Y_1, \ldots, Y_p) = \nabla_X(S)(Y_1, \ldots, Y_p) + \sum_{i=1}^p S(Y_1, \ldots, Y_{i-1}, \nabla_{Y_i} X, \ldots, Y_p).$$

The exterior derivative d and its adjoint d^* has the form:

$$d\omega(Y_i) = \sum (-1)^p \nabla_{Y_i} \omega(\check{Y_p}), \quad d^*\omega(Y_i) = -\sum \nabla_{e_j} \omega(e_j, Y_i)$$

where e_i is an orthonormal basis. Cf.[Jost P140].

⌟

Prop. (12.3.3.18)[Covariant Differential Symmetry]. For a parametrized surface: $s : (u, v) \to M$,

$$\frac{D}{\partial u}\frac{\partial s}{\partial v} = \frac{D}{\partial v}\frac{\partial s}{\partial u}.$$

⌟

Proof:

$$\frac{D}{\partial u}\frac{\partial s}{\partial v} = \frac{D}{\partial u}(\sum \frac{\partial s_i}{\partial v} X_i) = \frac{\partial^2 s_i}{\partial u \partial v} + \sum \frac{\partial s_i}{\partial v}(\sum \frac{\partial s_j}{\partial u} \nabla_j X_i) = \frac{\partial^2 s_i}{\partial u \partial v} + \sum_{ij} \frac{\partial s_i}{\partial v}\frac{\partial s_j}{\partial u} \nabla_j X_i$$

But now the Levi-Civita connection is symmetric, thus $\nabla_j X_i = \nabla_i X_j$, showing the symmetry in u and v. □

Lemma (12.3.3.19) [Gauss]. Let $p \in M$ and $v \in T_pM$ s.t. $\exp_p v$ is defined, $w \in T_pM$, then

$$\langle (d\exp_p)_v(v), (d\exp_p)_v(w)\rangle = \langle v, w\rangle.$$

⌟

Proof: Cf.[Do Carmo P69]. □

Prop. (12.3.3.20) [Geodesic Locally Minimizing]. In a normal nbhd of p, the geodesic starting at p is the minimal line. ⌟

Proof: And curve $c(t)$ can be written as $\exp_p(r(t)v(t)) = f(r(t), t)$, where $f(s,t) = \exp_p(sv(t))$, so by Gauss lemma, $\langle \frac{\partial f}{\partial r}, \frac{\partial f}{\partial t}\rangle = 0$. Now $dc/dt = \partial f/\partial r r'(t) + \partial f/\partial t$, so

$$|dc/dt|^2 = |r'(t)|^2 + |\partial f/\partial t|^2 \geq |r'(t)|^2.$$

Integrate this will give us the desired result. □

Prop. (12.3.3.21) [Totally normal nbhd]. For any point p, there exists a nbhd W and a number $\delta > 0$ s.t. for every $q \in W$, $\exp_q$ is a diffeomorphism on $B_\delta(0)$ and $\exp_q(B_\delta(0)) \supset W$. Thus, fine cover exists in every smooth manifold, because Riemannian metric exists on these manifolds. ⌟

Proof: Cf.[Do Carmo P72]. □

- (**Geodesic Frame**) In a neighborhood of every point p, there exists n vector fields, orthonormal at each point, and $\nabla_{E_i}E_j(p) = 0$.(Choose normal nbhd and parallel a orthonormal basis to every point. (WARNING: this is not a flat coordinate, it only helps when dealing with point-wise properties).

Def. (12.3.3.22) [Killing Fields]. A **Killing field** is a vector field which generates an infinitesimal isometry. X is killing $\iff L_X(g) = 0 \iff \langle \nabla_Y X, Z\rangle + \langle \nabla_Z X, Y\rangle = 0$ for all Y, Z, which is called the **Killing equation**. ⌟

Proof: Use Lie formula,

$$L_X(g)(Y,Z) = X\langle Y, Z\rangle - \langle [X,Y], Z\rangle - \langle Y, [X,Z]\rangle$$

. and Levi-Civita connection is torsion-free. □

Prop. (12.3.3.23). Let M be a compact Riemannian manifold of even dimension with positive sectional curvatures, then every Killing field on M has a singularity. ⌟

Proof: Cf.[Do Carmo P104]. □

Def. (12.3.3.24) [Geometric Differential Notations]. For $f \in C^\infty(M), X \in \Gamma(M, TM)$,

- The **gradient** of f is defined to be the tangent field $\operatorname{grad} f \in \Gamma(M, TM)$ s.t. for any $X \in \Gamma(M, TM)$, $\langle \operatorname{grad} f, X\rangle_p = X(f)(p)$.
- The **divergence** of X is defined to be a function $\operatorname{div} X \in C^\infty(M)$ s.t. for any $p \in M$, $\operatorname{div} X(p) =$trace of the linear map $Y(p) \to \nabla_Y X(p) = \sum_i \langle \nabla_{E_i} X, E_i\rangle$. It measures the variation of the volume and it depends only on the point.
- The **Hessian** of f is defined to be a symmetric form $\operatorname{Hess} f \in \Gamma(M, T^*M^{\otimes 2}) \cong \operatorname{Hom}(TM, TM)$ s.t. for any $Y, Z \in \Gamma(M, TM)$, $(\operatorname{Hess} f)(Y,Z) = \langle (\operatorname{Hess} f)Y, Z\rangle$ where $(\operatorname{Hess} f)Y = \nabla_Y \operatorname{grad} f$.

- The **Laplacian** of f is defined to be the function $\Delta f = \operatorname{div}\operatorname{grad} f = \operatorname{tr}(\operatorname{Hess} f) \in C^\infty(M)$.

⌟

Prop. (12.3.3.25). In a geodesic frame,

$$\operatorname{grad} f(p) = \sum_{i=1}^n (E_i(f))E_i(p)$$

$$\operatorname{div} X(p) = \sum_{i=1}^n E_i(f_i)(p), \text{where} X = \sum_i f_i E_i.$$

$$\Delta f = \sum_i E_i(E_i(f))(p).$$

⌟

Cor. (12.3.3.26).

$$\Delta(f\cdot g) = f\Delta g + g\Delta f + 2\langle \operatorname{grad} f, \operatorname{grad} g\rangle,$$

because these only depends on the point. ⌟

Prop. (12.3.3.27). $d(i(X)m) = (\operatorname{div} X)m$. where m is the volume form. ⌟

Proof: Choose a geodesic frame E_i, θ_i is a dual form of E_i, let $X = \sum f_i E_i$, then $\iota(X)m = \sum_i (-1)^{i+1} f_i\theta_i$, so

$$d(\iota(X)m) = \sum(-1)^{i+1} df_i \wedge \theta_i + \sum(-1)^{i+1} f_i \wedge d\theta = (\sum E_i(f_i))m + \sum(-1)^{i+1} f_i \wedge d\theta.$$

Notice that $d\theta_i = 0$, because $d\theta_k(E_i, E_j) = E_i\theta_k(E_j) - E_j\theta_k(E_i) - \theta_k([E_i, E_j]) = 0$(12.1.3.6), as it is a geodesic frame. And $\sum E_i(f_i) = \operatorname{div}(X)$(12.3.3.25). □

Prop. (12.3.3.28) [Hopf theorem]. If f is a differentiable function on a compact orientable manifold with $\Delta f \geq 0$, then f is constant. ⌟

Proof: Let $\operatorname{grad}(f) = X$, then

$$\int_M \Delta f dm = \int_M \operatorname{div}(X) dm = \int_M d(\iota(X)dm) = 0.$$

So $\Delta f = 0$. Now

$$0 = \int_M \Delta(f^2/2) dm = \int_M f\Delta f dm + \int_M |\operatorname{grad}(f)|^2 dm$$

by(12.3.3.26), thus $\operatorname{grad}(f) = 0$, so f is constant. □

Def. (12.3.3.29) [Riemannian Curvatures].

- The **sectional curvature** $K(X,Y) = \frac{\langle R(X,Y)X, Y\rangle}{|X\wedge Y|^2}$.
- The **Ricci curvature** $\operatorname{Ric}(x) = \operatorname{Ric}(x,x)$, where $\operatorname{Ric}(x,y)$ is the symmetric form of $\frac{1}{n}$ of trace of the map $z \to R(x,z)y$.
  Thus $\operatorname{Ric}_p(x) = \frac{1}{n-1}\sum\langle R(x,z_i)x, z_i\rangle$, for x a unit vector, where z_i is an orthonormal basis orthogonal to x.
- The **scalar curvature** $K(p) = 1/n\sum \operatorname{Ric}_p(z_i)$, where z_i is an orthonormal basis.

The curvatures only depends on the point(12.3.3.11). ⌟

Lemma (12.3.3.30).

$$\frac{D}{\partial t}\frac{D}{\partial s}V - \frac{D}{\partial s}\frac{D}{\partial t}V = R(\frac{\partial f}{\partial s}, \frac{\partial f}{\partial t})V.$$

⌟

Proof: Obvious because $\frac{\partial}{\partial_s}, \frac{\partial}{\partial_t}$ commutes.? □

Prop. (12.3.3.31) [Sectional Curvature Define Curvature]. The curvature tensor is determined by its sectional curvature.

In particular, if M is isotropic at a point p (The sectional curvature depends only on the point), then

$$R(X,Y,W,Z) = K_0(\langle X,W\rangle\langle Y,Z\rangle - \langle X,Z\rangle\langle Y,W\rangle).$$

⌟

Proof: Cf.[Do Carmo P95], should use the cyclicity of the first three terms. □

Prop. (12.3.3.32) [Bianchi Identities]. Recall the covariant differential $\nabla R(Y_i,Z) = Z(R(Y_i)) - \sum_i R(\nabla_Z Y_i, Y_j)$(12.3.3.5).

- (Bianchi Identity)$\sum_{(X,Y,Z)} R(X,Y)Z = 0$.
- (Second Bianchi Identity)$\sum_{(Z,W,T)} \nabla R(X,Y,Z,W,T) = 0$.

⌟

Proof: 1: Cf.[Do Carmo P91], should reduce to Jacobi identity.
2: □

Prop. (12.3.3.33)[Schur's Theorem]. Let M be a manifold of dimension $n \geq 3$, suppose the sectional curvature only depends on p, then M has constant curvature. ⌟

Proof: Use the second Bianchi Identity and geodesic frame and(12.3.3.31).Cf.[Do Carmo P106]. □

Def. (12.3.3.34)[Eisenstein Curvature]. A manifold M is called a **Eisenstein manifold** iff its Ricci curvature $\lambda(p)$ only depends on the point. Then

- If M is connected and Eisenstein of dimension≥ 3, then it has constant Ricci curvatures everywhere every direction.
- If M is connected and Eisenstein of dimension3, then it has constant sectional curvatures.

⌟

Proof: 1: Cf.[Do Carmo P108].
2: Now it has constant Ricci curvature, then

$$R_{1212} + R_{1313} = \lambda = R_{1212} + R_{2323} = R_{1313} + R_{2323}.$$

So we can solve these curvatures out. □

Prop. (12.3.3.35) [Riemannian Curvature Identities].

-
- $R(X,Y,Z,W) = R(Z,W,X,Y), \quad R(X,Y,Z,W) = R(X,Y,W,Z).$

⌟

Proof: Cf.[DO Carmo P91]. □

- $B(X,Y)=\overline{\nabla}_{\overline{X}}\overline{Y}-\nabla_X Y$. It is bilinear and symmetric.
- $H_\eta(x,y)=\langle B(x,y),\eta\rangle$. Thus $B(x,y)=\sum H_i(x,y)E_i$ for an orthonormal frame E_i in $\mathfrak{X}(U)^\perp$.
- $S_\eta(x)=-(\overline{\nabla}_x\eta)^T$. It satisfies:$\langle S_\eta(x),y\rangle=H_\eta(x,y)=\langle B(x,y),\eta\rangle$. It is self-adjoint. When codimension 1, it is the derivative of the Gauss mapping.
- (**Gauss Formula**): let x,y be orthonormal tangent vector. Then:
$$K(x,y)-\overline{K}(x,y)=\langle B(x,x),B(y,y)\rangle-|B(x,y)|^2.$$
- An immersion is called **geodesic** at p if the second fundamental form S_η is zero for all η, (which means $\nabla_X Y$ has no normal component). It is called **minimal** if the trace of S_η is zero.
- An immersion is called umbilic if there exists a normal unit field η s.t. $\langle B(X,Y),\eta\rangle(p)=\lambda(p)\langle X,Y\rangle$.
- If the ambient space has constant sectional curvature and the immersed manifold is totally umbilic, then λ is constant.
- mean curvature tensor of immersion $f=1/n\sum_i(\text{tr }S_i)E_i=1/n\text{ tr }B$. It is zero if f is minimal.
- normal connection $\nabla^\perp_X\eta=(\overline{\nabla}_X\eta)^N=\overline{\nabla}_X\eta+S_\eta(X)$.

Prop. (12.3.3.36).
- (Gauss equation)
$$\langle\overline{R}(X,Y)Z,T\rangle=\langle R(X,Y)Z,T\rangle-\langle B(Y,T),B(X,Z)\rangle+\langle B(X,T),B(Y,Z)\rangle.$$
- (Ricci equation)
$$\langle\overline{R}(X,Y)\eta,\zeta\rangle-\langle R^\perp(X,Y)\eta,\zeta\rangle=\langle[S_\eta,S_\zeta]X,Y\rangle.$$
- (Codazzo equation)
$$\langle\overline{R}(X,Y)Z,\eta\rangle=(\overline{\nabla}_Y B)(X,Z,\eta)-(\overline{\nabla}_X B)(Y,Z,\eta).\qquad\text{(Lie bracket)}$$

⌟

Parallel Transportations

Def. (12.3.3.37) [Parallel Transportation]. ⌟

Def. (12.3.3.38) [Holonomy Group]. The **holonomy group** $Hol_x(g)$ of a Riemannian manifold M w.r.t to the Levi-Civita connection is defined to be the subgroup of $O(T_x(M))$ induced by the parallel transportation along a loop. If M is connected, For different points, holonomy groups are conjugate, so holonomy group is defined up to conjugation. ⌟

Prop. (12.3.3.39) [Trivial Holonomy Group]. If M is a Riemannian manifold and the holonomy group is trivial, then for any $X,Y,Z\in X(M)$, $R(X,Y)Z=0$. ⌟

Proof: Cf.[Do Carmo P105]. □

Prop. (12.3.3.40) [Berger]. in fact, the groups that can be realized as a holonomy group of a simply connected complete Riemannian manifold can be classified. ⌟

Proof: Cf.[Complex geometry Daniel P214]. □

Def. (12.3.3.41). The **Geodesic flow** for a connection on TM is the flow on TM whose trajectories are $t \mapsto (\gamma(t), \gamma'(t))$, where γ is a geodesic on M. ⌟

Prop. (12.3.3.42) [The smoothness of geodesics]. For every point p, there exists a nbhd V and a C^∞ mapping

$$\gamma : (-\delta, \delta) \times V \times B(0, \epsilon) \to M,$$

s.t. $\gamma(t, q, v)$ is the geodesic passing through p with velocity v. ⌟

Prop. (12.3.3.43) [Curvature and Metric, Cartan]. Let $M, \widetilde{M}$ be two Riemannian manifold of dimension n and let $p \in M, \widetilde{p} \in \widetilde{M}$. Choose a linear isometry $i : T_p(M) \cong T_{\widetilde{p}}(\widetilde{M})$. Let V be a normal neighbourhood of p that $\exp_{\widetilde{p}}$ is defined on $i \circ \exp_p^{-1}(V)$. Define a mapping $f : V \to \widetilde{M}$ by $f(q) = \exp_{\widetilde{p}} \circ i \circ \exp_p^{-1}(q)$.

For any $q \in V$, there is a unique normalized geodesic $\gamma : [0, t] \to M$ that $\gamma(0) = p, \gamma(t) = q$. Denote by P_t the parallel transportation along γ, and the map $\varphi_t : T_q(M) \to T_{f(q)}(\widetilde{M})$ by $\varphi_t(v) = \widetilde{P}_t \circ i \circ P_t^{-1}(v)$.

If for all $q \in V$ and all $x, y, u, v \in T_q(M)$, we have

$$\langle R(x, y)u, v\rangle = \langle \widetilde{R}(\varphi_t(x), \varphi_t(y)\varphi_t(u), \varphi_t(v)\rangle,$$

then $f : V \to f(V) \subset \widetilde{M}$ is an isometry and $df_p = i$. ⌟

Proof: Cf.[Do Carmo P157]. Use Jacobi fields. The point is that the hypothesis implies that the map of a Jacobi field is also a Jacobi field. □

Cor. (12.3.3.44). Let $M, \widetilde{M}$ be Riemannian manifolds with the same dimension n in which parallel transportation preserves sectional curvature. Let $p \in M, \widetilde{p} \in \widetilde{M}$. If there is a linear isometry $i : T_p(M) \cong T_{\widetilde{p}}(\widetilde{M})$ s.t. $K(p, E) = K(\widetilde{p}, i(E))$ for any 2-dimensional subspace $E \subset T_p(M)$, then there exist nbhd V of p, nbhd $\widetilde{V}$ of $\widetilde{p}$ and an isometry $f : V \to \widetilde{V}$ that $df_p = i$. ⌟

Cor. (12.3.3.45). If in situation(12.3.3.44), M and $\widetilde{M}$ are moreover complete and simply connected, then there is a unique isometry $f : M \to \widetilde{M}$ s.t. $f(p) = \widetilde{p}$ and $df_p = i$. ⌟

Complete manifold

Prop. (12.3.3.46) [Hopf-Rinow theorem]. The following is equivalent definition of **completeness**.

1. $\exp_p$ is defined for all of $T_p(M)$ and all $p \in M$.
2. The closed and bounded sets of M are compact.
3. M is complete as a metric space.
4. M is $\sigma-$compact and if $q_n \notin K_n$, $d(p, q_n) \to \infty$.
5. The length of any divergent (compact escaping) curve is unbounded.

and if M is complete, then for any $p, q \in M$, there exists a minimizing geodesic between p, q. In particular, any compact submanifold of a complete manifold is complete. ⌟

Proof: Cf.[Do Carmo P147]. □

- For any two manifold of the same constant curvature and any two orthogonal basis, there is a local isometry (It is locally isotropic).

- Any complete manifold with a sectional curvature is like $\tilde{M}/\Gamma$, where $\tilde{M}$ is $\mathbf{H}^n, \mathbf{R}^n$ or $\mathbf{S}^n$.

Prop. (12.3.3.47) [Cartan]. in any nontrivial homotopy class in a compact manifold , there exists a closed geodesic. ⌟

Proof: □

4 Jacobi Field and Comparison Theorems

Def. (12.3.4.1) [Jacobi Field]. The **Jacobi field equation** along a normalized geodesic γ is defined to be

$$D^2 J(t) + R(\dot{\gamma(t)}, J(t))\dot{\gamma}(t) = 0.$$

It is defined by its initial condition $J(0)$ and $J^{'}(0)$. It can be used to detect the sectional curvature, the critical point of $\exp_p$ and calculate variation of energy. ⌟

Prop. (12.3.4.2) [Constant Curvature Case]. On a manifold with constant curvature K, the Jacobi field equation for a vector field J normal to γ is equivalent to

$$D^2 J(t) + KJ(t) = 0.$$

⌟

Proof: Use(12.3.3.31), we have

$$\langle R(\gamma', J)\gamma', T\rangle = K\{\langle\gamma',\gamma'\rangle\langle J, T\rangle - \langle\gamma', T\rangle\langle J,\gamma'\rangle\} = K\langle J, T\rangle$$

So $R(\gamma', J)\gamma' = KJ$. □

Prop. (12.3.4.3). The Jacobi field along a point with initial velocity 0 all has the form

$$J(t) = (d\exp_p)_{t\dot{\gamma}(0)}(tJ^{'}(0)).$$

⌟

Proof: Cf.[Do Carmo P113]. Should use uniqueness theorem of ODE. □

Cor. (12.3.4.4) [Conjugate Points]. If two points p, q are connected by a geodesic γ, and $q = \exp_p(v_0)$, then p, q are called **conjugate** along γ, if there is a non-trivial Jacobi field on γ that $J(p) = J(q) = 0$.

Then q is conjugate to p iff v_0 is the critical point of $\exp_p$, and the multiplicity of conjugacy is equal to the kernel of $(\exp_p)_{v_0}$. ⌟

Prop. (12.3.4.5). For a Jacobi field J along γ, $\langle J(t), \gamma'(t)\rangle$ is linear in t. ⌟

Proof: Take second derivatives. □

- If J is a Jacobi field $J(t) = (d\exp_p)_{tv}(tw)$, $|v| = |w| = 1$, then

$$|J(t)| = t - \frac{1}{6}K_p(v, w)t^3 + o(t^3).$$

Prop. (12.3.4.6). There are no conjugate points on a Riemannian manifold of non-positive curvature. ⌟

Proof: Cf.[Do Carmo P119]. □

Prop. (12.3.4.7) [Killing Field is everywhere Jacobi]. A Killing field is a Jacobi field along geodesics.

And if $X(p) = 0$, then X is tangent to the geodesic sphere near p, because X preserves length. ⌟

Proof: □

Energy Analysis

Def. (12.3.4.8) [Energy]. The **energy** of a geodesic $\gamma : [0, a] \to M$ is defined to be

$$E(s) = \int_0^a |\frac{\partial}{\partial t}\gamma(s,t)|^2 dt.$$

⌟

Prop. (12.3.4.9). A minimizing geodesic must minimize energy. ⌟

Proof: □

- (**First Variation of Energy**)

$$1/2E^{'}(0) = -\int_0^a \langle V(t), D\dot{c}(t)\rangle dt + \langle V(a), \dot{c}(a)\rangle - \langle V(0), \dot{c}(0)\rangle.$$

A piecewise differentiable curve is a geodesic iff every proper variation has first derivative 0.

- (**Second Variation of Energy**) If γ is a geodesic,

$$1/2E^{''}(0) = \int_0^a \{\langle DV(t), DV(t)\rangle - \langle R(\dot{\gamma}, V)\dot{\gamma}, V\rangle\}dt + \langle D_s V(a), \dot{\gamma}(a)\rangle - \langle D_s V(0), \dot{\gamma}(0)\rangle.$$

- a variation is equivalent to a vector field along the curve, and a variation that $f_s(t)$ are all piecewise geodesics corresponds to a piecewise Jacobi field(Choose a normal partition).

Prop. (12.3.4.10) [Rauch Comparison theorem]. Let M and $\tilde{M}$ be manifolds, dim$\tilde{M} \geq$ dim M. If J and $\tilde{J}$ be two normal Jacobi fields along geodesics γ and $\tilde{\gamma}$ that $|J(0)| = |J'(0)| = 0$ and $|J^{'}(0)| = |\tilde{J}^{'}(0)|$. If $\tilde{\gamma}$ has no conjugate point or focal point free and $\tilde{K}(\tilde{x}, \dot{\tilde{\gamma}}(t)) \geq K(x, \dot{\gamma})$ for any vector $x, \tilde{x}$, then $|\tilde{J}| \leq |J|$. ⌟

Cor. (12.3.4.11) [Injectivity Radius Estimate]. If the sectional curvature of M satisfies: $0 < L \leq K \leq H$, then the distance between any two conjugate points satisfies: $\frac{\pi}{\sqrt{H}} \leq d \leq \frac{\pi}{\sqrt{L}}$. ⌟

Prop. (12.3.4.12). If two manifold M and $M^{'}$ satisfy $K \leq K^{'}$, then in a normal nbhd of a point p in M and a nbhd of $p^{'}$ that exp is nonsingular, the transformation of a curve c shortens length.

Note that this is not Toponogov thoerem, because if you try to map from a large curvature manifold to a small curvature, then you cannot guarantee that the mapped curve is the shortest. ⌟

Cor. (12.3.4.13). In a complete simply connected manifold of non-positive curvature,

$$A^2 + B^2 - 2AB\cos\gamma \leq C^2$$

thus $\alpha + \beta + \gamma \leq \pi$. ⌟

Prop. (12.3.4.14) [Moore theorem]. Let $\overline{M}$ be a complete simply connected manifold of sectinoal curvature $\overline{K} \leq -b \leq 0$, M a compact manifold of sectional curvature satisfying $K - \overline{K} \leq b$. If dim$\overline{M}$ < dim$M$, M cannot be immersed into $\overline{M}$.(use Hadamard theorem to choose the furthest geodesic and calculate the second variation of energy and use Gauss formula). ⌟

Cor. (12.3.4.15). Let $\overline{M}$ be a complete simply connected manifold of sectinoal curvature $\overline{K} \leq 0$, M a compact manifold of sectional curvature satisfying $K \leq \overline{K}$. If dim$\overline{M}$ < dim$M$, M cannot immerse into $\overline{M}$. ⌟

Lemma (12.3.4.16) [Klingenberg Lemma]. Let M be a complete manifold of sectional curvature $K \geq K_0$, let γ_0, γ_1 be two homotopic geodesics from p to q, then there exists a middle curve γ_s s.t.

$$l(\gamma_0) + l(\gamma_s) \geq \frac{2\pi}{\sqrt{K_0}}.$$

⌟

Proof: Assume $l(\gamma_0) < \frac{2\pi}{\sqrt{K_0}}$, otherwise we are done. Then by Rauch comparison(12.3.4.10), the $\exp_p : T_pM \to M$ has no critical point in the open ball B of radius $\pi/\sqrt{K_0}$. Now we want to lift γ_s to T_pM. It is clear that we cannot lift γ_1, because otherwise it is not a curve. Hence for every $\varepsilon > 0$, there is a curve $\alpha_{t(\varepsilon)}$ that can be lifted and has a point with distance smaller than ε to the boundary ∂B, otherwise the s that can be lifted will be open and closed in $[0,1]$, thus containing 1.

So now if we choose a sequence of lifts curves γ_s converging to the boundary, then s has a convergent point, then we have $l(\gamma_0) + l(\gamma_{t_0}) \geq \frac{\pi}{\sqrt{K_0}}$. □

Prop. (12.3.4.17)[Klingenberg]. Let M be a simply connected compact manifold of dimension $n \geq 3$ such that $\frac{1}{4} < K \leq 1$, then $i(M)$(The infimum of distance to the cut locus)$\geq \pi$. ⌟

Cor. (12.3.4.18). If M is a compact orientable manifold of even dimension satisfying $0 < K \leq 1$, then $i(M) \geq \pi$. ⌟

Prop. (12.3.4.19) [1/4-pinch Sphere Theorem]. Let M be a compact simply connected manifold satisfying $0 < 1/4K_{\max} < K \leq K_{\max}$, then M is homeomorphic to a sphere.

(Use Klingenberg Theorem, this is a special case of diameter geodesic sphere theorem). Cf.(12.3.4.29).

It can be shown that in this case, this sphere is even diffeomorphic to S^n using Ricci flow. ⌟

Remark (12.3.4.20). $0 < 1/4K_{\max} < K$ cannot be changed to $\geq$. In fact, the Funibi-Study metric on CP^n has sectional curvature $1 \geq K \geq 4$. Cf. **??** ⌟

Hess$\rho(X,Y)$ where ρ is the distance to a fixed point, is important.

Prop. (12.3.4.21). Hess$\rho(X,Y)$ is positive definite on the tangent space of the geodesic sphere within the injective radius, and its principal value is $|\frac{J'}{J}|$ for a Jacobi field in that direction. And it is zero on the normal direction.

So there would be a Riccati comparison theorem on the eigenvalue of $\Pi_2 : \lambda' \leq -K - \lambda^2$,Hess$(\rho)$ is bounded. ⌟

Proof: Notice that

$$\text{Hess}\rho(X,Y) = (\nabla_X \text{grad}\rho, Y) = XY\rho - (\nabla_X Y)\rho$$

so if choose a normal geodesic γ of initial vector X, then

$$\text{Hess}\rho(X,X) = X\langle\dot{\gamma}, d\rho\rangle - (\nabla_X\dot{\gamma})\rho = X\langle\dot{\gamma}, d\rho\rangle = \langle\dot{\gamma}, d\langle\dot{\gamma}, d\rho\rangle\rangle = E''(0)$$
$$= I_q(X,X) = ((\nabla_{\dot{\gamma}}X)(q), X(q)) = \frac{\langle J', J\rangle}{|J|^2}$$

□

Prop. (12.3.4.22) [Toponogov]. Let$M$ be a complete manifold with $K \geq H$.

If a hinge satisfies γ_1 is minimal and $\gamma_2 \geq \frac{\pi}{\sqrt{H}}$ if $H > 0$., then on M^H the same hinge has smaller distance of endpoints than this hinge ⌟

Proof: Cf.[Cheeger Comparison Theorems in Riemannian Geometry P42]. And there is another triangle version: For a minimal geodesic triangle, the comparison triangle has smaller angles. NOTE this theorem cannot be derived from Rauch Comparison Theorem. □

Critical Point for Distance Function

Prop. (12.3.4.23). The critical point for distance function on a complete manifold is that for every direction v, there is a minimal geodesic γ s.t. $\langle\gamma'(l), v\rangle \leq \frac{\pi}{2}$.

The set of regular point is open and there exists a smooth gradient like vector field (i.e. acute angle with every minimal geodesic) on this open subset . ⌟

Prop. (12.3.4.24) [Berger's Lemma]. A maximal point for the distance function is a critical point. ⌟

Proof: If not, choose a convergent point v of the minimal geodesics with endpoint in a curve of that direction, then exp near v will generate a Jacobi field with endpoint Jacobi is the sam of that direction. So the distance will increase by $\cos\theta$ along that direction, contradiction. □

Prop. (12.3.4.25) [Soul Lemma]. Let M is a Riemannian manifold and A is a closed submanifold. If $dist(A, -)$ has no critical point on $D(A, R)\backslash A$, then $B(A, R)$ is diffeomorphic to the normal bundle of $A \to M$. ⌟

Proof: A has a normal exp radius ϵ, and we can vary the gradient-like vector field to be identical to the normal vector near A, and use Morse lemma (the flow) to get a diffeomorphism. □

Cor. (12.3.4.26) [Disk Theorem]. If A is a point then M is diffeomorphic to a disk. ⌟

Lemma (12.3.4.27) [Generalized Schoenflies Theorem]. Easy to do, just use the fact that exp is continuous to find a boundary sphere depending continuously on the direction (both p and q). ⌟

Prop. (12.3.4.28) [Sphere Theorem]. If M is a closed manifold and has a distance function with only one critical point (the furthest one), then M is homeomorphic to a twisted ball. ⌟

Proof: There exists a ϵ and r that $B(q, \epsilon)$ and $B(p, r)$ covering M, (Use the convergent point argument). Then use the generalized Schoenflies theorem. □

Prop. (12.3.4.29) [Diameter Sphere Theorem]. If a closed manifold M satisfies sec $M \geq K > 0$, and diam$(M) > \frac{\pi}{2\sqrt{K}}$, then M is homeomorphic to S^n. ⌟

Proof: First, if there are two maximal distance point, then use Toponogov to show contradiction. Second, at other points x,

$$\angle pxq > \frac{\pi}{2}$$

(Regular domain) because of Toponogov and The formula

$$\cos\tilde{\alpha} = \frac{\cos l - \cos l_1 \cos l_2}{\sin l_1 \sin l_2}.$$

So the geodesic direction $\overrightarrow{xq}$ will serve as a geodesic-like vector field (might need paracompactness). □

Prop. (12.3.4.30) [Critical Principle]. In a complete manifold M of sectional curvature $> K$, if q is a critical point of p, then for any point x with $d(p, x) > d(p, q)$ and any minimal geodesic from p to x, the $\angle xpq$ is smaller than the $\cosh_K^{-1}(\frac{d(p,x)}{d(p,q)})$. ⌟

Proof: Use Toponogov for the hinge xpq. Then notice that there is a different minimal geodesic from $p \to q$ that makes the $\angle pqx < \pi/2$ by the definition of critical point, thus there is another Toponogov inequality, this two inequality contradicts. □

Cor. (12.3.4.31). For a complete open manifold whose K are lower bounded, then it is homeomorphic to the interior of a manifold with boundary. (Use Soul lemma, otherwise there will be a sequence of critical point whose angles are big). ⌟

Prop. (12.3.4.32). ray construction and Line construction? ⌟

Prop. (12.3.4.33) [Soul Theorem]. If M is an open manifold with $K \geq 0$, then there is a totally geodesic submanifold S that M is diffeomorphic to the normal bundle over S. ⌟

Proof: Use the ray construction to get a totally convex compact subset, hence it is a manifold or with boundary , if it has boundary, then find to set of maximal distance to the distance to boundary, the distance to the boundary is a convex function, so it is a smaller totally geodesic manifold. So a S without boundary must exist and this constitutes a stratification, all the level set is strongly convex. Thus all point outside S is not critical, hence the soul lemma applies. Cf.[GeJian Comparison theorems in Riemannian Geometry Lecture7]. □

Prop. (12.3.4.34) [Perelman]. There is a distance non-increasing contraction unto the soul, and it must be just the projection along the normal bundle. Moreover, for any geodesic on the soul and a parallel vector field in the normal bundle along it, it spans a flat surface (by Rauch comparison). ⌟

Cor. (12.3.4.35) [Soul Conjecture]. For an open(non-compact) complete manifold M with $K \geq 0$, if it has a point p s.t. sectional curvature at p are all positive, then M is diffeomorphic to R^n. (It's enough to show that its soul is a point, otherwise for any point, it must has a direction that is flat, $K = 0$). ⌟

5 Curvature Inequalities and Topology

Sectional Curvature

Prop. (12.3.5.1) [Hadamard theorem]. M a complete simply connected Riemann manifold of sectional curvature ≤ 0, then $\exp_p : T_pM \to M$ is an isomorphism of M to $\mathbb{R}^n$.(negative sectional curvature to show exp is a local isomorphism, complete to show it is a covering map) ⌟

Prop. (12.3.5.2) [Liouville Theorem]. Any conformal mapping for an open subset of $\mathbb{R}^n, n > 2$ is restriction of a composition of isometry, dilations and/or inversions, at most once. ⌟

Prop. (12.3.5.3) [Positive Curved, Closed Geodesic not Minimal]. If M is an even dimensional orientable Riemannian manifold with positive sectional curvature, let $\sigma : [0, 1] \to M$ be a closed geodesic curve, then there exists an $\varepsilon > 0$ that parametrized closed curves $F; [0, 1] \times (-\varepsilon, \varepsilon) \to M$ near σ with lengths less than that of σ. ⌟

Proof: Cf.[Solution to Yau Test Geometry Individual2013 Prob5]. □

Prop. (12.3.5.4) [Synge]. f is an isometry of a compact oriented manifold M^n of positive sectional curvature, f alter orientation by $(-1)^n$, then f has a fixed pt. ⌟

Proof: Cf.[Do Carmo P203]. □

Cor. (12.3.5.5). M a compact manifold of positive sectional curvature, then

1. If M is orientable and n is even, then M is simply connected. So If M is compact and even dimension, then $\pi(M) = 1$ or $\mathbb{Z}_2$.

2. If n is odd, then M is orientable.

(Use the universal cover and covering transformation.) ⌟

Conj. (12.3.5.6) [Hopf Conjecture]. If M is a compact Riemannian manifold of even dimension that $K > 0$, then it has positive Euler characteristic. ⌟

Morse Index

Prop. (12.3.5.7) [Index Lemma]. Among the piecewise differentiable vector fields along a geodesic without conjugate point or without focal point, with initial value 0 and fixed end value, the Jacobi field attain minimum of the index form:

$$I_a(V,V) = \int_0^a \{\langle DV(t), DV(t)\rangle - \langle R(\dot{\gamma}, V)\dot{\gamma}, V\rangle\} dt.$$

⌟

Cor. (12.3.5.8). $I_l(J,J) = \langle J, J'\rangle(l)$ for a Jacobi field. ⌟

Prop. (12.3.5.9). a focal point is a critical value of $exp^{\perp}$. For an embedded manifold, the focal point equals $x + 1/t\eta$, where η is a vertical vector and t is a principal value of $S_e ta$. ⌟

Prop. (12.3.5.10) [Morse Index theorem]. The index of the the index form $I_a(V,W)$ on the space of vector fields 0 at the endpoints, equal to the number of points conjugate to $\gamma(0)$ in $[0,a)$. ⌟

Cor. (12.3.5.11). If γ is minimizing, γ has no conjugate points on $(0,a)$, γ has a conjugate point, it is not minimizing. ⌟

Prop. (12.3.5.12) [Morse]. If M is complete with non-negative sectional curvature, then $\pi_1(M)$ have no finite non-trivial cyclic group and $\pi_k(M) = 0$. ⌟

Proof: because universal cover of M is contractible, so the higher homotopy group vanish and $H^k(M) = H^k(\pi_1(M))$, so if a subgroup is finite cyclic, its homology is periodic, contradiction. □

Prop. (12.3.5.13) [Preissman]. For a compact manifold with $K < 0$, any nontrivial abelian subgroup of π_1 is infinite cyclic. ⌟

Prop. (12.3.5.14). If M is compact and $K < 0$, $\pi_1(M)$ is not abelian. ⌟

Assuming M complete,

- The cut point of p along γ is the maximum $\gamma(t)$ s.t. $d(p, \gamma(t)) = t$. It is either the first conjugate point of p or the intersection of two minimizing geodesics.
- Conversely, if a point is a conjugate point of p or is intersection of two geodesics of equal length, then there is a cut point before it. So, if intersection of two minimizing geodesics happens, it must happen before the occurrence of conjugate point.
- thus the cut point relation is reflexive, and if $q \in M \setminus C_m(p)$, then there exists a unique minimizing geodesic joining p and q.
- $M \setminus C_m(p)$ is homeomorphic to an open ball through exp.
- the distance of p to the cut locus is continuous, thus $C_m(p)$ is closed.
- If M is complete and there is a p which has a cut point for every geodesic, then M is compact.

- for q the closest of $C_m(p)$ to p, either there exists a minimizing geodesic and q is conjugate to p or there is to minimizing geodesic connecting at q.

Prop. (12.3.5.15). The index of a geodesic will decrease when transferred to a manifold of smaller sectional curvature K. ⌟

Prop. (12.3.5.16). In a complete manifold, if there is a sequence of points $\{p_i\}$ converging to a point p, choose for each point a minimal geodesic, then a subsequence of them will converge to a minimal geodesic to p. ⌟

Proof: The convergence is by smoothness and of exp and Hadamard. The minimality is by comparing distance. □

Ricci Curvature

Prop. (12.3.5.17)[Ricci Comparison]. Volume comparison, Laplacian Comparison, Mean Curvature comparison. Cf.[葛健 Week13]. ⌟

Prop. (12.3.5.18) [Bishop-Gromov]. Let M be an open manifold with $\mathrm{Ric} \geq H$, let $\tilde{M}(H)$ be a complete simply connected manifold of constant sectional curvature H, then

$$\mathrm{Vol}(B_r(x)) \leq \mathrm{Vol}(B_r(\tilde{p})), \quad \frac{\mathrm{Vol}(B_R(x))}{\mathrm{Vol}(B_r(x))} \leq \frac{\mathrm{Vol}(B_R(\tilde{p}))}{\mathrm{Vol}(B_r(\tilde{p}))}.$$

Cf.[葛健 Week13]. ⌟

Prop. (12.3.5.19)[Bonnet-Myer]. M a complete manifold of Ricci curvature $\mathrm{Ric}_p(v) \geq \frac{1}{r^2}$, Then M is compact and have diameter $\leq \pi r$.

And if the identity is achieved, $M \cong \mathbb{S}^n$. ⌟

Proof: Use Laplacian comparison $\Delta r \leq (n-1)\cot r$. Cf.[葛健 week13]. □

Cor. (12.3.5.20)[Positive Ricci Finite Fundamental Groups]. M is a complete manifold of Ricci curvature $\geq \delta > 0$, then the universal cover is compact thus $\pi_1(M)$ is finite. This can be seen as an obstruction for a compact manifold to have positive Ricci curvature. ⌟

Cor. (12.3.5.21)[Calabi-Yau]. For an open manifold with non-negative Ricci curvature, for any point, $\mathrm{Vol}(B(p,r)) \geq c_p r$. ⌟

Prop. (12.3.5.22)[Milnor]. Let M be an open manifold of non-negative Ricci curvature of dimension n, then any f.g. subgroup of $\pi_1(M)$ has polynomial growth $\leq n$. Milnor conjectured that $\pi_1(M)$ in fact is f.g.. ⌟

Prop. (12.3.5.23) [First Betti Number Theorem]. There is a number $f(n,\lambda,D)$, $f(n,0,D) = n, f(n,\lambda,D) = 0$ for $\lambda > 0$ that for a manifold of diameter $\leq D$ and Ricci curvature $\geq \lambda$, $b_1(M) \leq f(n,\lambda,D)$. ⌟

Cor. (12.3.5.24)[Splitting Theorem]. The universal cover of a compact RIemannian manifold with non-negative Ricci curvature splits isometrically as a product $\widetilde{M} = N \times \mathbb{R}^k$ where N is a compact manifold manifold. ⌟

Scalar Curvature

12.4 Low Dimensional Topology

1 Floer Homology

Def. (12.4.1.1)[Witten Complex]. Let $M \in \mathcal{D}\mathrm{iff}_{\mathrm{cpct}}$ and $f \in C(M)$ is a Morse function, then at each critical point P of f, the Hessian $H_P(f)$ is a non-degenerate quadratic form with signature n_P^+, n_P^-. We define the **Witten complex** C as follows:

- For $0 \leq q \leq \dim M, C_q$ is the free group generated by the critical points with $n_P^- = q$.
- Choose a metric on M, define the flow generated by $\mathrm{grad}\, f$. Then for critical points P, Q with $n_P^- = q, n_Q^- = q-1$, the number of trajectories under $\mathrm{grad}\, f$ from P to Q is finite, and this gives the boundary map coefficients $\partial_{P,Q}$.

⌟

References are [Supersymmetry and Morse Theory, Witten].

Casson Invariants

Def. (12.4.1.2) [Casson Invariants]. Let Y be a homological 3-sphere, the **Casson invariant** $\lambda(Y)$ of Y is defined to be the half of the number of isomorphism classes of irreducible representation $\pi_1(Y) \to SU(2)$. ⌟

Prop. (12.4.1.3). For a homological 3-sphere Y, let

- $\mathcal{A}$ be the space of $SU(2)$-connections for the trivial bundle on Y,
- $\mathcal{G}$ be the group of gauge transformations $Y \to SU(2)$.
- $\mathcal{C} = \mathcal{A}/\mathcal{G}$.

Then $\mathcal{C}$ is an infinite-dimensional manifold, and the connection map $F : A \mapsto F_A$ defines a 1-form F on $\mathcal{C}$. ⌟

Proof: □

Prop. (12.4.1.4) [Taubes]. Situation as in(12.4.1.3), the zeros of F, i.e. the set of flat connections, corresponds to irreducible representations $\pi_1(Y) \to SU(2)$. And we can use Fredholm perturbation to calculate the number, i.e. $2\lambda(Y)$. ⌟

Proof: ? □

Floer Homology Groups

Remark (12.4.1.5) [Relative Morse Indices]. The difficulty to construct Morse theory for Y lies in the fact that the Hessian of $f : \mathcal{C} \to \mathbb{R}/\mathbb{Z}$ at critical points has both Morse indices n^+, n^- infinite. The way around is to notice for critical points P, Q, the **relative Morse index** $n_{P,Q}^- = n_P^- - n_Q^-$ is finite. ⌟

Prop. (12.4.1.6)[Floer Homology Theory]. Using the flow generated by $\mathrm{grad}\, f$, we can get construct a chain complex with (mod 8)-grading, which is a finite complex with the critical points of f as simplexes. The corresponding homology groups are called the **Floer homology** of Y, denoted by $HF_q(Y)$, where $q \in \mathbb{Z}/(8)$.

Notice reversing the orientation of Y induces an action on $HF_*(Y)$ corresponding to Poincaré duality. ⌟

Prop. (12.4.1.7) [Floer Homologies and Casson Invariants]. It is clear now that $2\lambda(M) = \sum_{q=0}^{7} \dim HF(Y)$. Thus the Floer homology groups form a refinement of $\lambda(Z)$. ⌟

2 Gauge Theory

3 Donaldson-Floer Theory

Main references are [Geometry of 4-Manifolds, Donaldson, ICM1987].

Prop. (12.4.3.1) [Hodge]. For an algebraic surface $S/\mathbb{C}$, the signature b_2^+ of the intersection form on $H_2(S(\mathbb{C}))$ satisfies

$$b_2^+ = 1 + 2p_g(S).$$

⌟

Def. (12.4.3.2) [Donaldson Invariants]. Let Z be an oriented simply-connected differentiable 4-manifold, let b_2^+, b_2^- be the signature of the intersection form on $H_2(Z)$. Assume $b_2^+ > 1$ is odd, the **Donaldson invariants** are a sequence of integral polynomials φ_k on $H_2(Z)$ for k sufficiently large, and $\deg(\varphi_k) = 4k = 3\frac{b_2^+ + 1}{2}$.? ⌟

Thm. (12.4.3.3). If $Z = Z_1 \# Z_2$ is a connected sum with $b_2^+(Z_i) \neq 0$, then $\varphi_k(Z) = 0$ for all k. ⌟

Proof: □

Thm. (12.4.3.4). If Z is an algebraic surface, then for k sufficiently large, $\varphi_K(Z(\mathbb{C})) \neq 0$. In particular, Z is essentially indecomposable. ⌟

Proof: □

Prop. (12.4.3.5) [Λ-Splitting]. Suppose the intersection form on $H_2(Z)$ decomposes as $H_2(Z) = A_1 \oplus A_2$, where $A_i^+ > 0$. If $\varphi_k(Z) \neq 0$ for some k, then by(12.4.3.3), Z cannot be decomposed to a connected sum $Z_1 \# Z_2$ having intersection form A_i. However, there exists such a decomposition $Z = Z_1 \coprod_Y Z_2$ where Y is a homotopy 3-sphere. ⌟

Proof: Cf.[Freeman and Taylor, Λ-Splitting 4-Manifolds]. □

Prop. (12.4.3.6). For a Λ-splitting $Z = Z_1 \coprod_Y Z_2$, the Donaldson invariant polynomials are related to the Floer homology groups of Y.? ⌟

12.5 Differential Forms in Algebraic Topology(Bott-Tu)

This section is dedicated to the analysis of algebraic geometry, using the tool of differential forms. Basic references are [Differential Forms in Algebraic Geometry Bott-Tu].

1 Basics

Prop. (12.5.1.1)[Cohomological Generator of Sphere]. Let $v : x \mapsto x/|x|$ be the outward-pointing vector field on $\mathbb{R}^n - \{0\}$, then the differential form

$$\iota(v)(dm) = \frac{1}{|x|} \sum x_i(-1)^{i-1} dx_1 \wedge dx_2 \wedge \ldots \widehat{dx_i} \wedge \ldots dx_n$$

restricts to a differential form on S^{n-1} that is a generator of $H^{n-1}(S^{n-1})$. ⌟

Proof: First we calculate $d(\iota(v)(dm)) = \operatorname{div}(v) dm = \frac{n-1}{|r|} dm$(12.3.3.27). Consider using Stoke's formula:

$$\int_{\partial B_1} \iota(v)(dm) - \int_{\partial B_\varepsilon} \iota(v)(dm) = \int_{B(0,1)-B(0,\varepsilon)} \frac{n-1}{|r|} dm = 0$$

Leting $\varepsilon \to 0$, $\int_{\partial B_\varepsilon} \iota(v)(dm)$ converges to 0 as $|\iota(v)(dm)|$ is bounded and $V(B_\varepsilon)$ converges to 0. And using the polar coordinate $dm = r^{n-1} dr d\omega$, the right hand side is just

$$\int_{S^{n-1}} \int_0^1 (n-1) r^{n-2} dr d\omega = V(S^{n-1}).$$

□

Prop. (12.5.1.2) [Degree Formula]. If $f : X \to Y$ is an arbitrary map of two compact oriented manifolds of dimension k, then for any k-form ω on Y,

$$\int_X f^*\omega = \deg(f) \int_Y \omega.$$

⌟

Proof: deg is defined in(12.1.4.16). Cf.[Pollack P188]**?**. □

Prop. (12.5.1.3) [Hopf Invariant]. Let $n > 1$, given a map $S^{2n-1} \to S^n$, let α be a generator of $H^n)S^n$, then $f^*\alpha = d\omega$ on S^{2n-1} for some ω. Define the **Hopf invariant** of f to be $H(f) = \int_{S^{2n-1}} \omega \wedge d\omega$, then:

- The definition of Hopf invariant is independent of ω chosen.
- For odd n, the Hopf invariant is 0.
- Homotopic maps f, g have the same Hopf invariant.

⌟

Proof: 1: If $d\omega = d\omega'$, then

$$\int_{S^{2n-1}} \omega' \wedge d\omega' - \int_{S^{2n-1}} \omega \wedge d\omega = \int_{S^{2n-1}} (\omega' - \omega) \wedge d\omega = \pm \int_{S^{2n-1}} d((\omega - \omega') \wedge \omega) = 0.$$

2: If n is odd, then ω is of even dimensional, thus $\omega \wedge d\omega = \frac{1}{2} d(\omega \wedge \omega)$, so $H(f) = 0$ by Stokes.

3: If $F : S^{2n-1} \times I \to S^n$ is a homotopy of f, g, then $F^*\alpha = d\omega$ for some ω on $S^{2n-1} \times I$. Thus consider

$$H(f) - H(g) = \int_{S^{2n-1}} \omega_1 \wedge d\omega_1 - \int_{S^{2n-1}} \omega_0 \wedge d\omega_0 = \int_{\partial(S^{2n-1} \times I)} \omega \wedge d\omega = \int_{S^{2n-1} \times I} d\omega \wedge d\omega,$$

But $d\omega \wedge d\omega = F^*(\alpha \wedge \alpha)$, and $\alpha \wedge \alpha = 0$. □

12.6 Symplectic Geometry

Cf.[Methods in Classical Mechanics Arnold Chapter8],[辛几何讲义范辉军].

1 Basics

Symplectic Forms

Def. (12.6.1.1). A **symplectic form** ω is a closed 2-form that is non-degenerate on any point. A smooth manifold with a symplectic form is called a **symplectic manifold**. A symplectic manifold must be even dimensional and orientable. ⌟

Prop. (12.6.1.2). A hamiltonian phase flow preserves the symplectic form. $g^{t*}\omega = \omega$. ⌟

Proof: by Cartan's magic formula,

$$\frac{d}{dt}(g^t)^*\omega = L_X\omega = \iota_X(d\omega) + d(\iota_X\omega) = d(\iota_X\omega)$$

because ω is closed. And by definition, $d(\iota_X\omega)(\eta) = \omega(J\mathrm{d}H, \eta) = \langle dH, \eta\rangle$, so $d(\iota_X\omega) = dH$, Thus the theorem. □

For the following Cf.[辛几何讲义范辉军 lecture3].

Prop. (12.6.1.3) [Moser's Stability]. If ω_t is a smooth family of cohomologous forms on a closed manifold M, then there exists an isotopy Ψ_t s.t.

$$\Psi_t^*(\omega_t) = \omega_0.$$

⌟

Prop. (12.6.1.4) [Relative Moser Stability]. If M is a closed manifold and S is a compact submanifold, then if two closed 2-form equals on S, then there is an open neighborhood N_0, N_1 of S and a diffeomorphism $\Psi : N_0 \to N_1$ that

$$\Psi|S = \mathrm{id},\ \Psi^*\omega_1 = \omega_0.$$

⌟

Cor. (12.6.1.5) [Darboux's Theorem]. Every symplectic form ω on M is locally diffeomorphic to the standard form ω_0 on $\mathbb{R}^{2n}$. ⌟

Proof: Choose $S = \mathrm{pt}$ and uses relative Moser stability. □

Prop. (12.6.1.6). For a compact symplectic manifold M, its even dimensional cohomology groups doesn't vanish, because ω^k are nontrivial. ⌟

Proof: This is because ω^n is a volume form on M that never vanish, so it gives M an orientation and $\int_M \omega^n \neq 0$. If ω^k is exact, then ω^n is exact, so $\int_M \omega^n = 0$ by Stokes', contradiction. □

12.7 Other Geometries

1 Hyperbolic Geometry

Prop. (12.7.1.1). Isometries of hyperbolic ball are all given by Mobius transformations, because the distance to three non-colinear point can localize a point. Cf.[双曲几何 刘毅]. ⌟

Def. (12.7.1.2) [Hyperbolic Disk]. The **hyperbolic disk** is a Riemannian manifold homeomorphic to $\mathbb{D}$ endowed with the **Poincaré metric** or **hyperbolic metric**

$$\mathrm{d}^P s=\frac{|\mathrm{d}z|}{1-|z|^2}=\sigma_{\mathbb{D}}(z)|\mathrm{d}z|.$$

⌟

Prop. (12.7.1.3). The Poincaré metric on $\mathbb{D}$ is preserved by $\mathrm{Aut}(\mathbb{D})$. ⌟

Proof: Cf.[李忠, P26]. □

Prop. (12.7.1.4). For any $z_1, z_2\in\mathbb{D}$,

$$d^P(z_1,z_2)=\log\frac{|1-\overline{z}_1z_2|+|z_1-z_2|}{|1-\overline{z}_1z_2|-|z_1-z_2|}.$$

⌟

Proof: Cf.[李忠, P27]. □

2 Metric Geometry

Def. (12.7.2.1) [Hausdorff dimension]. $\dim^H(X)$. ⌟

Def. (12.7.2.2). The **Hausdorff distance** for two subset $Y_1,Y_2\in X$ is the

$$d^H_X(Y_1,Y_2)=\inf\{\varepsilon|Y_2\subset B(Y_1,\varepsilon),Y_1\subset B(Y_2,\varepsilon)\}.$$

The **Gromov-Hausdorff metric** for two metric space is

$$d^{GH}(X_1,X_2)=\inf\{d^H_Z(i_1(X_1),i_2(X_2))\}$$

where i_1,i_2 are isometry of X_1,X_2 into a metric space Z.

This metric makes the set of all compact metric space into a complete Hausdorff space $\mathcal{MET}$. ⌟

Def. (12.7.2.3). A map from X to Y is called a ε**-approximation** iff $B(f(X),\varepsilon)=Y$ and $|d(x,y)-d(f(x),f(y))|\leq\varepsilon$.

We have: if there is a ε approximation, then $d^{GH}(X,Y)\leq 3\varepsilon$, and if $d^{GH}(X,Y)\leq\varepsilon$, there is a 3ε approximation. ⌟

Prop. (12.7.2.4). Fix a function $N:(0,1)\to\mathbb{N}$, the space $\mathcal{MET}(D,N)$ of complete metric space of diameter bounded by D and for every ε, there is a ε-net with no more then $N(\varepsilon)$ points. Then it is a compact subspace of $\mathcal{MET}$. ⌟

Proof: We show it is totally bounded and closed. It is totally bounded because the space of discrete space of no more than $N(\varepsilon)$ is compact and it ε approximate $\mathcal{MET}(D,N)$ by definition. Thus we have it is totally bounded. And □

Prop. (12.7.2.5)[Gromov Compactness Theorem]. Denote the space $\mathcal{RIC}^D_{*,-1}(n)$ of manifold with Ricci curvature bounded below by -1 and diameter bounded above by D, then it is a precompact subset of $\mathcal{MET}$. ⌟

Proof: By Bishop-Gromov(12.3.5.18), there is a $N(\varepsilon)$ that M can only have $N(\varepsilon)$ many balls of radius ε, because M has bounded diameter (Packing argument). So $\mathcal{RIC}^D_{*,-1}(n)\subset\mathcal{MET}(D,2N)$ is precompact. □

Prop. (12.7.2.6). Any metric space X in the closure of $\mathcal{RIC}^D_{*,-1}(n)$ has Hausdorff dimension $\dim^H(X)\leq n$. ⌟

Prop. (12.7.2.7)[Gromov]. If a sequence of manifold $\{M_i\}$ in $\mathcal{M}^{D,k}_{V,-k}(n)$, then they has a limit point $X\in\mathcal{MET}$. Then X is a C^∞ manifold and there is a $C^{1,\alpha}$-metric for every $\alpha<1$. And M_i are all diffeomorphic to X for large X.

In particular, this implies that there are only finitely many diffeomorphic classes. ⌟

Prop. (12.7.2.8)[Peterson]. $\mathcal{M}^D_{*,v,k}(n)$ has only finitely many homotopy classes. ⌟

3 Spectral Geometry

12.8 Complex Geometry

Basic References are [Voi02], [Principle of Algebraic Geometry Griffith/Harris], more advanced stuffs to add from [Kähler Geometry] and [Huy05]. Even more advanced is [Demailly Complex Analytic and Differential Geometry].

1 Complex Manifolds

Def. (12.8.1.1) [Complex Manifold]. A **complex manifold** is an even dimensional manifold that the transformation matrices are holomorphic. The category of complex manifolds are denoted by $\mathbb{C}$-$\mathfrak{Mani}$. ⌟

Prop. (12.8.1.2) [Andreotti-Franlcel]. Let $M^n\subset\mathbb{C}^n\in\mathbb{C}\text{-}\mathfrak{Mani}^n$, then M is homotopic to a CW complex of real dimension$\leq n$. ⌟

Proof: □

Prop. (12.8.1.3) [Adjunction Formula]. The normal sheaf of a submanifold $Y\subset X$ is defined the same as the case of nonsingular varieties(6.11.1.17), then the same is true of the adjunction formula:

$$\mathcal{K}_Y\cong\mathcal{K}_X\otimes\det\mathcal{N}_{Y/X}$$

In case Y is of codimension 1, $\mathcal{N}_{Y/X}\cong\mathcal{L}(Y)|_Y=\mathcal{O}_Y(Y)$. ⌟

Prop. (12.8.1.4) [Remmert]. A non-compact complex manifold admits a proper holomorphic embedding into $\mathbb{C}^N$ for some N iff it is a Stein manifold. ⌟

Proof: ? □

Prop. (12.8.1.5) [Siegel]. Let $X\in\mathbb{C}\text{-}\mathfrak{Mani}^n$, then the field $R(X)$ of meromorphic functions on X has transcendence degree$\leq n$ over $\mathbb{C}$. And in case $\mathrm{tr.deg}[R(X):\mathbb{C}]=n$, it is a f.g. field extension of $\mathbb{C}$. Then we define the **algebraic dimension** of a compact connected complex manifold X to be $\dim^{\mathrm{alg}}(X)=\mathrm{tr.deg}\,R(X)$. ⌟

Proof: It suffices to show that given any meromorphic functions $f_1,\ldots,f_{n+1}$, there is an algebraic relation between them.

Now for each x, there is a nbhd U_x that any f_i writes as the quotient of two holomorphic functions $\frac{g_{i,x}}{h_{i,x}}$. And assume $W_x\subset V_x\subset\overline{V_x}\subset U_x$ are the metric balls $B(x,\frac{1}{2})\subset B(x,1)$. As X is compact, there are N x_k that $X=\cup W_{x_k}$.

As on the intersections, $\frac{g_{i,k}}{h_{i,k}}=\frac{g_{i,l}}{h_{i,l}}$, any we can assume they are all prime, so $\frac{g_{i,k}}{g_{i,l}}=\varphi_{i,kl}$ is a unit. Let $\varphi_{kl}=\prod_i\varphi_{i,kl}$, as X is compact, let $C=\max_{k,l}\varphi_{kl}\geq 1$.

For any homogenous polynomial $F\in\mathbb{C}[X_1,\ldots,X_{n+1}]$ of deg m, let $G_k=F(\frac{g_{1,k}}{h_{1,k}},\ldots,\frac{g_{n,k}}{h_{n,k}})(\prod_i h_{ik})^m$. Then G_k are holomorphic and $G_k=\varphi_{lk}^mG_l$ on the intersection. Now I claim for any $M>0$, there is a F that G_k vanishes vanishes up to at least order M at x_k.

For this, just consider the dimension of all homogenous polynomials of degree m is C^m_{m+n+1}, and the number of desired equations of elements needs to be vanish is $N\cdot C^{m'-1}_{m'-1+n}$, so this always can be achieved when m is sufficiently large.

By Schwartz lemma(11.5.6.4), $|G_k(x)|\leq(\frac{1}{2})^{m'}C'$, where $C'=\max\{|G_k(x)||k=1,\ldots,n,x\in\overline{V_k}\}$.

If $C'=|G_k(x)|$, and $x\in W_l$, then $C'=|G_l(x)||\varphi_{lk}^m(x)|\leq\frac{C'}{2^{m'}}\cdot C^m$. If for some m,m', $C^m<2^{m'}$, then this shows $C'=0$ which will finish the proof.

Look back at the condition of m, m', $C^m_{m+n+1} > N \cdot C^{m'-1}_{m'-1+n}$ can be achieved together with $m < \lambda m'$ for any λ, because the left hand is degree $n+1$ in m and the right hand is degree n in m'. □

Almost Complex Structure

Def. (12.8.1.6) [Almost Complex Structures]. For M a real orientable manifold of dimension $2n$, an **almost complex structure** is a real bundle map $J : T_{\mathbb{C}}M \to T_{\mathbb{C}}M$ satisfying $J^2 = -1$. A manifold with an almost complex structure is called an **almost complex manifold**.

A complex manifold has an almost complex structure, just define

$$J(\frac{\partial}{\partial x_i}) = \frac{\partial}{\partial y_i}, \quad J(\frac{\partial}{\partial y_i}) = -\frac{\partial}{\partial x_i}.$$

⌟

Def. (12.8.1.7) [Complex Differentials]. Situation as in(12.8.1.6), J will define a bundle map $J : T^*M \to T^*M$, and it has two eigenvalues $\pm\mathrm{i}$, denoted by $T^{*1,0}M$ and $T^{*0,1}M$. The **formal differential forms** $\wedge^k T^*M \cong \oplus_{0\le p\le k} \wedge^{p,k-p} T^*M$.

Define $\partial = \mathrm{pr}_{p+1,q} \circ \mathrm{d}$ on $\wedge^{p,q}T^*M$, and $\overline{\partial} = \mathrm{pr}_{p,q+1} \circ \mathrm{d}$ on $\wedge^{p,q}T^*M$. ⌟

Def. (12.8.1.8)[Integrability]. An almost complex structure (M, J) is called **integrable** iff it satisfies the following equivalent conditions:

- $d\alpha = \partial\alpha + \overline{\partial}\alpha$.
- $d\alpha = \partial\alpha + \overline{\partial}\alpha$ is true for $\alpha \in \Omega^{1,0}(M)$
- $[T^{0,1}X, T^{0,1}X] \subset T^{0,1}X$.
- $\overline{\partial}^2 f = 0$ for functions f.

⌟

Proof: 1 $\iff$ 3 is because by(12.1.3.6), if $u, v \in T^{0,1}X$,

$$d\alpha(u, v) = u(\alpha(v)) - v(\alpha(u)) - \alpha([u, v]) = -\alpha([u, v]).$$

3 $\iff$ 4 is because by(12.1.3.6), if $\alpha = \overline{\partial}f$ and $u, v \in T^{0,1}X$, then

$$\overline{\partial}^2 f(u, v) = u(\overline{\partial}f(v)) - v(\overline{\partial}f(u)) - \overline{\partial}f([u, v]) = u(df(v)) - v(df(u)) - \overline{\partial}f([u, v]) = \partial f([u, v])$$

□

Thm. (12.8.1.9)[Nirenberg-Newlander]. Given an almost complex manifold (M, J), it is integrable iff it comes from a complex structure. ⌟

Proof: Cf.[Foundation of Differential Geometry Kobayashi Chap9.2]. □

Cor. (12.8.1.10). For $M \in \mathbb{C}$-$\mathfrak{Mani}$,

$$\overline{\partial}^2 = 0, \quad \partial\overline{\partial} + \overline{\partial}\partial = 0, \quad \partial^2 = 0.$$

⌟

2 Deformation of Complex Structures

Cf.[Kähler Geometry] and [Complex Geometry, Daniel Chap6], should be completed as soon as possible.

3 Analytic Spaces and Coherence Sheaves

Cf.[Demailly] and [GAGA Serre].

Analytic Subvarieties

Def. (12.8.3.1) [Analytic subvariety]. An **analytic subvariety** is a closed subset of a complex manifold that is locally defined by f.m. holomorphic functions. The **regular points** of an analytic subvatiety locally defined by k functions is the points that $\mathrm{rank}((\frac{\partial}{\partial z_j}f_i)_{i\leq k,j\leq n})=k$. ⌟

Prop. (12.8.3.2) [Proper Mapping Theorem]. If U,M are complex manifolds and $M\subset U$ is an analytic subvariety, then if $f:U\to N$ is a holomorphic mapping whose restriction on M is proper, then $f(M)$ is an analytic subvariety of N. ⌟

Proof: Cf.[Griffith/harris P395]. □

Def. (12.8.3.3) [Local Analytic Spaces]. An **analytic space of** $\mathbb{C}^n$ is an analytic subvariety of $\mathbb{C}^n$. On an analytic space, there is a sheaf of holomorphic functions $\mathcal{O}_U$. So we can define **holomorphic map** φ as continuous functions that maps holomorphic germs to holomorphic germs, which is equivalent to the coordinates of φ are all holomorphic. ⌟

Def. (12.8.3.4) [Analytic Spaces]. An **analytic space** is a Hausdorff space X with a structure sheaf $\mathcal{O}_X$ that is locally isomorphic to an analytic space of $\mathbb{C}^n$(12.8.3.3). Morphisms are continuous maps that are locally holomorphic. Sub-analytic spaces are defined as usual.

The products of analytic spaces can be defined, and it has the product topology, unlike the case of schemes. ⌟

Prop. (12.8.3.5) [Analytic Modules]. Let $(X,\mathcal{O}_X)$ be an analytic space(12.8.3.4), an **analytic module** over X is just an $\mathcal{O}_X$-module. For a sub-analytic space Y, we have a sheaf of ideals $\mathcal{I}_Y$ which is the sheaf of germs vanishing at Y, and $\mathcal{O}_X/\mathcal{I}_Y$ is a sheaf on X that is zero outside Y, and we identify it with $\mathcal{O}_Y$. ⌟

Def. (12.8.3.6) [Coherent Analytic Sheaves]. ? ⌟

Prop. (12.8.3.7) [Coherence of Structure Sheaf]. If $(X,\mathcal{O}_X)$ is an analytic space, then $\mathcal{O}_X$ is coherent?, and the sheaf of ideals $\mathcal{I}_Y$ of any sub-analytic-space Y is also coherent. ⌟

Proof: First prove for X is an open subset of $\mathbb{C}^n$, Cf.[GAGA Serre P4]. And by definition $\mathcal{O}_X$ is a $\mathcal{O}_X$-module of f.t., and it is also coherent?, so $\mathcal{O}_X$ is coherent. $\mathcal{I}_Y$ is coherent because it is a kernel of $\mathcal{H}_X\to\mathcal{H}_Y$. □

4 Positive Current

5 Hermitian Vector Bundles

Def. (12.8.5.1) [Holomorphic and Hermitian Vector Bundles]. H A **holomorphic vector bundle** is a vector bundle on a complex manifold that the transition functions are holomorphic. A **Hermitian vector bundle** is a holomorphic vector bundle endowed with a Hermitian metric**?**. Any holomorphic vector bundle has a Hermitian structure, by partition of unity method. ⌟

Prop. (12.8.5.2) [Hodge Star for Hermitian bundles]. If $\mathcal{E}$ is a Hermitian vector bundle over a compact complex manifold X of complex dimension n, we define a conjugate-linear operator $\overline{*}$: $A^{p,q}(\mathcal{E}) \to A^{n-p,n-q}(\mathcal{E}) : \eta \mapsto *\overline{\eta}$, and a conjugate-linear functor $\tau E \to E^*$ induced by the Hermitian metric on E.

Then we can define $\overline{*}_E : A^{p,q}(E) \to A^{n-p,n-q}E : \eta \otimes s \mapsto \overline{*}(\eta) \otimes \tau(s)$. It can be checked that

$$(\alpha, \beta) * 1 = \alpha \wedge *_E \beta,$$

$$\overline{\partial}^*_E = -\overline{*}_{E^*}\overline{\partial}_{E^*}\overline{*}_E, \quad \overline{*}_E \Delta_{\overline{\partial}_E} = \Delta_{\overline{\partial}_{E^*}}\overline{*}_{E^*}, \quad \overline{*}_{E^*}\overline{*}_E = (-1)^{p+1} \text{ on } \Omega^{p,q}(E).$$

⌟

Hermitian Manifold

Def. (12.8.5.3) [Holomorphic Tangent Bundle]. Let M be a complex manifold, the complexified tangent bundle $T_{\mathbb{C}}M$ is defined as $TM \otimes_{\mathbb{R}} \mathbb{C}$, the **holomorphic tangent bundle** $T^{1,0}M$ and anti-holomorphic bundle $T^{0,1}M$ are defined to be the vectors generated resp. by $\frac{\partial}{\partial z_i}$ and $\frac{\partial}{\partial \overline{z_i}}$. The **holomorphic cotangent bundle** and anti-holomorphic cotangent bundle is defined to be the covectors generated by $\mathrm{d}z_i$ and $\mathrm{d}\overline{z}_i$. ⌟

Def. (12.8.5.4) [Hermitian Metric]. Let M be an almost complex manifold, a **Hermitian metric** on $T_{\mathbb{C}}M$ is a metric that is J-invariant, that is $g(Ju, Jv) = g(u, v)$. Notice(3.5.10.12) shows a Hermitian metric is equivalent to a non-degenerate Hermitian form on $T_{\mathbb{C}}M$, where g appears as the real part of the Hermitian form. ⌟

Def. (12.8.5.5) [Hermitian Manifolds]. A complex manifold with a Hermitian metric is called a **Hermitian manifold**. ⌟

Def. (12.8.5.6) [the Kähler Form]. Given a Hermitian manifold M, define the **Kahler form** ω_g as $\omega_g(u, v) = g(Ju, v)$. Then it is a real 2-form on M.

Notice $g(u, v) = \omega_g(u, Jv)$, so g can be constructed by ω_g, iff ω_g is positive(12.9.6.1). ⌟

Analytic Picard Groups

Def. (12.8.5.7) [Analytic Picard Groups]. The group of isomorphisms of holomorphic line bundles on a complex manifold X is denoted by $\mathrm{Pic}_{\mathbb{C}}(X)$, called the **analytic Picard group** of X. ⌟

Prop. (12.8.5.8) [First Chern Class]. For a connected space X, there is an exact sequence

$$0 \to \mathbb{Z} \to \mathcal{O}_X \xrightarrow{f \to e^{2\pi i f}} \mathcal{O}^*_X \to 0,$$

and it induces a map $\mathrm{Pic}_{\mathbb{C}}(X) = H^1(X, \mathcal{O}^*_X) \to H^2(X, \mathbb{Z})$, which is a just the first Chern class(same proof as in(4.15.4.19)).

WARNING: in this case it is not necessarily isomorphism, not as in the case of topological line bundles.

in particular, The image of the first Chern class is trivial in $H^2(X,\mathcal{O}_X)$. ⌟

Def. (12.8.5.9). The dual of the universal line bundle on $\mathbb{CP}^n$ is called the **hyperplane line bundle**, denoted by H or $\mathcal{O}(1)$. ⌟

Prop. (12.8.5.10). $\mathrm{Pic}_{\mathbb{C}}(\mathbb{CP}^n)\cong\mathbb{Z}$, with $\mathcal{O}(1)$ as a generator. ⌟

Proof: As $\mathbb{CP}^n$ is Kähler, use(12.10.2.5), then $H^{0,k}(X,\mathbb{C})\cong H^k(X,\mathcal{O}_X)=H^k(X,\mathcal{K}_X\otimes\mathcal{O}(2))=0$ for $k\geq 1$ by Kodaira vanishing(12.9.7.3), and then $\mathrm{NS}(X)=H^{1,1}(X)=H^2(X,\mathbb{Z})=\mathbb{Z}$ by Lefschetz $(1,1)$-form theorem(12.10.2.6). It remains to prove $c_1(\mathcal{O}(1))$ is the generator, for this, Cf.[Demailly P280]. □

Prop. (12.8.5.11). Let S_d be the set of homogenous polynomials of degree d, then

$$H^0(\mathbb{CP}^n,\mathcal{O}(d))=\begin{cases}S_d & d\geq 0\\ 0 & d<0\end{cases}$$

⌟

Proof: This is because it is sections that satisfy $f_\alpha([z])=(\frac{z_\beta}{z_\alpha})^k f_\beta([z])$, which says f_α glue together to give a holomorphic function homogenous of degree k on $\mathbb{C}^n\setminus\{0\}$, which extends to a function on $\mathbb{C}^n$ by(11.5.6.3), then it is easy to see it is a homogenous polynomial using the power series expansion. □

Def. (12.8.5.12) [Neron-Severi Group]. For a compact complex manifold X, the **Néron-Severi group** $\mathrm{NS}(X)$ is the image of $\mathrm{Pic}_{\mathbb{C}}(X)\to H^2(X,\mathbb{Z})$. $\mathrm{rank}(\mathrm{NS}(X))$ is called the **Picard number** of X.

There is a good description of $\mathrm{NS}(X)$ in case X is Kähler , See Lefschetz theorem(12.10.2.6).

This is compatible with the the algebraic Néron-Severi group(9.7.2.38), Cf.[**?**]P457, [Vak17]P484. ⌟

Chern Connection

Prop. (12.8.5.13)[Chern Connection]. Given a Hermitian holomorphic bundle $E\to M$ on a complex manifold, there is a unique **Chern connection** ∇ on E, that ∇ is holomorphic(i.e. the connection matrix is holomorphic w.r.t a homomorphic frame), and it is compatible with the Hermitian metric. ⌟

Proof: Write out the requirement: if $H=h_{ij}$ is the matrix of the Hermitian metric, so H is Hermitian, and we need $dh_{ij}=(\nabla e_i,e_j)+(e_i,\nabla e_j)=\sum_k\omega_{ik}h_{kj}+\sum\overline{\omega_{jk}}h_{ik}.\omega$ is holomorphic, so must

$$\partial H=\theta H,\quad \overline{\partial}H=H\overline{\theta}^t.$$

But $H^t=\overline{H}$ so these two equations are equivalent and $\theta=\partial HH^{-1}$. □

Cor. (12.8.5.14). The curvature of the Chern connection is $\Omega=\overline{\partial}(\partial(h)h^{-1})$. In particular, it is a skew-symmetric matrix of $(1,1)$-forms. If it is of dimension 1, then $\Omega=\overline{\partial}\partial\log h$. ⌟

Proof: Ω is locally $d\omega+\omega\wedge\omega$, so if we choose a unitary basis, then ω is skew-symmetric by definition and $\omega\wedge\omega$ is also skew-symmetric, so Ω is skew-symmetric. The calculation is direct calculation. □

Prop. (12.8.5.15). The transformation matrix of a complex manifold is holomorphic, so it is possible to define globally $\overline{\partial}$ operator. And locally on a nbhd, ∂ is defined as $d-\overline{\partial}$. ⌟

Prop. (12.8.5.16) [Normal Coordinate]. For a Hermitian vector bundle E over a complex manifold X, given any coordinate frame (z_j), there exists a holomorphic frame (e_λ) that

$$\langle e_\lambda, e_\mu\rangle = \delta_{\lambda,\mu} - \sum c_{jk\lambda\mu} z_j \overline{z}_k + O(|z|^3)$$

where $c_{ij\lambda\mu}$ is the coefficient of the Chern connection Ω. Such a coordinate is called the **normal coordinate frame** of E at x. ⌟

Proof: Cf.[Demailly P270]. □

6 Cohomology

Lemma (12.8.6.1) [Dolbeault Complex, $\overline{\partial}$-Poincaré Lemma]. If X is a complex manifold of dimension n, and $\mathcal{E}$ a holomorphic vector bundle, then there is an exact sequence:

$$0 \to \Omega^{p,0}(\mathcal{E}) \xrightarrow{\overline{\partial}_{\mathcal{E}}} \Omega^{p,1}(\mathcal{E}) \xrightarrow{\overline{\partial}_{\mathcal{E}}} \ldots \xrightarrow{\overline{\partial}_{\mathcal{E}}} \Omega^{p,n-p}(\mathcal{E}) \to 0$$

If $p=0$, it is called the **Dolbeault complex** of $\mathcal{E}$. ⌟

Proof: Because tensoring $\mathcal{E}$ is exact, it suffices to show for $\mathcal{E} = \underline{\mathbb{C}}_X$. As $\overline{\partial}^2 = 0$(12.8.1.10), and the sequence is clearly exact at $\Omega^{p,0}(\mathcal{E})$, it suffices to show that if $\alpha \in \Omega^{p,q}(X), q > 0$ satisfies $\overline{\partial}\alpha = 0$, then $\alpha = \overline{\partial}\beta$ for some $\beta \in \Omega^{p,q-1}(X)$. Let

$$\alpha = \sum_I \sum_J \alpha_{I,J} \mathrm{d}z_I \wedge \mathrm{d}\overline{z}_J = \sum_I \mathrm{d}z_I (\sum_J \alpha_{I,J} \wedge \mathrm{d}\overline{z}_J),$$

then it is clear it suffices to prove for $(\sum_J \alpha_{I,J} \wedge \mathrm{d}\overline{z}_J)$, and the question is reduced to the case $p=0$.

Suppose $\alpha = \sum_J \alpha_J \wedge \mathrm{d}\overline{z}_J$, then we use induction on k which equals the maximal number s.t. there is a J with $k \in J$ and $\alpha_J \neq 0$. Notice $k \geq q$. If $k = q$, then

$$\alpha = f \mathrm{d}\overline{z}_1 \wedge \ldots \wedge \mathrm{d}\overline{z}_q,$$

and f is holomorphic in the variables $z_l, l > q$. Then the proof of(11.4.1.12) gives us a smooth function g s.t. $\frac{\partial}{\partial \overline{z}_q} g = f$ that is holomorphic in the variables $z_l, l > q$. So

$$\overline{\partial}((-1)^{q-1} g \mathrm{d}\overline{z}_1 \wedge \ldots \wedge \mathrm{d}\overline{z}_{q-1}) = f \mathrm{d}\overline{z}_1 \wedge \ldots \wedge \mathrm{d}\overline{z}_q.$$

So the case $k = q$ is proved. Suppose the assertion is true for $k-1 \geq q$, suppose

$$\alpha = \alpha_1 + \alpha_2 \wedge \mathrm{d}\overline{z}_k,$$

where only the coordinates of index$< k$ appear in α_i. Then α_2 is holomorphic in the same argument as above shows that for each J, $\alpha_{2,J} = \frac{\partial}{\partial \overline{z}_k} \beta_{2,J}$ that each $\beta_{2,J}$ is holomorphic in the variables $z_l, l > q$. Then

$$\overline{\partial}(\sum_J \beta_{2,J} \mathrm{d}\overline{z}_J) = (-1)^{q-1} \alpha_2 \wedge \mathrm{d}\overline{z}_k + \alpha_1'$$

where α_1' involves only the coordinates z_l for $l < k$. Then we eliminated $\mathrm{d}\overline{z}_k$ and can use induction hypothesis from now. □

Def. (12.8.6.2) [Dolbeault Cohomology]. The **Dolbeault cohomology group** $H^{p,q}_{\overline{\partial}}(X,\mathcal{E})$ of a holomorphic vector bundle $\mathcal{E}$ over a complex manifold X is defined to be the q-th cohomology group of the complex

$$0 \to \Omega^{p,0}(\mathcal{E}) \xrightarrow{\overline{\partial}_{\mathcal{E}}} \Omega^{p,1}(\mathcal{E}) \xrightarrow{\overline{\partial}_{\mathcal{E}}} \ldots \xrightarrow{\overline{\partial}_{\mathcal{E}}} \Omega^{p,n-p}(\mathcal{E}) \to 0$$

and $H^{p,q}_{\overline{\partial}}(X)$ is defined to be $H^{p,q}_{\overline{\partial}}(X,\underline{\mathbb{C}}_X)$. By(12.8.6.5), $H^{p,q}_{\overline{\partial}}(X,\mathcal{E}) \cong H^q_{\overline{\partial}}(M,\Omega^p_{\mathrm{hol}} \otimes_{\mathcal{O}_X} \mathcal{E})$. ⌟

Cor. (12.8.6.3). If X is a complex manifold of dimension n, there are exact sequences:

$$0 \to \underline{\mathbb{C}}_X \xrightarrow{\partial} \mathcal{O}_X \xrightarrow{\partial} \Omega^1_{\mathrm{hol}} \xrightarrow{\partial} \ldots \xrightarrow{\partial} \Omega^n_{\mathrm{hol}} \to 0$$

⌟

Proof: This follows from the Poincaré lemma(6.3.5.10) and $\overline{\partial}$-Poincare lemma(12.8.6.1), by applying the spectral sequence(I mean in the category of sheaves).**?** □

Prop. (12.8.6.4) [Holomorphic Cohomology]. For $X \in \mathbb{C}$-$\mathfrak{Mani}$,

$$H^p(X,\underline{\mathbb{C}}) = H^p(X,\Omega^\bullet_{\mathrm{hol}}).$$

⌟

Prop. (12.8.6.5) [Dolbeault]. For $X \in \mathbb{C}$-$\mathfrak{Mani}$ and $\mathcal{E}$ a holomorphic bundle,

$$H^{p,q}_{\overline{\partial}}(X,\mathcal{E}) \cong H^q(M,\Omega^p_{\mathrm{hol}} \otimes_{\mathcal{O}_X} \mathcal{E}),$$

where the left is Dolbeault cohomology and the right is sheaf cohomology. (Use the fact that smooth sheaf is fine so adapted to sheaf cohomology(6.3.5.4), and $\overline{\partial}$-Poincare lemma(12.8.6.1)).

Moreover, there is a spectral sequence of

$$E_1^{p,q} = H^{p,q}_{\overline{\partial}}(X) \Rightarrow E^n = H^n_{dR}(X,\mathbb{R}) \times_{\mathbb{R}} \mathbb{C}.$$

⌟

Prop. (12.8.6.6) [Cartan]. The class of Coh-Acyclic subsets of an analytic space is exactly the class of Stein manifolds. ⌟

Proof: □

De.Rham Cohomology

Prop. (12.8.6.7). The Frölicher spectral sequence of a compact Kähler manifold generates at E_1. ⌟

Proof: □

7 GAGA

Main references are [Ser55].

Analytification of Algebraic Varieties and Sheaves

Prop. (12.8.7.1) [Analytification]. For any variety over $\mathbb{C}$, any open affine subset is isomorphic to an analytic space of $\mathbb{C}^n$, hence can be given an analytic structure X^{an} called the **analytification of** X. It is a locally ringed space, together with a map $X^{\mathrm{an}} \to X$ of local ringed spaces.

This construction extends to a functor

$$\mathcal{S}\mathrm{ch}^{\mathrm{loc.ft},sep}/\mathbb{C} \to \mathrm{AnSpa}/\mathbb{C}.$$

An **algebraic analytic space** is an analytic space that is in the essential image of this functor.

Notice X^{an} and X have in fact the same underlying sets. ⌟

Remark (12.8.7.2). There is in fact a more general analytification for any scheme locally of finite type over $\mathbb{C}$. That is, we define it as the right adjoint to the forgetful functor from analytic spaces to local ringed spaces. Where an analytic space is a local ringed space that locally has immersions into $\mathbb{C}^n$. Should consult [Grothendieck EGA1-7]. ⌟

Proof: Notice the schemes that have an analytification is stable under open subscheme, closed subscheme and products, and we can make a glue a large space from open subschemes by the unicity. So we only need to consider $\operatorname{Spec}\mathbb{C}[T]$, whose analytification is $\mathbb{C}$. □

Def. (12.8.7.3) [Betti Cohomologies]. For any variety defined over $\mathbb{C}$, and $\mathbb{R}$ a ring, let $H^i_{Betti}(X,R) = H^i(X^{\mathrm{an}},R)$ be the **Betti cohomology** of X with coefficients in R. ⌟

Prop. (12.8.7.4) [Transfer of Properties].

- X^{an} is locally compact and σ-compact.
- X^{an} is Hausdorff
- A morphism $f : X \to Y$ is smooth/étaleiff f^{an} is smooth/a local isomorphism. X is smooth over $\mathbb{C}$ iff X^{an} is a complex manifold.
- A morphism $f : X \to Y$ is proper iff $X^{\mathrm{an}} \to Y^{\mathrm{an}}$ is proper. In particular, X is complete(proper) iff X^{an} is compact.
- If X is projective and connected, then X^{an} is connected iff X is connected.

⌟

Proof: 1: X is qc hence covered by f.m. affine subsets hence second-countable and use(4.4.2.23). X^{an}/X is flat because completion of Noetherian rings are flat(5.2.3.14).

2: Because analytification preserves products and morphisms, and separatedness of X shows that $\Delta(X)$ is closed in $X \times X$, hence it is also closed in the analytification.

3: This follows from the Jacobian criterion(5.4.5.24).

4: Cf.[GAGA Serre P8].

5: This follows from(12.8.7.16), as $H^0(X,\mathcal{O}_X) = H^0(X^{\mathrm{an}},\mathcal{O}_X)$. □

Prop. (12.8.7.5). There is a natural map from $\mathcal{O}_x$ to $\mathcal{H}_x$ that maps $\mathfrak{m}_x$ to $\mathfrak{m}_x\mathcal{H}_x$, thus inducing a map $\widehat{\theta} : \widehat{\mathcal{O}}_x \to \widehat{\mathcal{H}}_x$. This is an isomorphism. In particular, $\theta : \Omega_x \to \mathcal{H}_x$ is injective.

Moreover, if Y is a locally closed subscheme of X, then the local ideal of functions vanishing at Y maps to $\mathcal{A}_x(Y)$, and $\mathcal{A}_x(Y)$ is generated by $\theta(\mathcal{I}_x(Y))$. Moreover, $\mathcal{H}_{x,Y} = \mathcal{H}_x/\mathcal{I}_x(Y)$. ⌟

Proof: [GAGA Serre P6]. □

Cor. (12.8.7.6). The inclusion $\mathcal{O}_x \subset \mathcal{H}_x$ is flat ring extension, by(5.4.1.20) and the fact $\widehat{A}/A$ is flat. And $\dim \mathcal{O}_x = \dim \mathcal{H}_x$ because $\dim A = \dim \widehat{A}$(5.2.4.16). ⌟

Cor. (12.8.7.7). Given an open and dense subscheme U of an algebraic variety X over $\mathbb{C}$, U^{an} is dense in X^{an}. ⌟

Proof: Consider the complement Y, if U^{an} is not dense in X^{an}, then there exists a x that $\mathcal{A}_x(Y) = 0$, so by(12.8.7.5), $\mathcal{I}_x(Y) = 0$, so Y is not dense near x, contradiciton. □

Cor. (12.8.7.8). For a morphism f of algebraic varieties over $\mathbb{C}$, $\overline{f(X)^{\mathrm{an}}} = \overline{f(X)}^{\mathrm{an}}$. ⌟

Proof: By Chevalley theorem(6.6.1.6), there is a open dense subscheme U of $\overline{f(X)}$ that is contained in $f(X)$, then(12.8.7.7) shows U^{an} is dense in $\overline{f(X)}^{\mathrm{an}}$, so $\overline{f(X)}^{\mathrm{an}} \subset \overline{f(X)^{\mathrm{an}}}$. The converse is obvious. □

Def. (12.8.7.9)[Analytification of Sheaves]. Denote for a sheaf $\mathcal{F}$ over X $\mathcal{F}'$ the inverse image sheaf over X^{an} pulled back along $X^{\mathrm{an}} \to X$. Define $\mathcal{F}^{\mathrm{an}}$ the **analytification of** $\mathcal{F}$ as the sheaf $\mathcal{F}' \otimes_{\mathcal{O}_X} \mathcal{H}_X$. ⌟

Prop. (12.8.7.10). $\mathcal{F} \to \mathcal{F}^{\mathrm{an}}$ is exact from the category of sheaves on X to the category of analytic sheaves on X^{an}, $\mathcal{F}' \to \mathcal{F}^{\mathrm{an}}$ is injective, and it maps coherent sheaves to coherent analytic sheaves. ⌟

Proof: The first two follows from the fact that $\mathcal{H}_X$ is flat over $X^{\mathrm{an}} \to X$(12.8.7.6). For the last assertion, notice if $\mathcal{O}_X^p \to \mathcal{O}_X^q \to \mathcal{F} \to 0$, then $\mathcal{H}_X^p \to \mathcal{H}_X^q \to \mathcal{F}^{\mathrm{an}} \to 0$, so it is coherent because $\mathcal{H}_X$ is coherent(12.8.3.7)(6.2.2.28). □

Prop. (12.8.7.11). Let $i : Y \to X$ be a closed subscheme, then for a coherent sheaf $\mathcal{F}$ on Y, $(i^{\mathrm{an}})_*\mathcal{F}^{\mathrm{an}} \cong (i_*\mathcal{F})^{\mathrm{an}}$. ⌟

Proof: These two sheaves are both 0 outside Y^{an}, consider a point of Y, their stalks are respectively $\mathcal{F}_x \otimes_{\mathcal{O}_{x,X}} \mathcal{H}_{x,X}$ and $\mathcal{F}_x \otimes_{\mathcal{O}_{x,Y}} \mathcal{H}_{x,Y}$. By(12.8.7.5) we notice

$$\mathcal{H}_{x,Y} = \mathcal{H}_{x,X}/\mathcal{I}_x(Y)\mathcal{H}_{x,X} = \mathcal{H}_{x,X} \otimes_{\mathcal{O}_{x,X}} \mathcal{O}_{x,Y}.$$

So this two are equal by associativity of tensor product. □

Prop. (12.8.7.12). By Leray Spectral sequence(6.3.1.9), for an analytic sheaf $\mathcal{G}$, there is a boundary map $H^k(X, \mathcal{G})H^k(X^{\mathrm{an}}, \mathcal{G})$. So for a sheaf $\mathcal{F}$ on X, there is a map

$$\varepsilon : H^k(X, \mathcal{F}) \to H^k(X, an_*\mathcal{F}^{\mathrm{an}}) \to H^k(X^{\mathrm{an}}, \mathcal{F}^{\mathrm{an}})$$

⌟

Equivalence between Algebraic Variety and Analytic Spaces

Remark (12.8.7.13) [GAGA Principle]. In principal, any complete analytic object in $\mathbb{CP}^n$ is algebraic. ⌟

Prop. (12.8.7.14). Let X, Y be algebraic varieties over $\mathbb{C}$ and $f : X \to Y$ is morphism that is bijective, if f^{an} is an analytic isomorphism, then f is an isomorphism. ⌟

Proof: Cf.[GAGA Serre P9]. □

Cor. (12.8.7.15). Let X, Y be algebraic varieties over $\mathbb{C}$, iff $f: X^{\mathrm{an}} \to Y^{\mathrm{an}}$ is holomorphic map and the image of f in $X^{\mathrm{an}} \times Y^{\mathrm{an}} = (X \times Y)^{\mathrm{an}}$ comes from an algebraic subscheme, then f comes from an algebraic morphism. (Because $X^{\mathrm{an}} \to \Gamma(X)$ is an analytic isomorphism). ⌟

Prop. (12.8.7.16) [GAGA on $\mathfrak{Coh}(X)$]. Let X be a proper scheme over $\mathbb{C}$, then $\mathcal{F} \to \mathcal{F}^{\mathrm{an}}$ defines an equivalence of categories between $\mathfrak{Coh}(X)$ and $\mathfrak{Coh}^{\mathrm{an}}(X^{\mathrm{an}})$. ⌟

Proof: Cf.[GAGA Serre P13], [SGA1,Chap12].. □

Prop. (12.8.7.17) [GAGA on Projective Varieties].

- (Chow)Any analytic subvariety of $\mathbb{CP}^n$ is algebraic.
- Any meromorphic function on an algebraic variety $V \subset \mathbb{CP}^n$ is rational.
- Any meromorphic differential form on a smooth variety is algebraic.
- Any holomorphic map between smooth varieties can be given by rational maps.
- Any holomorphic vector bundle on a smooth variety is algebraic, i.e. transition function can be made rational.

Cf.[Griffith/Harris P168,170].? ⌟

Cor. (12.8.7.18). If the analytification of a variety X is a compact complex manifold, i.e. X is smooth(12.8.7.4), then $K(X) = K(X^{\mathrm{an}})$, as they are both morphism to $\mathbb{P}^1$. ⌟

Applications

Prop. (12.8.7.19) [Generalized Riemann Existence Theorem]. Let X be a normal scheme of finite type over $\mathbb{C}$. Given any finite morphism of analytic spaces(i.e. proper and has finite fibers) form a normal complex analytic space $f: X' \to X^{\mathrm{an}}$, then there is a unique normal scheme X' and a finite morphism $g: X' \to X$ that $g^{\mathrm{an}} = f$. ⌟

Proof: Cf.[SGA1, Chap12], using resolution of singularities. □

Cor. (12.8.7.20) [Algebraic Fundamental Group]. ⌟

8 Algebraic Compact Complex Manifolds

Def. (12.8.8.1) [Moishezon Manifolds]. A compact complex manifold is called a **Moishezon manifold** iff $\operatorname{tr.deg.} K(X) = \dim X$, by(12.8.1.5) this is the highest degree it can have. When X is an analytification of an algebraic variety X^{an}, $K(X^{\mathrm{an}}) = K(X)$ by(12.8.7.18), so Moishezon is a necessary condition for a compact complex manifold to be algebraic. ⌟

Prop. (12.8.8.2) [Chow-Kodaira]. Any Moishezon manifold of dimension2 is algebraic and projective. ⌟

Proof: □

Prop. (12.8.8.3) [Moishezon]. Any Moishezon manifold becomes algebraic and projective after a finite number of monoidal transformations with non-singular centers. ⌟

Proof: □

Prop. (12.8.8.4) [Artin]. The category of smooth proper algebraic spaces over $\mathbb{C}$ is equivalent to the category of Moishezon manifolds.

In particular, there are non-algebraic Moishezon manifolds in dimension≥ 3. Examples are given in[Har77]P444. ⌟

Proof: □

Prop. (12.8.8.5) [Moishezon]. Every Moishezon manifold that is Kähler is projective and algebraic. ⌟

Proof: Cf.[Moishezon On n-dimensional compact varieties with n algebraically independent meromorphic functions]. □

9 Riemann Surfaces

Prop. (12.8.9.1) [Genus]. ⌟

Thm. (12.8.9.2) [Uniformization Theorem, Poincaré-Klein-Koebe]. Any simply-connected Riemann surface is analytically isomorphic to one of the following:

$$\mathcal{H} \cong \mathbb{D}, \mathbb{C}, \mathbb{P}^1(\mathbb{C}).$$

⌟

Proof: □

Cor. (12.8.9.3)[Classifying Riemann Surfaces]. For any Riemann surface S with universal covering space $\widetilde{S}$,

- If $\widetilde{S} \cong \overline{\mathbb{C}}$, then S is compact, so by(12.8.9.6) and Riemann-Hurewitz(6.12.1.32), $\widetilde{S} \to S$ is an isomorphism. So in this case $S \cong \overline{\mathbb{C}}$.
- If $\widetilde{S} \cong \mathbb{C}$, then $\pi_1(S) \subset \mathrm{Aut}(\widetilde{S}) = \mathbb{C} \ltimes \mathbb{C}^\times$ by(11.4.7.8). But $\pi_1(S)$ can have no fixed point, so they are all of the form $\tau : z \mapsto z + b$. So it is a lattice of $\mathbb{C}$, thus isomorphic to $\mathbb{1}, \mathbb{Z}$ or $\mathbb{Z}^2$. The corresponding S is $\mathbb{C}, \mathbb{C}^\times$ or $\mathbb{C}/\Lambda$ a torus.
- If $\widetilde{S} \cong \mathcal{H}$, then $S = \mathcal{H}/\Gamma$ where $\Gamma \subset \mathrm{PSL}(2, \mathbb{R})$ is a Fuchs group**?**. Such S are called a t**hyperbolic Riemann surface.**

⌟

Cor. (12.8.9.4). If S is a Riemann surface with a non-constant meromorphic function omitting at most 3 points, then S is of hyperbolic type. ⌟

Proof: This is because $\mathbb{C}$ or $\mathbb{P}^1(\mathbb{C})$ cannot be mapped into $\mathbb{D}$. □

Prop. (12.8.9.5) [Metrics on Riemann Surfaces]. For a Riemann surface S,

- If $S = \overline{\mathbb{C}}$, then S has a natural Fubini-Study metric
$$\mathrm{d}s^2 = \frac{4|\mathrm{d}z|^2}{(1 + |z|^2)^2}.$$
with curvature 1.
- If $\widetilde{S} = \mathbb{C}$, then $\pi_1(S) \subset \mathrm{Aut}(\mathbb{C})$ are all translations so preserves the Euclidean metric $\mathrm{d}s^2 = |\mathrm{d}z|^2$, thus S has a flat metric.
- If $\widetilde{S} = \mathcal{H}$, then $\pi_1(S) \subset \mathrm{Aut}(\mathbb{C}) \cong \mathrm{PSL}(\mathbb{R})$ preserves the hyperbolic metric $\mathrm{d}s^2 = y^{-2}\mathrm{d}x\mathrm{d}y$ by(12.12.0.6), thus inducing a hyperbolic metric on S with curvature -1.

⌟

Compact Riemann Surfaces

References are [Li04].

Prop. (12.8.9.6) [Riemann Existence Theorem]. Any compact Riemann Surface is a Hodge manifold, thus projective algebraic, by(12.9.8.6) and Chow's lemma**??**. And the category of compact Riemann surfaces is equivalent to the category of compact algebraic curves, by GAGA(12.8.7.17). ⌟

Proof: Because $H^{1,1}(X) = H^2(X, \mathbb{Z})$, so it clearly contains integral classes. And it is positive because there is a basis generated by any Hermitian metric on X. So the theorem follows from(12.9.8.6). □

Remark (12.8.9.7). In fact the same argument shows that any Kähler manifold with $H^{0,2}(X) = 0$ is projective. ⌟

Cor. (12.8.9.8). Any compact Riemann surface of genus 0 is analytically isomorphic to $\overline{\mathbb{C}}$. ⌟

Prop. (12.8.9.9).

- For any meromorphic function f on a compact Riemann surface, $(f) = (f)_0 - (f)_\infty$ has degree 0.
- Let ω be a differential form on a compact Riemann surface, then the sum of residues of ω at its poles is zero.

⌟

Proof: 2: Choose a triangularization of the Riemann surface, then use the fact for any simple region Ω be boundary C,

$$\int_C \omega = 2\pi \mathrm{i}(\sum_{\text{poles}} \mathrm{res}_p \omega).$$

And the integrals cancel out.

1: This is a direct consequence of 2 applied to the differential form $\omega = df/f$. □

Abel's Theorem and Reciprocity Law

Prop. (12.8.9.10) [Reciprocity Law I]. Cf.[Griffith/Harris P230]. ⌟

Prop. (12.8.9.11) [Weil]. f, g are meromorphic functions on a compact Riemann surface that $(f), (g)$ are disjoint, then

$$\prod f(p)^{v_p(g)} = \prod g(p)^{v_p(f)}.$$

⌟

Proof: Cf.[Griffith/Harris, P242]. □

Prop. (12.8.9.12) [Differentials on Plane Curves]. ⌟

10 Conformal Geometry

12.9 Kähler Geometry

Basic References are [Voi02], [Principle of Algebraic Geometry Griffith/Harris], more advanced stuffs to add from [Kähler Geometry] and [Huy05]. Even more advanced is [Demailly Complex Analytic and Differential Geometry].

Notation (12.9.0.1).

- Use notations as in Complex Geometry.

⌟

1 Kähler Metric

Def. (12.9.1.1) [Kähler Manifolds]. A metric g on a manifold M is called a **Kähler metric** if the metric form ω_g is closed. In which case, it is called the **Kähler class** or Kähler form of g in $H^2_{\mathrm{dR}}(M)$. A complex manifold with a Kähler metric is called a **Kähler manifold**.

If $g_{ij} = g(\frac{\partial}{\partial z_i}, \frac{\partial}{\partial \overline{z}_j})$, then $\omega_g = \sum_{ij} g_{ij} dz_i \wedge d\overline{z}_j$. Then the condition of ω_g being closed can in fact be written in derivatives of g.

⌟

Prop. (12.9.1.2). If g is Hermitian, then ω_g is real, non-degenerate and $\frac{1}{n!}\omega^n$ is a volume form on M. In particular, if ω is Kähler, then it is a symplectic form. ⌟

Proof: If $g = \sum \varphi_i \otimes \overline{\varphi}_i$, then $\omega = \mathrm{i} \sum \varphi_i \wedge \overline{\varphi}_i$, so it is clear that $\overline{\omega} = \omega$. ω is non-degenerate as g is. The last assertion follows from(3.5.10.22). □

Cor. (12.9.1.3). If M is a compact Kähler manifold, then its even dimensional cohomology group doesn't vanish(12.6.1.6). ⌟

Remark (12.9.1.4). Notice there are notions like almost Hermitian and almost Kähler, similar to the definition of Hermitian and Kähler, but they are just defined using an almost complex structure on M. And an almost Kähler structure is Kähler iff $\nabla J = 0$, Cf.[Foundation of Differential Geometry Kobayashi]. ⌟

Example (12.9.1.5) [Kähler Manifolds].

- If $M = \mathbb{R}^{2n}$, $g = \sum dx_i \wedge dx_i + \sum dy_i \wedge dy_i$, then $\omega_g = \frac{\mathrm{i}}{2} \sum dz_i \wedge d\overline{z}_i$ is Kähler.
- The metric $\omega_g = \sum dz_i \wedge dz_i$ on a complex tori $\mathbb{C}^n/\Lambda$ is Kähler.
- Any Riemann surface is Kähler , because $d\omega$ is a 3-form so vanish.
- if $M = B(0,1) \subset \mathbb{C}^n$ and $\omega_g = \mathrm{i}\, \partial\overline{\partial} \log \frac{1}{1-|z|^2}$, then it is Kähler.
- The product metric on the product space $M \times N$ of two Kähler manifold is Kähler.
- A submanifold of a Kähler manifold is Kähler, as the Kähler form is the pullback of the Kähler form of the large manifold.

⌟

Prop. (12.9.1.6) [Fubini-Study Metric]. The **Fubini-Study metric** form on $\mathbb{CP}^n$ is defined locally to be $\mathrm{i}\, \partial\overline{\partial}|s|^2$, for any local lifting s of the projection $\mathbb{C}^n \backslash \{0\} \to \mathbb{CP}^n$. This doesn't depend on the lifting, as $\partial\overline{\partial}(\log f + \log \overline{f}) = 0$, so they glue together to be a global form on $\mathbb{CP}^n$. It can be checked, ω is translation invariant and on the coordinate $(1, w_1, \ldots, w_n) \to (w_1, \ldots, w_n)$, $\omega|_{(0,\ldots,0)} = \sum dw_i \wedge dw_i$, so it is positive definite. ⌟

Cor. (12.9.1.7). Any projective manifold is Kähler. ⌟

Prop. (12.9.1.8). the Fubini-Study metric on $\mathbb{CP}^n$ has sectional curvature $1 \leq K \leq 4$. ⌟

Proof: Cf.[Do Carmo P188].**?** □

Prop. (12.9.1.9) [Kähler Normal Coordinate]. For a Hermitian metric g on M, g is Kähler iff for any point p of M, there is a holomorphic coordinate centered at p, $\omega_g = \sum g_{ij} dz_i \wedge d\overline{z}_j$ satisfying $g_{ij}(p) = 0$ and $dg_{ij}(p) = 0$. This coordinate is called **Kähler normal coordinate**. (Notice this is different from Darboux theorem, because this coordinate should be holomorphic). ⌟

Proof: Cf.[Complex Geometry P210]. □

2 Geometry of Kähler Manifolds

Prop. (12.9.2.1). Let (M, J, g) be a Kähler manifold, then the complexification of the Levi-Civita connection of g restricts to the Chern connection on $T^{1,0}M$. ⌟

Proof: Cf.[Complex Geometry note 石亚龙 48] and [Complex geometry Daniel Chap4.A]. □

Prop. (12.9.2.2). For a Kähler manifold, $\nabla J = 0$. ⌟

Proof: The problem depends only on first derivative, so choosing a Kähler normal nbhd(12.9.1.9), we may choose J to be constant, so obviously $\nabla J(p) = 0$, P is arbitrary, so $\nabla J = 0$. □

Cor. (12.9.2.3). $\nabla(JX) = J\nabla X$, so $R(X, Y)JZ = JR(X, Y)Z$, thus

$$\langle R(JX, JY)Z, W\rangle = \langle R(Z, W)JX, JY\rangle = \langle R(Z, W)X, Y\rangle = \langle R(X, Y)Z, W\rangle,$$

so $R(JX, JY)Z = R(X, Y)Z$. ⌟

Prop. (12.9.2.4). The curvature tensor of the complexified Levi-Civita connection on a Kähler manifold can be calculated in terms of $\partial_i, \overline{\partial}_j$, Cf.[Complex Geometry note 石亚龙 50]. ⌟

3 Kähler Identities

Let X be a compact complex Kähler manifold.

Def. (12.9.3.1). Introduce some operators:

- $d^c = i(\overline{\partial} - \partial)$, then $dd^c = 2i\partial\overline{\partial}$.
- The **Lefschetz operator** $L(\eta) = \omega \wedge \eta$. Λ is defined as the formal adjoint of L as $A^{p,q}$ is an inner space. In fact, $\Lambda = \pm * L *$.
- $h = (k - n)$ on $\mathcal{A}^k(X)$.

⌟

Prop. (12.9.3.2). $[L, \Lambda] = p + q - n$ on (p, q)-forms. ⌟

Proof: The problem doesn't depends on the derivatives, so using the Kähler normal coordinate(12.9.1.9), it suffice to prove for $\mathbb{C}^n$, for this, Cf.[Griffith/Harris P120] or [Complex Geometry P34]. □

Prop. (12.9.3.3) [Kähler Identities].

$$[\Lambda, \partial] = i\overline{\partial}^*, \quad [\Lambda, \overline{\partial}] = -i\partial^*.$$

⌟

Proof: The second one follows from the first because ω is a real form. For the first, notice only first derivation are involved, so by using the Kähler normal coordinate, it suffice to prove for $\mathbb{C}^n$, and this is by [Complex Geometry 石亚龙 P61]. □

Cor. (12.9.3.4).

$$[\Lambda, d^c] = d^*, \quad [\Lambda, d] = -d^{c*}.$$

⌟

Prop. (12.9.3.5). Δ_d commutes with both L and Λ. ⌟

Proof: L commutes with d because ω is closed, so taking adjoints, Λ commutes with d^*. Now by Kähler identities,

$$\Lambda\Delta_d = \Lambda(dd^* + d^*d) = -d^{c*}d^* + dd^*\Lambda - dd^{*c} + d^*d\Lambda = \Delta_d\Lambda.$$

So taking adjoints, Δ_d also commutes with L. □

Prop. (12.9.3.6). In the Kähler case, $\Delta_\partial = \Delta_{\overline{\partial}} = \frac{1}{2}\Delta_d$. ⌟

Proof:

$$\Delta_d = (\partial + \overline{\partial})(\partial^* + \overline{\partial}^*) + (\partial^* + \overline{\partial}^*)(\partial + \overline{\partial}) = \Delta_\partial + \Delta_{\overline{\partial}} + (\partial\overline{\partial}^* + \overline{\partial}^*\partial) + (\overline{\partial}\partial^* + \partial^*\overline{\partial})$$

So it suffice to prove $\partial\overline{\partial}^* + \overline{\partial}^*\partial = 0$(so $\overline{\partial}\partial^* + \partial^*\overline{\partial} = 0$ by conjugation), and $\Delta_\partial = \Delta_{\overline{\partial}}$. For the first, use Kähler identities, then

$$i(\partial\overline{\partial}^* + \overline{\partial}^*\partial) = \partial[\Lambda, \partial] + [\Lambda, \partial]\partial = 0$$

For the second, using Kähler identities,

$$i\Delta_{\overline{\partial}} = \overline{\partial}[\Lambda, \partial] + [\Lambda, \partial]\overline{\partial} = \overline{\partial}\Lambda\partial + \partial\overline{\partial} - \Lambda\overline{\partial}\partial - \partial\Lambda\overline{\partial}$$

and the same is miraculous true for Δ_∂, so the result is true. □

4 Hodge Theory

Thm. (12.9.4.1) [Hodge Decomposition for compact Kähler Manifolds]. For a compact Kähler manifold X,

$$H^r_{\mathrm{dR}}(X, \mathbb{C}) = \bigoplus_{p+q=r} H^{p,q}_{\overline{\partial}}(X) \cong \bigoplus_{p+q=r} H^q(X, \Omega^p)$$

and $\overline{H^{p,q}_{\overline{\partial}}(X)} \cong H^{q,p}_{\overline{\partial}}(X)$. Moreover, this decomposition doesn't depends on the Kähler metric. ⌟

Proof: (12.9.3.6) shows that Δ_d maps $A^{p,q}$ to $A^{p,q}$, so $\mathcal{H}^{p+q}_d \cap A^{p,q} = H^{p,q}_{\overline{\partial}}(X)$. The last assertion is seen using the Δ_d definition.

If chosen two different Kähler metric g, g', there $\mathcal{H}^{p,q}(X, g) \cong H^{p,q}(X) \cong H^{p,q}(X, g')$. If α, α' be g, g' $\overline{\partial}$-harmonic respectively, so by definition $\alpha - \alpha' = \overline{\partial}\gamma$ for some γ, and they are both d-harmonic, so $d\overline{\partial}\gamma = 0$, and $\overline{\partial}\gamma$ is g-orthogonal to $\mathcal{H}^k(X, g)$ by Hodge decomposition for $\overline{\partial}$ with metric g, so by Hodge theorem for d with metric g, $\partial\gamma$ is d-exact, so $[\alpha] = [\alpha']$. □

Cor. (12.9.4.2). Betti number $b_r = \sum_{p+q=r} h^{p,q}$, $h^{p,q} = h^{q,p}$. In particular, b_{2k+1} is always even. ⌟

Cor. (12.9.4.3) [Holomorphic Forms on Kähler Manifolds are Closed]. $\mathcal{H}^{p,0}_{\overline{\partial}}(X) = H^0(X, \Omega^p)$. Now a $(p,0)$-form is automatically $\overline{\partial}^*$-closed, so it is $\overline{\partial}$-harmonic iff it is holomorphic. So we conclude any holomorphic p-form on a Kähler manifold is d-closed, even d-harmonic. ⌟

Lemma (12.9.4.4) [$\partial\overline{\partial}$-lemma]. A closed differential form η on a compact Kähler manifold M is d-exact iff it is ∂-exact iff it is $\overline{\partial}$-exact iff it is $\partial\overline{\partial}$-exact. ⌟

Proof: Now $\Delta_d, \Delta_{\overline{\partial}}, \Delta_\partial$ are all the same, By Hodge theorem, it suffice to prove, if a form is orthogonal to $\mathcal{H}^{p,q}(X)$, then it is $\partial\overline{\partial}$-exact(this implies other exactness).

Noe η is d-closed hence ∂ and $\overline{\partial}$-closed, then $\eta = \partial\gamma$ for some γ, and then $\gamma = \overline{\partial}\beta + \overline{\partial}^*\beta' + \beta''$ for β'' harmonic. So $\eta = \partial\overline{\partial}\beta + \partial\overline{\partial}^*\beta'$, and then $\overline{\partial}\eta = \overline{\partial}\overline{\partial}^*\partial\beta = 0$, but then inner product with $\partial\beta$ shows $\overline{\partial}^*\partial\beta = 0$, so $\eta = \partial\overline{\partial}\beta$. □

Cor. (12.9.4.5) [Kodaira-Serre Duality]. By(12.2.4.15), For a Hermitian line bundle over a compact Hermitian complex manifold X, from Hodge theorem and(12.8.5.2), we get

$$H^p(X, \Omega^q(E)) \cong H^{n-p}(X, \Omega^{n-q}(E^*))$$

induced by $\overline{*}_E$ and $\overline{*}_{E^*}$. Moreover, there is a perfect pairing

$$H^p(X, \Omega^q(E)) \times H^{n-p}(X, \Omega^{n-q}(E^*)) \to \mathbb{C}$$

induced by

$$\mathcal{H}^{p,q}(X, E) \times \mathcal{H}^{n-p,n-q}(X, E^*) \to \mathbb{C} : (\alpha, \beta) \mapsto \int_X \alpha \wedge \overline{*}_E \beta$$

In fact, $\int_X \alpha \wedge \overline{*}_E \alpha = ||\alpha||^2 \neq 0$. ⌟

Prop. (12.9.4.6). Holomorphic 1-forms on a compact complex surface is closed.**?** ⌟

Prop. (12.9.4.7) [Hard Lefschetz Theorem]. For a compact Kähler manifold M, the map

$$L^k : H^{n-k}(M) \to H^{n+k}(M)(12.9.3.1)$$

is an isomorphism,(notice it is defined because L commutes with Δ_d(12.9.3.5)).

Define the **primitive cohomology class** $H^{n-k}_{\mathrm{prm}}(M) = \ker(L^{k+1}|_{H^{n-k}})$, then

$$H^m(M) = \oplus_k L^k H^{m-2k}_{\mathrm{prm}}(M).$$

⌟

Proof: Cf.[Griffith/Harris P122], using representation theory of $\mathfrak{sl}_2$. □

Thm. (12.9.4.8) [Hodge-Riemann Bilinear Relation]. Let (X, ω) be a Kähler manifold of dimension n, then for $k \leq n$, we can define a Hermitian form

$$H(\alpha, \beta) = \mathrm{i}^k \int_X \omega^{n-k} \wedge \alpha \wedge \beta = \mathrm{i}^k \langle L^{n-k}\alpha, \beta \rangle$$

on $H^k(X; \mathbb{R})$. Then it satisfies:

- The Hodge decomposition(12.9.4.1) is orthogonal for H.

- If $\alpha \neq 0 \in H^{p,q}_{\text{prm}}(X)$, then

$$i^{p-q-k}(-1)^{\frac{k(k-1)}{2}} H(\alpha) > 0$$

⌟

Proof: Cf.[Griffith/Harris] or [Complex Geometry Daniel P138] or[Hodge Theory, Chap6.3.2]. □

Cor. (12.9.4.9). For a compact Kähler manifold of complex dimension $2m$,

$$\operatorname{sgn}(X) = \sum_{p,q=0}^{m} (-1)^p h^{p,q}(m)$$

⌟

Proof: Cf.[Complex Geometry Daniel P140]. □

Prop. (12.9.4.10)[Hirzebruch-Riemann-Roch]. By(12.2.4.8), for a n-dimensional complex line bundle L over a compact Kähler manifold M,

$$\chi(M, L) = \int_M [\operatorname{ch}(E)\operatorname{td}(T^{1,0}M)]_n.$$

Where $\chi(M, L) = \sum_{q=0}^{n}(-1)^q \dim H^q(M, E)$, ch is the Chern character(12.2.3.5) and $\operatorname{td}(T^{1,0}M)$ is the Todd polynomial, i.e. Taylor expansion of $\prod_{i=1}^{r} \dfrac{t_i}{1-e^{-t_i}}$ in terms of the symmetric polynomial, applied to $c_i(T^{1,0}M)$. ⌟

Cor. (12.9.4.11) [Riemann-Roch]. By(12.2.4.9), for a complex vector bundle E over a Riemann surface M, let $\deg E = \int_M c_1(E)$, then

$$\chi(M, E) = H^0(M, E) - \dim H^1(M, E) = \deg E + \operatorname{rk}(E)(1-g).$$

⌟

Cor. (12.9.4.12). For other examples of corollaries of Hirzebruch-Riemann-Roch theorem, Cf.[Complex Geometry P232]. ⌟

5 Complex Tori

Def. (12.9.5.1) [Complex Tori]. A **complex torus** is a pointed complex manifold isomorphic to the complex manifold V/Λ, where V is a f.d. vector space over $\mathbb{C}$ and Λ is a complete lattice in V. ⌟

Prop. (12.9.5.2). Let $X = V/\Lambda, X' = V'/\Lambda'$ be complex tori, then any $\mathbb{C}$-linear map $\alpha : V \to V'$ s.t. $\alpha(\Lambda) \subset \Lambda'$ defines a holomorphic map $X \to X'$ sending 0 to 0. And any holomorphic map $X \to X'$ sending 0 to 0 is of this form. ⌟

Proof: Any $\varphi : X \to X'$ lifts to a continuous map $\psi : V \to V'$, and it is holomorphic because the morphisms $V \to X, V' \to X'$ are locally biholomorphic, ψ is also holomorphic. For any $\omega \in \Lambda$, $\psi(z+\omega) - \psi(z)$ has value in Λ' for any z, so $\psi(z+\omega) = \psi(z) + a(\omega)$. From here it is easy to see that ψ is linear. □

Def. (12.9.5.3) [Riemann Pairs]. A **Riemann pair** is a pair (Λ, J) where Λ is a finite $\mathbb{Z}$-module of finite rank, and J is a complex structure on $\Lambda \otimes \mathbb{R}$. A homomorphism of Riemann pairs is a group homomorphism $\Lambda \to \Lambda'$ that preserves the complex structure. ⌟

Prop. (12.9.5.4) [Riemann Pairs and Abelian Varieties]. There is an equivalence of the category of Riemann pairs with $\mathcal{A}b\,\mathcal{V}ar\,/\mathbb{C}$ by

$$(\Lambda, J) \mapsto (\Lambda \otimes \mathbb{R})/\Lambda.$$

⌟

Proof: It is fully faithful by(12.9.5.2), and it is clearly essentially surjective. □

Prop. (12.9.5.5) [Cohomology of Complex Tori]. For any complex torus $X = V/\Lambda$, $H_1(X, \mathbb{Z}) \cong \Lambda$, so $H^1(X, \mathbb{Z}) \cong \mathrm{Hom}(\Lambda, \mathbb{Z})$, and by Künneth formula,

$$H^n(X, \mathbb{Z}) \cong \wedge^n H^1(X, \mathbb{Z}) \cong \wedge^n \mathrm{Hom}(\Lambda, \mathbb{Z}).$$

Then

$$H^n(X, \mathbb{C}) \cong \wedge^n \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{C}) \cong \wedge^n(\mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C}) \oplus \mathrm{Hom}_{\mathbb{C}}(\overline{V}, \mathbb{C})) = \bigoplus_{p+q=n} \wedge^p V^* \otimes \wedge^q \overline{V}^*$$

and

$$H_1(X, \mathbb{C}) \cong \Lambda \otimes_{\mathbb{Z}} \mathbb{C} \cong V \otimes_{\mathbb{R}} \mathbb{C} \cong V \otimes \overline{V} = \mathrm{Tgt}_0(X) \oplus \overline{\mathrm{Tgt}_0(X)}.$$

⌟

Cor. (12.9.5.6) [Complex Tori are Kähler]. A complex torus(12.9.5.1) $X = V/\Lambda$ is a Kähler manifold, and $H^2(X, \mathbb{R}) \cong \wedge^2 \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{R})$, by(12.9.5.5). ⌟

Prop. (12.9.5.7) [Hodge Theory of Complex Tori]. Let $X = V/\Lambda$ be a complex torus, as X is Kähler(12.9.5.6), there is a decomposition

$$H^n_{\mathrm{dR}}(X, \mathbb{C}) \cong \bigoplus_{p+q=n} H^q(X, \Omega^p)$$

by(12.9.4.1). Then this decomposition corresponds to the decomposition in(12.9.5.5) via the isomorphism $H^n_{\mathrm{dR}}(X, \mathbb{C}) \cong H^n(X, \mathbb{C})$. In particular, there is a canonical isomorphism

$$H^q(X, \Omega^p) \cong \wedge^p V^* \otimes \wedge^q \overline{V}^*.$$

⌟

Proof: □

Def. (12.9.5.8) [Dual Complex Tori]. Let $X = V/\Lambda$ be a complex torus with a Riemann form, then we can define the **dual complex torus** as

$$X^\vee = V^*/\Lambda^*$$

where $V^* = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$ and $\Lambda^* = \{f \in V^* | f(\Lambda) \subset \mathbb{Z}\}$. ⌟

Riemann Forms

Prop. (12.9.5.9) [Riemann Forms]. For a complex torus V/Λ, it is projective iff there exists a **Riemann form** on V, which is an alternating bilinear form $\omega : V\times V\to\mathbb{R}$ that:

- $\omega(\mathrm{i}\,u,\mathrm{i}\,v)=\omega(u,v)$.
- $\omega(v,\mathrm{i}\,v)>0$ for $v\neq 0$.
- $\omega(u,v)\in\mathbb{Z}$ for $u,v\in\Lambda$.

Notice ω is clearly non-degenerate. ⌟

Proof: Use(12.9.5.6). The conditions are just equivalent to ω being an integral positive Kähler form(12.9.8.6). **?** How to interpret? □

Cor. (12.9.5.10). Notice these conditions are equivalent to the fact the Hermitian form

$$\lambda(x,y)=\omega(\mathrm{i}\,x,y)+\mathrm{i}\,\omega(x,y)$$

is Hermitian and positive definite. ⌟

Proof: □

Cor. (12.9.5.11) [Riemann Relations]. Let $X=V/\Lambda$ be a complex torus of dimension g. Choose a complex basis $e_1,\ldots,e_g$ of V and a $\mathbb{Z}$-basis $u_1,\ldots,u_{2g}$ of Λ. Let $\Pi\in\mathrm{Mat}(n\times 2n,\mathbb{C})$ be the basis of $(u_1,\ldots,u_{2g})$ in $(e_1,\ldots,e_g)$, so $X\cong\mathbb{C}^g/\Pi\mathbb{Z}^{2g}$. Then $X\in\mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/\mathbb{C}$ iff there exists a non-degenerate skew-symmetric matrix $A\in\mathrm{GL}(2g,\mathbb{Z})$ satisfying the **Riemann relations**

$$\Pi A^{-1}\Pi^t=0,\quad \mathrm{i}\,\Pi A^{-1}\overline{\Pi}^t\in\mathrm{Pos}(g,\mathbb{C}).$$

⌟

Proof: By(12.9.5.9), it suffices to show that if ω is the alternating form on Λ corresponding to A, then these two conditions are equivalent to the condition that ω is a Riemann form.

Notice that $E(\Pi x,\Pi y)=x^tAy$ for any $x,y\in\mathbb{R}^{2g}$, and if

$$I=\begin{bmatrix}\Pi\\ \overline{\Pi}\end{bmatrix}^{-1}\begin{bmatrix}\mathrm{i}\,\mathbf{1}&\\&-\mathrm{i}\,\mathbf{1}\end{bmatrix}^{-1}\begin{bmatrix}\Pi\\ \overline{\Pi}\end{bmatrix},$$

then

$$\begin{bmatrix}\Pi\\ \overline{\Pi}\end{bmatrix}I=\mathrm{i}\begin{bmatrix}\Pi\\ -\overline{\Pi}\end{bmatrix},$$

so $\mathrm{i}\,\Pi=\Pi I$. Then $\omega(\mathrm{i}\,u,\mathrm{i}\,v)=\omega(u,v)$ is equivalent to $I^tAI=A$, or equivalently

$$\begin{bmatrix}\mathrm{i}\,\mathbf{1}&\\&-\mathrm{i}\,\mathbf{1}\end{bmatrix}\Big(\begin{bmatrix}\Pi\\ \overline{\Pi}\end{bmatrix}A^{-1}\begin{bmatrix}\Pi\\ \overline{\Pi}\end{bmatrix}^t\Big)^{-1}\begin{bmatrix}\mathrm{i}\,\mathbf{1}&\\&-\mathrm{i}\,\mathbf{1}\end{bmatrix}=\Big(\begin{bmatrix}\Pi\\ \overline{\Pi}\end{bmatrix}A^{-1}\begin{bmatrix}\Pi\\ \overline{\Pi}\end{bmatrix}^t\Big)^{-1}.$$

By comparing blocks, this is equivalent to $\Pi A^{-1}\Pi^t=0$.

And if $x,y\in\mathbb{R}^{2g}$ and $u=\Pi x,v=\Pi y$, using the fact $\Pi A^{-1}\Pi^t=0$,

$$\omega(\mathrm{i}\,u,u)=x^tI^tAx=\begin{bmatrix}u\\ \overline{u}\end{bmatrix}^t\begin{bmatrix}\mathrm{i}\,\mathbf{1}&\\&-\mathrm{i}\,\mathbf{1}\end{bmatrix}\Big(\begin{bmatrix}\Pi\\ \overline{\Pi}\end{bmatrix}A^{-1}\begin{bmatrix}\Pi\\ \overline{\Pi}\end{bmatrix}^t\Big)^{-1}\begin{bmatrix}v\\ \overline{v}\end{bmatrix}$$

$$= \begin{bmatrix} u \\ \overline{u} \end{bmatrix}^t \begin{bmatrix} 0 & \mathrm{i}(\overline{\Pi}A^{-1}\Pi^t)^{-1} \\ \mathrm{i}(\Pi A^{-1}\overline{\Pi}^t)^{-1} & 0 \end{bmatrix} \begin{bmatrix} v \\ \overline{v} \end{bmatrix}$$
$$= \mathrm{i}\, u^t(\overline{\Pi}A^{-1}\Pi^t)^{-1}\overline{v} - \mathrm{i}\,\overline{u}^t(\Pi A^{-1}\overline{\Pi}^t)^{-1}v$$

And because ω is alternating,

$$u^t(\overline{\Pi}A^{-1}\Pi^t)^{-1}\overline{u} + \overline{u}^t(\Pi A^{-1}\overline{\Pi}^t)^{-1}u = 0,$$

so

$$\omega(\mathrm{i}\,u, u) = 2\overline{u}\,\mathrm{i}(\overline{\Pi}A^{-1}\Pi^t)^{-1}\overline{u},$$

and it is positive definite iff $\mathrm{i}\,\Pi A^{-1}\overline{\Pi}^t \in \mathrm{Pos}(n, \mathbb{C})$. □

6 Positivity

Def. (12.9.6.1) [Positive Line Bundle]. A 2-form ω on a Hermitian complex manifold M is called **positive** iff $\omega(u, Ju) \geq 0$ for $u \neq 0 \in TM$, which is equivalent to $-i\omega(v, \overline{v}) > 0$ for all $v \in T^{1,0}X$.

A holomorphic vector bundle is called **(Griffith-)positive** iff there exists a Hermitian metric on it that the curvature form Ω for the Chern connection(12.8.5.13) satisfies $h(\Omega(s), s)(v, \overline{v}) > 0$ for all $s \in E$ and $v \in T^{1,0}X$.

The pullback of a positive line bundle along an immersion is positive. ⌟

Prop. (12.9.6.2) [Positivity on Kähler Manifolds]. On a compact Kähler manifold, being positive is a topological property for line bundles. It is equivalent to the first Chern class of L can be represented by a positive form in $H^2_{dR}(M)$. ⌟

Proof: $c_1(L) = [\frac{i}{2\pi}\Omega]$, so one direction is trivial, and if $c_1(L) = [\frac{i}{2\pi}\theta]$, choose an arbitrary Hermitian metric h on L, then by $\partial\overline{\partial}$-lemma(12.9.4.4), $\theta = \Omega + \overline{\partial}\partial\rho$ for some smooth function ρ. Then $e^\rho h$ has $\Omega = \theta$ by formula(12.8.5.14). □

Cor. (12.9.6.3). On a compact Kähler manifold, if L is positive, then for any other Hermitian line bundle L', $kL + L'$ is positive. ⌟

Prop. (12.9.6.4). The hyperplane line bundle $\mathcal{O}(1)$(12.8.5.9) is positive. ⌟

Proof: The hyperplane line bundle is dual to the tautological line bundle. The metric on the tautological line bundle is given by locally $g_i = \frac{1}{|z_i|^2}\sum |z_i|^2$. It is compatible with the transition map, and then by(12.8.5.14), the Chern curvature is

$$\overline{\partial}\partial(\frac{1}{|z_i|^2}\sum |z_i|^2) = \overline{\partial}\partial(\sum |z_i|^2).$$

So by(12.3.3.6) the curvature of the hyperplane line bundle times i is just the Fubini-Study metric form(12.9.1.6), so it is positive. □

Prop. (12.9.6.5). For $\widetilde{X} \to X$ the blowing-up of X at a point x, If L is a positive line bundle on X, then for any integer n, there exists a $k > 0$ that $\pi^* L^k - nE$ is a positive line bundle on $\widetilde{X}$, where E is the exceptional divisor. ⌟

Proof: Involves explicit metric calculation, Cf.[Kodaira Embedding Theorem P11] and [Complex Geometry P249].. □

7 Kodaira Vanishing Theorem

Prop. (12.9.7.1) [Nakano Identities]. For a holomorphic vector bundle over a compact Kähler manifold (M,ω) with Hermitian metric h, introduce operators L and Λ as before. If we denote the $(1,0)$ and $(0,1)$-part of the Chern connection on E by D' and $D''=\overline{\partial}$, then

$$[\Lambda,\overline{\partial}]=-iD'^*,\quad [\Lambda,D']=i\overline{\partial}^*$$

⌟

Proof: The question is local, choose normal coordinate frame at x(12.8.5.16), then by the formula of Chern connection(12.8.5.14), $\nabla_E=d+A$, $A(x)=0$, and $\nabla_{E^*}=d+B$, $B(x)=0$. so

$$[\Lambda,\overline{\partial}_E]+iD'^*=[\Lambda,\partial]+i\partial^*+[\Lambda,A^{0,1}]+iB^{0,1}$$

where the usual Kähler identities(12.9.3.3) are used. Then it is zero when evaluated at x, Cf.[Demailly Complex Analytic and Differential Geometry P329]. □

Cor. (12.9.7.2) [Bochner-Kodaira-Nakano Identity].

$$\Delta_{\overline{\partial},E}-\Delta_{D',E}=i[\Omega,\Lambda]$$

⌟

Proof:

$$-i\Delta_{D',E}=D'[\Lambda,\overline{\partial}]+[\Lambda,\overline{\partial}]D'=D'\Lambda\overline{\partial}-D'\overline{\partial}\Lambda+\Lambda\overline{\partial}D'-\overline{\partial}\Lambda D'$$

and similar calculation for $i\Delta_{\overline{\partial},E}$, so

$$i\Delta_{\overline{\partial},E}-i\Delta_{D',E}=\Lambda(\overline{\partial}D'+D'\overline{\partial})-(\overline{\partial}D'+D'\overline{\partial})\Lambda=-[\Omega,\Lambda].$$

□

Prop. (12.9.7.3) [Kodaira-Akizuki-Nakano Vanishing Theorem]. If L is a positive line bundle on a compact Kähler manifold M, then

$$H^p(M,\Omega^q(\mathcal{L}))=0$$

for $p+q>n$. In particular, $H^p(M,\mathcal{K}_M\otimes\mathcal{L})=0$ for $p>0$. ⌟

Proof: By Hodge theorem(12.2.4.13), it suffice to prove there are no harmonic (p,q)-forms$\in\mathcal{H}^{p,q}(X,L)$ on L.

As $i\Omega=\omega$ is positive, we may endow M with the metric ω, then by(12.9.7.2) and(12.9.3.2), $\Delta_{\overline{\partial}}-\Delta_{D'}=[L,\Lambda]=p+q-n$ on $A^{p,q}$.

So if $s\in\mathcal{H}^{p,q}(X,L)$, then $(\Delta_{\overline{\partial}}s-\Delta_{D'}s,s)=(p+q-n)||s||^2\geq 0$, but $(\Delta_{\overline{\partial}}s-\Delta_{D'}s,s)=-(\Delta_{D'}s,s)=-||D's||^2-||D'^*s||^2\leq 0$, so $s=0$. □

Cor. (12.9.7.4) [Serre's Theorem]. Let $\mathcal{L}$ be a positive line bundle on a compact complex Kähler manifold M, then for any holomorphic vector bundle $\mathcal{E}$, for m large, $H^q(M,\mathcal{L}^m\otimes\mathcal{E})=0$. ⌟

Proof: Same notation as in the proof of(12.9.7.3), choose Hermitian structure on E and L and their Chern connections by ∇_E, ∇_L, the corresponding Chern connection on $E \otimes L^m$ is denoted by ∇, and make sure $\frac{i}{2\pi}F_{\nabla_L}$ is the Kähler form ω, then for any harmonic form $\alpha \in \mathcal{H}^{p,q}(X, E \otimes L^m)$, by(12.9.7.2), $\frac{i}{2\pi}([\Lambda, F_\nabla](\alpha), \alpha) \geq 0$, but $\frac{i}{2\pi}F_\nabla = \frac{i}{2\pi}F_{\nabla_E} + m\omega$, so

$$0 \leq \frac{i}{2\pi}([\Lambda, F_{\nabla_E}](\alpha), \alpha) + m(n-p-q)||\alpha||^2$$

Notice $|([\Lambda, F_{\nabla_E}](\alpha), \alpha)|$ has a bound by Schwartz inequality, then if $p+q > n$ and m sufficiently large, α must by 0. In this case $\mathcal{H}^{p,q}(X, E\otimes L^m) = 0$, but $\mathcal{H}^{0,q}(X, \mathcal{K}_X \otimes E \otimes L^m) \subset \mathcal{H}^{n,q}(X, E\otimes L^m)$, so it is 0. Now we've proved $H^q(X, \mathcal{K}_X \otimes E \otimes L^m) = 0$ for any E if m is large. But E is arbitrary, so the conclusion is true. □

Cor. (12.9.7.5) [Grothendieck's Lemma]. Every holomorphic vector bundle E over $\mathbb{CP}^1$ is uniquely isomorphic to a finite direct sum of $\mathcal{O}(a_i)$. ⌟

Proof: If E has rank 1, this is the content of(12.8.5.10), so use induction on rank of E. Choose a maximal a that $\mathrm{Hom}(\mathcal{O}(a), E) = H^0(CP^1, E(-a)) \neq 0$. This a exists because Serre's Theorem(12.9.7.4) shows that $H^1(\mathbb{CP}^1, E(-a)) = 0$ for a sufficiently small, and Riemann-Roch(12.2.4.9) shows that $\chi(\mathbb{CP}^1, E(-a)) = \deg E + \mathrm{rk}(E)(1-a)$ is positive for a sufficiently small, so $H^0(CP^1, E(-a)) \neq 0$. Conversely, if a is sufficiently large, then $H^0(\mathbb{CP}^1, E(-a)) \cong H^1(\mathbb{CP}^1, E^*(a-2)) = 0$(Notice $\mathcal{K}_{\mathbb{CP}^n} = \mathcal{O}(-n-1)$).

So now there is an exact sequence of sheaves

$$0 \to \mathcal{O}(a) \xrightarrow{s} E \to E_1 \to 0$$

I claim E_1 is also a vector bundle, because s never vanishes, otherwise if it vanish at some x, then we can divide by a linear factor $s_x \in H^0(\mathbb{CP}^1, \mathcal{O}(1))$ to get a map $\mathcal{O}(a+1) \to E$, contradicting the maximality. So by induction $E_1 = \oplus\mathcal{O}(a_i)$, then I claim $a_i \leq a$, because otherwise $H^0(\mathbb{CP}^1, E_1(-a-1)) \neq 0$, and by the exact sequence $0 \to \mathcal{O}(-1) \to E(-a-1) \to E_1(-a-1) \to 0$, $H^0(\mathbb{CP}^1, E(-a-1)) \neq 0$, contradiction.

Then we want to show the above sequence splits, this is equivalent to

$$0 \to E_1^*(a) \to E^*(a) \to \mathcal{O} \to 0$$

splits, and his follows from the fact $H^1(\mathbb{CP}^1, E_1^*(a)) = H^1(\mathbb{CP}^1, \oplus\mathcal{O}(a-a_i)) = 0$, by Serre duality. So there is a section lifting $\mathcal{O} \to E^*(a)$, which splits the sequence. □

Prop. (12.9.7.6) [Weak Lefschetz Theorem]. Let X be a compact Kähler manifold and Y be a submanifold that the line bundle $\mathcal{L}(Y)$ is positive, then the canonical restriction map $H^k(X, \mathbb{C}) \to H^k(Y, \mathbb{C})$ is isomorphism for $k \leq n-2$ and injective for $k = n-1$. ⌟

Proof: In fact, using Hodge decomposition, it suffices to prove on the level of $H^q(X, \Omega_X^p)$. Tensoring the exact sequence

$$0 \to \mathcal{O}_X(-Y) \to \mathcal{O}_X \to i_* i_Y^* O_X \to 0$$

with Ω_X^p and taking the cohomology. By Serre duality and Kodaira vanishing(12.9.7.3), the map $H^q(X, \Omega_X^p) \to H^q(X, \Omega^p i_* i_Y^* O_X)$ is isomorphism for $p+q < n-1$ and injection for $p+q = n-1$.

Next consider the exact sequence $0 \to TY \to TX \to \mathcal{N}_{Y/X} \to 0$. By(6.5.1.26) there is an exact sequence

$$0 \to \wedge^p TY \to \wedge^p TX|_Y \to \wedge^{q-1} TY \mathcal{N}_{Y/X} \to 0$$

Taking dual and applying adjunction formula(12.8.1.3), it becomes:

$$0 \to \Omega_Y^{q-1} \otimes \mathcal{O}(-N) \to \Omega_X^q|Y \to \Omega_Y^q \to 0$$

Taking cohomology and use Serre duality and Kodaira vanishing as before, the result follows, and the composition is also true. □

Remark (12.9.7.7). There is a topological proof of weak Lefschetz theorem in [Bott, On a Theorem of Lefschetz]. ⌟

8 Kodaira Embedding

Prop. (12.9.8.1)[Kodaira map]. For a holomorphic line bundle L on a compact complex manifold M, if $s_0, \ldots, s_n$ be a basis of $H^0(X, L)$, we try to define a map from M to $\mathbb{CP}^n : x \to [s_0(x), \ldots, s_n(x)]$. This is independent of the change of coordinates because $g_{\alpha\beta}$ is invertible, and it is definable iff L is basepoint-free. This map is holomorphic where it is definable. ⌟

Def. (12.9.8.2) [Ample Holomorphic Line Bundles]. A holomorphic line bundle $\mathcal{L}$ on a compact complex manifold X is called a

- **semi-ample holomorphic line bundle** iff for m large, $\mathcal{L}^m$ is basepoint-free.
- **very ample holomorphic line bundle** iff L is basepoint-free and the Kodaira map $\iota_L : X \to \mathbb{CP}^N$ is a holomorphic embedding.
- **ample holomorphism line bundle** iff for m large, L^m is very ample.

⌟

Lemma (12.9.8.3) [Cohomological Method for Very Ampleness]. For the above Kodaira map to be a holomorphic embedding, it suffice to show that the map is definable, injective and surjective on cotangent space. For these, it is equivalent to $H^0(X, L) \to L_x$ surjective, $H^0(X, L) \to L_x \oplus L_y$ surjective, and $L \otimes \mathcal{I}_x \to L_x \otimes T^{1,0*}(X)_x$ surjective. And they are true if

$$H^1(X, L \otimes \mathcal{I}_x) = 0, \quad H^1(X, L \otimes \mathcal{I}_{x,y}) = 0, \quad H^1(X, L \otimes \mathcal{I}_x^2) = 0.$$

respectively. ⌟

Proof: Basepoint-free at x is easily seen to be equivalent to $H^0(X, L) \to L_x$ surjective. And there is an exact sequence of sheaves:

$$0 \to L \otimes \mathcal{I}_x \to L \to L_x \to 0$$

where L_x means the skyscraper sheaf. So $H^1(X, L \otimes \mathcal{I}_x^2) = 0$ induces the result.

Injective is easily seen to be equivalent to $H^0(X, L) \to L_x \oplus L_y$ surjective. And there is an exact sequence of sheaves:

$$0 \to L \otimes \mathcal{I}_{x,y} \to L \to L_x \oplus L_y \to 0$$

where $\mathcal{I}_{x,y}$ is the sheave of functions vanishing at x and y, and $L_x \oplus L_y$ means the skyscraper sheaf. So $H^1(X, L \otimes \mathcal{I}_{x,y}) = 0$ induces the result.

For the surjection on cotangent spaces, given any point x, choose a basis $s_1, \ldots, s_n$ of sections in $H^0(X, L)$ vanishing at x, and by basepoint-free, there is a s_0 not vanishing at x, then on a coordinate, the Kodaira map is given by $x \to (s_1/s_0, \ldots, s_n/s_0)$, then it need to be checked $d_x(s_i/s_0) = d_x(x_i)/s_0$ span $T^{1,0*}(X)_x$. But there are exact sequences of sheaves:

$$0 \to L \otimes \mathcal{I}_x^2 \to L \otimes \mathcal{I}_x \xrightarrow{d_x} L_x \otimes T_x^{1,0*} \to 0$$

where d_x is given by $d_x(s\otimes f)=s(x)\otimes d_x(f)$(by the universal property of skyscraper sheaf), it suffice to give a map $(L\otimes\mathcal{I}_x\to L_x\otimes T_x^{1,0*})$, notice this is independent of the coordinate because $d_x(s_\alpha)=d_x(g_{\alpha\beta}s_\beta)=g_{\alpha\beta}d_x(s_\beta)$, as s_α vanishes at x, so this is truly a sheaf map, and its kernel is $L\otimes\mathcal{I}_x^2$. So $H^1(X,L\otimes\mathcal{I}_x^2)=0$ induces the result. □

Prop. (12.9.8.4) [Ampleness and Positivity]. A holomorphic line bundle $\mathcal{L}$ on a compact Kähler manifold is ample iff it is positive. ⌟

Proof: If L is ample, then L^m is the pullback of the hyperplane bundle by the Kodaira map. The hyperplane line bundle is positive by(12.9.6.4), so L^m is positive with the induced metric, so L is also positive given the m-th roots of the induced metric (notice the metric of line bundle is just locally a number compatible with transition map).

Conversely, using(12.9.8.3), we want to find a L^k that $H^1(X,L^k\otimes\mathcal{I}_x)=0, H^1(X,L^k\otimes\mathcal{I}_{x,y})=0, H^1(X,L^k\otimes\mathcal{I}_x^2)=0$. First notice it suffice to prove for single points when k is sufficiently large, because the holomorphic embedding is an open property and X is compact so a sufficiently large k will suffice.

Consider the blowing-up $\widetilde{X}$ at a point x, there is a commutative diagram

$$\begin{array}{ccc} H^0(X,L^k) & \longrightarrow & L_x^k \\ \downarrow{\scriptstyle \pi^*} & & \downarrow{\scriptstyle \cong} \\ H^0(\widetilde{X},\pi^*L^k\otimes L_x^k) & \longrightarrow & H^0(E,\mathcal{O}_E)\otimes L_x^k \end{array}$$

The right vertical map is isomorphism as $E\cong\mathbb{CP}^n$, so $H^0(E,\mathcal{O}_E)=\mathbb{C}$. The left exact sequence is also isomorphism: it is injective because π is surjective, and it is surjective because: if $\dim X=1$, then $\pi=\mathrm{id}$ so trivially true, and if $\dim X\geq 2$, then because $\pi:\widetilde{X}-E\cong X-\{x\}$, any holomorphic function on $\widetilde{X}$ induces a holomorphic function on $X-\{x\}$ and by Hartog's theorem(11.5.6.3), it comes from a holomorphic function on X.

Now the second horizontal line is part of the cohomology exact sequence of(6.5.3.15)

$$0\to\pi^*L^k\otimes\mathcal{O}_{\widetilde{X}}(-E)\to\pi^*L^k\to\pi^*L^k|_E\to 0$$

So it is reduced to prove $H^1(\widetilde{X},\pi^*L^k\otimes\mathcal{O}(-E))=0$, but by(6.8.2.8), $\pi^*L^k-E=\pi^*L^k-E+\mathcal{K}_{\widetilde{X}}-\pi^*\mathcal{K}_X-(n-1)E=\mathcal{K}_{\widetilde{X}}+(\pi^*L^k-E)+\pi^*(L^k-\mathcal{K}_X)$, and by(12.9.6.5)(12.9.6.3) the last two are positive when k is large, so the conclusion follows from Kodaira vanishing(12.9.7.3).

The proof of $H^1(X,L^k\otimes\mathcal{I}_{x,y})=0$ is verbatim, just use blowing-up at two different points.

To prove $H^1(X,L^k\otimes\mathcal{I}_x^2)=0$, consider the blowing-up $\widetilde{X}$ at a point x, notice there is a commutative diagram

$$\begin{array}{ccc} H^0(X,L^k\otimes\mathcal{I}_x) & \xrightarrow{d_x} & L_x^k\otimes T^{1,0*}X_x \\ \downarrow{\scriptstyle \pi^*} & & \downarrow{\scriptstyle \cong} \\ H^0(\widetilde{X},\pi^*L^k-E) & \longrightarrow & L_x^k\otimes H^0(E,-E) \end{array}$$

In fact this comes from the two commuting exact sequences twisted with π^*L^k:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \pi^*\mathcal{I}_x^2 & \longrightarrow & \pi^*\mathcal{I}_x & \xrightarrow{d_x} & \pi^*T^{1,0*}X_x & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{O}(-2E) & \longrightarrow & \mathcal{O}(-E) & \longrightarrow & \mathcal{O}_E(-E) & \longrightarrow & 0 \end{array}$$

The second line is(6.5.3.15) and the fact a section vanishing at x lifts to a section vanishing at E thus equivalent to a section in the twisted sheaf $-\otimes\mathcal{O}(-E)$. These two exact sequences commutes because

Back to the commutative diagram, the above argument also shows that the first vertical map is isomorphism. To show the second vertical map is isomorphism, notice by(6.8.2.7) $\mathcal{O}(-E)$ is just the hyperplane line bundle on E, so $H^0(E,-E)\cong T^{1,0*}X_x$, we need to know the vertical map is the natural map $V^*\to H^0(\mathbb{P}(V),\mathcal{O}(1))$. This in fact need some careful calculation using coordinates in(6.8.2.7).**?**

Now the map d_x is surjective iff the second horizontal map is surjective, with is part of the cohomology exact sequence of

$$0\to\pi^*L^k\otimes\mathcal{O}_{\widetilde{X}}(-2E)\to\pi^*L^k\mathcal{O}_{\widetilde{X}}(-E)\to\pi^*L^k|_E\to 0$$

So it is reduced to prove $H^1(\widetilde{X},\pi^*L^k\otimes\mathcal{O}(-wE))=0$, which is by Kodaira vanishing theorem the same reason as before. □

Cor. (12.9.8.5) [Kodaira Embedding Theorem]. If a compact complex manifold M has a positive line bundle, then it is projective. ⌟

Def. (12.9.8.6) [Hodge Manifolds]. A compact Kähler manifold X is projective iff it has a closed positive $(1,1)$-form ω whose cohomology class $[\omega]$ is rational(resp. integral)(i.e. in $H^2(X,\mathbb{Q})$(resp. $H^2(X,\mathbb{Z})$)). In fact, a compact Kähler manifold with a Hodge metric is called a **Hodge manifold**. A pair $(X,[\omega])$ where X is a compact Kähler manifold and $[\omega]\in H^2(X,\mathbb{Z})$ is called a **polarized manifold**.

So compact Hodge manifolds are just those compact Kähler manifolds together with an ample line bundle class. ⌟

Proof: if ω is rational, then a multiple of it is integral, then there is a L that $c_1(L)=k[\omega]$ by Lefschetz theorem on $(1,1)$-forms(12.10.2.6), so L is positive by(12.9.6.2), which is equivalent to ampleness by(12.9.8.4), so X is projective. Conversely, the Chern class of the pullback of the hyperplane line bundle is positive and rational(12.9.6.4)(12.10.2.6). □

Cor. (12.9.8.7) [Compact Riemann Surfaces are Hodge Manifolds]. A **Riemann surface** is a complex variety of dimension 1. Any compact Riemann surface is a compact Hodge manifold. ⌟

Proof: This is because $H^2(X,\mathbb{C})=H^2(X,\mathbb{Q})\otimes_{\mathbb{Q}}\mathbb{C}\cong\mathbb{C}$ is generated by the metric form ω, so there must be a multiple of ω that is integral. □

Cor. (12.9.8.8). if $\widetilde{X}$ is the blowing-up of a Kähler manifold X at a point x, then if X is projective, then $\widetilde{X}$ is also projective, because by(12.9.6.5) $\pi^*L^k\backslash E$ is positive for k large. ⌟

Cor. (12.9.8.9). For a finite unbranched cover of compact Kähler manifolds $\widetilde{X}\to X$, $\widetilde{X}$ is projective iff X is projective. ⌟

Proof: A positive rational closed $(1,1)$-form on X pull backs to a positive rational closed $(1,1)$-form on $\widetilde{X}$, and it can even be pulled forward: $\omega'=\sum_{y\in\pi^{-1}(x)}(\pi^{-1})^*\omega(y)$, then it is also positive closed. It is rational because $\int_X\omega'\wedge\eta=\frac{1}{d}\int_{X'}\omega\wedge\pi^*\eta$, where $\widetilde{X}\to X$ is branched of degree d. □

Def. (12.9.8.10)[the Kähler Cone]. For a Kähler manifold X, the **Kähler cone** K_X is defined to be the set of closed real positive $(1,1)$-forms. Then K_X is an open convex cone in $H^{1,1}(X)\cap H^2(X,\mathbb{R})$. Then(12.9.8.6) says X is projective iff $K_X\cap H^2(X,\mathbb{Z})\neq 0$. ⌟

9 Fujiki Manifolds

12.10 Hodge Theory

1 Hodge-Structures

Cf.[Huy05]Chap3.A, [Hodge 1, 2, 3, Deligne] and [Shimura Varieties, Milne].

Def. (12.10.1.1) [Mixed Hodge Structures]. An integral **mixed Hodge structure** is given by a f.g. Abelian group Λ together with

- An increasing **weight filtration** $W_\bullet$ of $\Lambda_{\mathbb{Q}}$.
- A decreasing **Hodge decomposition** $F^\bullet$ of $\Lambda_{\mathbb{C}}$.
- A bigradation $V^{\bullet,\bullet}$ of $\Lambda_{\mathbb{C}}$.

such that

- For any $k\in\mathbb{Z}$, $W_k\otimes\mathbb{C}=\bigoplus_{p+q\geq k}V^{p,q}$.
- For any $p\in\mathbb{Z}$, $F^p=\bigoplus_{r\geq p}V^{r,s}$.
- $\overline{V^{p,q}}=V^{q,p}$.

⌟

Prop. (12.10.1.2). For any subring $Q\subset\mathbb{R}$, we can naturally define morphisms between Q-mixed Hodge structures. Then integral Hodge structures form an Abelian category, denoted by $m\,\mathrm{Hdg}_Q$.

And it is easy to define tensor products of mixed integral Hodge structures. ⌟

Proof: Cf.[Theorie de Hodge, Deligne]. □

Def. (12.10.1.3) [Integral Hodge Structures]. For $k\in\mathbb{Z}$, an integral **Hodge structure** of weight k is a mixed Hodge structure pure of weight k.

Equivalently, it is a a f.g. free Abelian group Λ together with a **Hodge decomposition** of graded C-vector spaces

$$\Lambda_{\mathbb{C}}=\bigoplus_{p+q=k}V^{p,q}$$

satisfying $\overline{V^{p,q}}=V^{q,p}$.

This is because given an integral Hodge structure of weight k, we can associate a **Hodge filtration** $F^\bullet V:F^pV=\bigoplus_{r\geq p}V^{r,k-r}$. It satisfies

$$V_{\mathbb{C}}=F^p\Lambda\bigoplus\overline{F^{k-p+1}\Lambda}$$

for any p, and for any $p+q=k$,

$$V^{p,q}=F^p\Lambda\bigcap\overline{F^q\Lambda}.$$

Thus giving the Hodge decomposition is equivalent to giving the Hodge filtration. ⌟

Prop. (12.10.1.4) [Hodge Structure as Representations of Deligne Torus]. Giving a real representation $h:\mathbb{S}\to\mathrm{GL}(V)$(6.1.5.33) is equivalent to giving a bigradation $V^{p,q}$ of $V_{\mathbb{C}}$ s.t. $\overline{V^{p,q}}=V^{q,p}$, thus equivalent to a real Hodge structure.

And in this correspondence, V is pure of weight n iff $h\circ w:\mathbb{G}_m\to\mathrm{GL}(V)$ acts as character $z\mapsto z^n$.

Then for any subring $Q\subset\mathbb{R}$, this defines an equivalence of categories: $\mathrm{Rep}_Q(\mathbb{S})\cong\mathrm{Hdg}_Q$. ⌟

Proof: We use Galois descent and(6.1.5.33): A bigradation is equivalent to a homomorphism

$$\mathbb{S}_{\mathbb{C}} \cong \mathbb{G}_m \times \mathbb{G}_m \to \mathrm{GL}(V_{\mathbb{C}})$$

where $z \mapsto z^{-p}\overline{z}^{-q}$ on $V^{p,q}$. And this homomorphism descends to a representation $\mathbb{S} \to \mathrm{GL}(V)$ iff $\overline{V^{p,q}} = V^{q,p}$. □

Def. (12.10.1.5) [Weil Operators]. Given a Hodge structure (V, h), the **Weil operator** is defined to be the real homomorphism $C = h(\mathrm{i})$. Equivalently, C acts by i^{q-p} on $V^{p,q}$. ⌟

Def. (12.10.1.6) [Tate Hodge Structure]. A **Tate Hodge Structure** is the Hodge structure $\mathbb{Z}(1)$ pure of type $(-1,-1)$ s.t.

$$\mathbb{Z}(1) = 2\pi\,\mathrm{i}\,\mathbb{Z} \subset \mathbb{Z}(1)_{\mathbb{C}} \cong \mathbb{C}.$$

Also denote $\mathbb{Z}(n) = \mathbb{Z}(1)^{\otimes n}$. In the correspondence(12.10.1.4), $\mathbb{Z}(n)$ correspond to the representation

$$\mathbb{S} \to \mathbb{G}_m : z \mapsto (z\overline{z})^m.$$

In particular, the Weil operator is identity on a Tate Hodge structure. ⌟

Prop. (12.10.1.7) [Hodge Structures of Type $(-1,0),(0,-1)$]. A Hodge structure of type $(-1,0),(0,-1)$ is equivalent to a complex vector space. And the Weil operator is just acting by i. ⌟

Proof: This follows from(3.5.9.2). □

Polarizations

Def. (12.10.1.8) [Hodge Tensors]. For $(V, h) \in Q\text{-Hdg}^n$, an r-**Hodge tensor** is a map of Q-Hodge-structures

$$T : V^{\otimes r} \to Q(-nr/2).$$

In particular, $T(C_V v_1, \ldots, C_V v_r) = T(v_1, \ldots, v_r)$. ⌟

Def. (12.10.1.9) [Polarizations]. For $(V, h) \in Q\text{-Hdg}^n$, an r-**Hodge polarization** is a Hodge tensor $\psi : V \times V \to Q(-n)$ s.t.

$$\psi_C(u, v) = (2\pi\,\mathrm{i})^n \psi(u, Cv)$$

is symmetric and positive-definite. In particular,

$$\psi(u, v) = \psi(Cu, Cv) = (-1)^n \psi(v, u).$$

⌟

Def. (12.10.1.10) [Polarizations]. **?** An integral **polarized Hodge structure** of weight $k \in \mathbb{Z}$ is given by a Hodge structure $(\Lambda, F^p\Lambda)$ of weight k together with a Hermitian form H s.t.

- The Hodge decomposition is orthogonal for H.
- If $\alpha \neq 0 \in H^{p,q}(X)$, then

$$\mathrm{i}^{p-q-k}(-1)^{\frac{k(k-1)}{2}} H(\alpha) > 0$$

⌟

Example (12.10.1.11) [Complex Spaces and Hermitian Forms]. For a complex vector space (V,J), a polarization on V is equivalent to a Hermitian form.? ⌟

Example (12.10.1.12) [Smooth Projective Varieties]. If $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}\mathcal{V}\mathrm{ar}/\mathbb{C}$, then any embedding $X \hookrightarrow \mathbb{P}^n_{\mathbb{C}}$ induces a polarized rational Hodge structure on the primitive part of $H^n(X,\mathbb{Q})$ for each n, by the Hodge index theorem? ⌟

Proof: Cf.[Voison]Thm6.3.2.. □

Example (12.10.1.13) [Complex Abelian Varieties]. By Riemann theorem(12.9.5.9) and(12.10.1.11), for any $n \in \mathbb{Z}_+$, there is an equivalence of categories: $\mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}^{\mathrm{polar}}/\mathbb{C} \cong$ int-Hdg$^{-1,\mathrm{polar}}$. ⌟

Def. (12.10.1.14)[K-Hodge-deRham Structures]. For a subfield $\iota: K \subset \mathbb{C}$, a **$K$-Hodge-deRham structure** is a 4-tuple $V = (V_{\mathbb{Q}}, V_K, u, (V^{p,q})_{p,q\in\mathbb{Z}})$ where

- $V_{\mathbb{Q}} \in \mathcal{V}\mathrm{ect}_{\mathbb{Q}}$, $V_K \in \mathcal{V}\mathrm{ect}_K$,
- u is an isomorphism
$$u : V_K \otimes_K \mathbb{C} \cong V_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{C},$$
endowing $V_K \otimes_K \mathbb{C}$ with a real structure,
- $(V_{p,q})$ is a finite disjoint family of $\mathbb{R}$-subspaces of $V_K \otimes_K \mathbb{C}$ s.t.
$$V_K \otimes_K \mathbb{C} = \bigoplus_{p,q} V^{p,q}, \overline{V^{p,q}} = V^{q,p}$$

and for $i \in \mathbb{Z}$, V is called **pure of weight** i iff $V^{p,q} = 0$ unless $p + q = i$. ⌟

Def. (12.10.1.15) [Primitive Parts]. ⌟

Def. (12.10.1.16) [Hodge Classes]. For $\Lambda \in$ int-Hdg^{2p}, define the **Hodge classes** of degree $2p$ to be
$$\mathrm{Hdg}^{2p}(\Lambda) \triangleq \Lambda \cap V^{p,p} = \ker(\Lambda \to \Lambda_{\mathbb{C}}/F^pV).$$

⌟

Def. (12.10.1.17). ⌟

Variations of Hodge Structures

Mumford-Tate Groups

Def. (12.10.1.18) [Mumford-Tate Groups]. ⌟

Prop. (12.10.1.19). The Mumford-Tate group of a polarizable Hodge structure is a reductive group. ⌟

Proof: Cf.[Ngo]P32. □

2 Abel-Jacobi Maps

Intermediate Jacobians

Def. (12.10.2.1) [Intermediate Jacobians]. For any integral Hodge structure of weight $2k-1$, we can define

$$J^{2k-1}(\Lambda) = \Lambda_{\mathbb{C}}/(F^k\Lambda \oplus H^{2k-1}(X,\mathbb{Z})).$$

This is a complex torus. ⌟

Proof: We have a decomposition

$$\Lambda_{\mathbb{C}} = F^k\Lambda \oplus \overline{F^k\Lambda},$$

so $F^k\Lambda \cap \Lambda_{\mathbb{R}} = \{0\}$, thus the map

$$\Lambda_{\mathbb{R}} \to \Lambda_{\mathbb{C}}/F^k\Lambda$$

is an isomorphism of $\mathbb{R}$-vector spaces. □

Prop. (12.10.2.2). If $(\Lambda, F^\bullet\Lambda) \to (\Lambda', F^\bullet\Lambda')$ is a morphism of Hodge-structure of bidegree (r,r), then it induces a morphism of complex tori

$$J^{2p-1}(\Lambda) \to J^{2(p+r)-1}(\Lambda').$$

⌟

Def. (12.10.2.3) [Jacobian and Albanese Varieties]. If X is a compact Kähler manifold of dimension n, then $J^1(X)$ is also denoted by $\mathrm{Jac}(X)$, called the **Jacobian variety of** X, and $J^{2n-1}(X)$ is denoted by $\mathrm{Alb}(X)$, called the **Albanese variety** of X. ⌟

Prop. (12.10.2.4) [Jacobian]. The **Jacobian** $\mathrm{Jac}(X)$ of a compact Kähler manifold X is defined to be $H^1(X,\mathcal{O}_X)/H^1(X,\mathbb{Z})$, so it is a complex torus of dimension $b_1(X)$ by(12.10.2.1), it is also the kernel of the first Chern class map by the long exact seqence(12.8.5.8), i.e.

$$0 \to \mathrm{Jac}(X) \to \mathrm{Pic}(X) \xrightarrow{c} \mathrm{NS}(X) \to 0$$

⌟

Lemma (12.10.2.5). if X is compact Kähler , then the natural map $H^k(X,\mathbb{C}) \to H^k(X,\mathcal{O}_X)$ is just the projection onto the $(0,k)$-part. In particular, the image is in $H^{0,k}(X)$. ⌟

Proof: By Hodge decomposition, the definition of Dolbeault cohomology and the commutative diagram

$$\begin{array}{ccccccc} \mathbb{C} & \longrightarrow & \mathcal{A}^0(X) & \xrightarrow{d} & \mathcal{A}^1(X) & \xrightarrow{d} & \mathcal{A}^2(X)\ldots \\ \downarrow & & \downarrow = & & \downarrow \pi_{0,1} & & \downarrow \pi_{0,2} \\ \mathcal{O}_X & \longrightarrow & \mathcal{A}^0(X) & \xrightarrow{\bar\partial} & \mathcal{A}^1(X) & \xrightarrow{\bar\partial} & \mathcal{A}^2(X)\ldots \end{array}$$

□

Prop. (12.10.2.6) [Lefschetz theorem on $(1,1)$-forms]. By(12.8.5.8), the image of $\mathrm{Pic}_{\mathbb{C}}(X) \to H^2(X,\mathbb{Z})$ is trivial in $H^2(X,\mathcal{O}_X)$. And if X is compact Kähler , there is Hodge decomposition(12.9.4.1) $H^2(X,\mathcal{O}_X) = H^{2,0}(X) \oplus H^{1,1}(X) \oplus H^{0,2}(X)$.

So the image of $\mathrm{Pic}_{\mathbb{C}}(X)$ is contained in $H^{1,1}(X,\mathbb{Z}) = H^2(X,\mathbb{Z}) \cap H^{1,1}(X)$ by(12.10.2.5) and daulity. Then it is also surjective, this is to say, $\mathrm{NS}(X) = H^{1,1}(X)$ ⌟

Proof: Because by the long exact sequence of(12.8.5.8) and(12.10.2.5) again, an $\alpha \in H^2(X,\mathbb{C})$ is in $H^{1,1}(X,\mathbb{Z})$ iff α is in the image of $\mathrm{Pic}_{\mathbb{C}}(X) \to H^{1,1}(X,\mathbb{Z})$. □

Abel-Jacobi Maps

Def. (12.10.2.7) [Abel-Jacobi Map]. For any $k \in \mathbb{Z}_+$, there is an **Abel-Jacobi map**

$$\Phi_X^k : Z^k(X)_{\text{hom}} \to J^{2k-1}(X).$$

⌟

Proof: Cf.[Voison, P292].**?** □

Thm. (12.10.2.8) [Griffith1968]. Let X is a compact Kähler manifold, Y be a connected complex manifold and $y_0 \in Y$, $Z \subset Y \times X$ a cycle of codimension k s.t. each component Z_i of Z is smooth and the projection $Z_i \to Y$ is a submersion. Then the map

$$Y \to J^{2k-1}(X) : y \mapsto \Phi_X^k(Z_y - Z_{y_0})$$

is holomorphic. ⌟

Proof: Cf.[Voison, P294].**?** □

Def. (12.10.2.9) [Albanese Maps]. Fix a base point x_0 of X, by Griffith's theorem(12.10.2.8) applied to $\Delta \subset X \times X$, we get an **Albanese map**

$$\text{Alb}_X : X \to \text{Alb}(X) : x \mapsto \Phi_X^{2n-1}(x - x_0)$$

that is holomorphic and functorial in (X, x_0). ⌟

Prop. (12.10.2.10). if T is a torus, then the Albanese map $\text{Alb}_T : T \to \text{Alb}(T)$ is an isomorphism. ⌟

Proof: □

Prop. (12.10.2.11) [Universal Properties]. The Albanese map satisfies the following universal property: Any complex torus T and a map $f : X \to T$ s.t. $f(x_0) = 0$ factors through the Albanese map. ⌟

Proof:

□

Lemma (12.10.2.12). For $k \in \mathbb{Z}_+$ sufficiently large,

$$\text{Alb}^k : X^k \to \text{Alb}(X)$$

is surjective. ⌟

Proof: Cf.[Voison, P298].**?** □

Prop. (12.10.2.13). If $X \in \mathcal{S}\text{m}\mathcal{P}\text{roj}/\mathbb{C}$, then $\text{Alb}(X) \in \mathcal{A}\text{b}\,\mathcal{V}\text{ar}/\mathbb{C}$. ⌟

Proof: Cf.[Voison, P300].**?** The factorized map is

$$g : \text{Alb}(X) = H^0(X, \Omega_X)^*/H_1(X, \mathbb{Z}) \to T = H^0(T, \Omega_T)^*/H_1(T, \mathbb{Z}).$$

□

3 Deligne Cohomology

Cf.[Voisin1, 2] and [Esnault-Viehweg, Deligne-Beilinson Cohomology].

Def. (12.10.3.1) [Deligne Complex]. Let X be a complex manifold and $p \in \mathbb{Z}_+$, the (real)**Deligne complex** $\mathbb{R}_{\mathrm{Del}}(p)$ is the complex

$$0 \to \mathbb{R}[0] \xrightarrow{(2\pi\,\mathrm{i})^p} \mathcal{O}_X \xrightarrow{d} \Omega_X \xrightarrow{d} \ldots \xrightarrow{d} \Omega_X^{p-1} \to 0.$$

Similarly we can define the Deligne complex with coefficients in A for any ring $A \subset \mathbb{R}$. ⌟

Def. (12.10.3.2) [Deligne Cohomologies]. Let X be a complex manifold and $p \in \mathbb{Z}, k \in \mathbb{N}$, the **Deligne cohomology** $H^k_{\mathrm{Del}}(X, \mathbb{R}(p))$ is defined to be the hypercohomology $\mathbb{H}^k(X, \mathbb{R}_{\mathrm{Del}}(p))$(12.10.3.1). Similarly we can define the Deligne cohomology with coefficients in A for any ring $A \subset \mathbb{R}$. ⌟

Example (12.10.3.3). For $p = 1$, $\mathbb{Z}_{\mathrm{Del}}(1)$ is quasi-isomorphic to $\mathcal{O}_X^*[-1]$, so $H^{k+1}_{\mathrm{Del}}(X, \mathbb{Z}(1)) \cong H^k(X, \mathcal{O}_X^*)$.

For $p = 2$, there is a quasi-isomorphism

$$\begin{array}{ccccc} (2\pi\,\mathrm{i})^2\mathbb{Z} & \longrightarrow & \mathcal{O}_X & \longrightarrow & \Omega_X^1 \\ & & \downarrow{\scriptstyle \exp((2\pi\,\mathrm{i})^{-1}(-))} & & \downarrow{\scriptstyle (2\pi\,\mathrm{i})^{-1}} \\ & & \mathcal{O}_X^* & \xrightarrow{f \mapsto \mathrm{dlog}(f)} & \Omega_X^1 \end{array},$$

so $H^1_{\mathrm{Del}}(X, \mathbb{Z}(2)) = \mathbb{C}^\times$, and $H^2_{\mathrm{Del}}(X, \mathbb{Z}(2))$ corresponds to holomorphic line bundles with a holomorphic connection. ⌟

Prop. (12.10.3.4). If X is a compact Kähler manifold and $A \subset \mathbb{R}$, then there is a long exact sequence

$$\ldots \to H^k_{\mathrm{Del}}(X, A(p)) \to H^k(X, A) \to H^k(X, \mathbb{C})/\operatorname{Fil}^p H^k(X, \mathbb{C}) \to H^{k+1}_{\mathrm{Del}}(X, A(p)) \to \ldots$$

⌟

Proof: There is an exact sequence of complexes

$$0 \to \Omega_X^{\leq p-1}[-1] \to A_{\mathrm{Del}}(p) \to A(p) \to 0,$$

which induces a long exact sequence

$$\ldots \to H^k_{\mathrm{Del}}(X, A(p)) \to H^k(X, A(p)) \to \mathbb{H}^k(X, \Omega_X^{\leq p-1}) \to H^{k+1}_{\mathrm{Del}}(X, A(p)) \to \ldots.$$

And the exact sequence of complexes

$$0 \to \Omega_X^{\geq p} \to \Omega_X^{\bullet} \to \Omega_X^{\leq p-1} \to 0$$

and the fact $\mathbb{H}^k(X, \Omega_X^{\geq p}) \cong \operatorname{Fil}^p H^k(X, \mathbb{C}) \subset H^k(X, \mathbb{C})$**?** implies that $\mathbb{H}^k(X, \Omega_X^{\leq p-1}) \cong H^k(X, \mathbb{C})/F^p H^k(X, \mathbb{C})$. □

Cor. (12.10.3.5). There is an exact sequence

$$0 \to J^{2p-1}(X) \to H^{2p}_{\mathrm{Del}}(X, \mathbb{Z}(p)) \to \mathrm{Hdg}^{2p}(X, \mathbb{Z}) \to 0.\text{(12.10.2.1)(12.10.1.16)}$$

⌟

Prop. (12.10.3.6). Let X be compact Kähler of dimension p and $i < 2p$, then

$$H^i(X, \mathbb{R}(i)) \hookrightarrow H^k(X, \mathbb{C})/\operatorname{Fil}^p H^k(X, \mathbb{C}).$$

So there are exact sequences

$$0 \to H^{i-1}(X, \mathbb{R}(p)) \to H^{i-1}(X, \mathbb{C})/\operatorname{Fil}^p H^{i-1}(X, \mathbb{C}) \to H^i_{\mathrm{Del}}(X, \mathbb{R}(p)) \to 0.$$

And because $\mathbb{C} = \mathbb{R}(p) \oplus \mathbb{R}(p-1)$, there are exact sequences

$$0 \to \operatorname{Fil}^p H^{i-1}(X, \mathbb{C}) \to H^{i-1}(X, \mathbb{R}(p-1)) \to H^i_{\mathrm{Del}}(X, \mathbb{R}(p)) \to 0$$

is injective. ⌟

Proof: This is because c acts as multiplication by $(-1)^p$ on the LHS, and $\operatorname{Fil}^p H^k(X, \mathbb{C}) \cap \overline{\operatorname{Fil}^p H^k(X, \mathbb{C})} = \oplus_{r,s \geq p} H^{r,s}(X)$, so the kernel is $\{0\}$. □

Prop. (12.10.3.7) [Comparison of Complex Conjugations]. For $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/\mathbb{R}$, the canonical isomorphism

$$H_{\mathrm{Betti}}(X, \mathbb{R}) \otimes_{\mathbb{R}} \mathbb{C} = H_{\mathrm{Betti}}(X, \mathbb{C}) \xrightarrow{I_{\mathrm{dR}}} H^i_{\mathrm{dR}}(X^{\mathrm{an}}) \xrightarrow{GAGA} H^i_{\mathrm{dR}}(X) \otimes_{\mathbb{R}} \mathbb{C}$$

is an isomorphism that identifies the complex conjugation $\mathsf{c}^* \otimes \mathsf{c}$ on the LHS with c on the RHS, so ⌟

Proof: Deligne, Prop1.4. □

Cor. (12.10.3.8). By taking the complex conjugation fixed part, we get an exact sequence

$$0 \to \operatorname{Fil}^p H^{i-1}_{\mathrm{Betti}}(X, \mathbb{R}) \to H^{i-1}_{\mathrm{Betti}}(X, \mathbb{R}(p-1))^{\mathsf{c}^* = (-1)^{p-1}} \to H^i_{\mathrm{Del}}(X/\mathbb{R}, \mathbb{R}(p)) \to 0$$

⌟

Differential Characters

Def. (12.10.3.9)[Differential Characters]. Let X be a differential manifold and Z^∞_l be the subgroup of closed singular differentiable chains, and $\Xi^l_\infty(X) \subset \mathrm{Hom}(Z^\infty_l, \mathbb{R}/\mathbb{Z})$ consisting of characters χ s.t. there exists $\omega \in \Omega^{l+1}(X)$ s.t.

$$\chi(\partial\varphi) = \int_{\Delta_{l+1}} \varphi^*\omega \in \mathbb{R}/\mathbb{Z}, \quad \forall \varphi \in C^\infty_{l+1}(X).$$

Such an ω is clearly uniquely determined by χ. ⌟

Prop. (12.10.3.10). For any $\chi \in \Xi^l_\infty(X)$, ω_χ is an integral closed form. ⌟

Proof: Cf.[Voisin, P306].? □

Prop. (12.10.3.11). If X is a complex manifold, and $\mu \in \Omega_{\mathbb{R}}^{l-1}(X)$, then for any closed chain $\varphi \in C_l^\infty(X)$,

$$\overline{\int_{\Delta_l} \varphi^*(\mathrm{i}\,\partial\mu)} = \int_{\Delta_l} \varphi^*(-i\bar{\partial}\mu) = \int_{\Delta_l} \varphi^*(-\mathrm{i}\,d\mu + \mathrm{i}\,\partial\mu) = \int_{\Delta_l} \varphi^*(\mathrm{i}\,\partial u),$$

so $\int_{\Delta_l} \varphi^*(\mathrm{i}\,\partial u) \in \mathbb{R}$, and we can define a differential character

$$\int \mathrm{i}\,\partial\mu \in \Xi_\infty^l(X) : \varphi \mapsto \int_{\Delta_l} \varphi^*(\mathrm{i}\,\partial u).$$

⌟

Prop. (12.10.3.12). For a compact Kähler manifold X and $p \in \mathbb{N}$, consider the subgroup $\Xi_\infty^{2p-1}(X)^{p,p} \subset \Xi_\infty^{2p}(X)$ consisting of differential characters χ s.t. ω_χ is of the type (p,p). Then

$$H_{\mathrm{Del}}^{2p-1}(X)^{p,p} \cong K_\infty^{2p-1}(X) = \Xi_\infty^{2p-1}(X)^{p,p}/\{\int \mathrm{i}\,\partial\mu | \mu \in \Omega^{p-1,p-1}(X)\}.$$

⌟

Proof: Cf.[Voisin, P307].? □

<u>**Properties of the Deligne Cohomology**</u>

Prop. (12.10.3.13) [Cup Products]. There are cup products

$$H_{\mathrm{Del}}^p(X, \mathbb{Z}(q)) \times H_{\mathrm{Del}}^{p'}(X, \mathbb{Z}(q')) \to H_{\mathrm{Del}}^{p+p'}(X, \mathbb{Z}(q+q')).$$

⌟

Proof: □

Prop. (12.10.3.14) [Cycle Class Maps]. For $X \in \mathcal{S}m\mathcal{P}roj/\mathbb{C}$ and $p \in \mathbb{N}$, there are class maps

$$\mathrm{CH}^p(X) \to H_{\mathrm{Del}}^{2p}(X, \mathbb{Z})$$

that lifts the class $[Z] \in H^{2p}(X, \mathbb{Z})$(12.10.3.4), and commutes with products and cup products. ⌟

Proof: Cf.[Voisin, P311].? □

4 Coniveau

Def. (12.10.4.1) [Coniveau]. The **coniveau** of $\alpha \in H_{\mathrm{Betti}}^\bullet(X, \mathbb{Q})$ is the smallest number c s.t. there is a closed algebraic subscheme $Y \subset X$ s.t. $\alpha|_{X\setminus Y} = 0 \in H_{\mathrm{Betti}}^\bullet(X \setminus Y, \mathbb{Q})$. ⌟

Thm. (12.10.4.2) [Deligne]. If $\alpha \in H_{\mathrm{Betti}}^\bullet(X, \mathbb{Q})$ is mapped to $0 \in H_{\mathrm{Betti}}^\bullet(X \setminus Y, \mathbb{Q})$ where Y is pure of codimension c, then $\alpha = j_*\beta$, where $j : \overline{Y} \to Y \to X$ is a resolution of singularities of Y and $\beta \in H_{\mathrm{Betti}}^{\bullet-2c}(\widetilde{Y}, \mathbb{Q})$. ⌟

Proof: □

12.11 Lie Groups

Main references are [Eti21], [Lee13], [Kna96].

1 Basics

Def. (12.11.1.1) [Lie Groups]. Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$, a **Lie group** is a group object in the category of smooth $\mathbb{K}$-manifolds. Notice it suffices to check that multiplication is smooth. The left and right translations L_g, R_g are all smooth morphisms hence diffeomorphisms.

A **homomorphism of Lie groups** is a smooth morphism that is also a group homomorphism. By translation invariance, a group homomorphism always has constant ranks, so a homomorphism of Lie groups that is a bijection is an isomorphism by global rank theorem(12.1.1.12).

The tangent space of G at e is denoted by $\mathfrak{g}$. ⌟

Proof: We show if a topological group G that is a smooth manifold satisfies $m : G \times G \to G$ is smooth, then G is a smooth manifold: consider the map $F : G \times G \to G \times G : (g, h) \mapsto (g, gh)$, it is a smooth map that is bijective.

The tangent map of F at (g, h) is $(X, Y) \mapsto (X, (dR_h)_g(X) + (dL_g)_h(Y))$, which is surjective because L_g is a diffeomorphism by(12.1.1.12). Then $F^{-1} : G \times G \to G \times G : (g, h) \mapsto (g, g^{-1}h)$ is smooth, and $g \mapsto g^{-1}$ is smooth. □

Prop. (12.11.1.2). A connected Lie group is automatically second countable. ⌟

Proof: This follows from the fact that a connected Lie group is a manifold hence locally second-countable and it is a union of products of a nbhd of e(4.12.1.3). □

Prop. (12.11.1.3). Any homomorphism of smooth manifolds has constant rank. ⌟

Proof: F being a homomorphism means that $F \circ L_g = L_{F(g)} \circ F$. Taking derivative and noticing the fact $L_g, L_{F(g)}$ are diffeomorphisms shows dF_{g_0} and dF_e have the same rank for any g. □

Prop. (12.11.1.4) [Discrete Subgroups]. Any discrete subgroup Γ of a Lie group G is a closed Lie subgroup of dimension 0. ⌟

Proof: Firstly Γ is countable: Let U be a nbhd of e containing no other points, choose another nbhd of e that $VV \subset U$, then $\{gV\}_{g\in\Gamma}$ is a family of disjoint open subsets of G, so there are countably many because G is second countable. Secondly Γ is closed in G, because

Γ is closed in G: Let U be a nbhd of e containing no other points, choose another nbhd of e that $VV \subset U$, then $\{gV\}_{g\in\Gamma}$ is a family of disjoint open subsets of G each containing an element of Γ. Then it is clear Γ is closed. Then(12.11.1.22) shows Γ is a closed Lie subgroup of dimension 0. □

Def. (12.11.1.5) [Adjoint Representation]. For a Lie group G, the conjugation map $C_g : G \to G : h \mapsto ghg^{-1}$ is a Lie group homomorphism. Let $\mathrm{Ad}(g) : \mathfrak{g} \to \mathfrak{g}$ denote its derivative, then $\mathrm{Ad} : g \mapsto \mathrm{Ad}(g)$ is an action of G on $\mathfrak{g}$, Bbcause $C_{g_1g_2} = C_{g_1}C_{g_2}$, $\mathrm{Ad}(g_1g_2) = \mathrm{Ad}(g_1)\,\mathrm{Ad}(g_2)$. ⌟

Prop. (12.11.1.6). Let G be a connected Lie group, and $\Gamma \subset G$ be a discrete normal subgroup. Show that Γ is in the center of G. ⌟

Proof: For $\gamma \in \Gamma$, consider the map $G \to G : g \mapsto g\gamma g^{-1}$, then it is a map with images in Γ. But Γ is discrete, so its image must be a single point, which is γ because $e\gamma e^{-1} = \gamma$. This means γ is in the center of G. □

Prop. (12.11.1.7) [Aut($\mathfrak{g}$)]. Let $\mathfrak{g}$ be a f.d. Lie algebra, then Aut($\mathfrak{g}$) is a closed Lie subgroup of $GL(\mathfrak{g})$, and its Lie algebra is Der($\mathfrak{g}$). Denote Int($\mathfrak{g}$) = Der($\mathfrak{g}$)^0. ⌟

Proof: For the Lie algebra, it suffices to show for $A \in \mathrm{End}(\mathfrak{g})$, $[e^{tA}X, e^{tA}Y] = e^{tA}[X,Y]$ iff $A([X,Y]) = [A(X),Y] + [X, A(Y)]$.

One direction is by taking derivative w.r.t. t, for the other, we can show $y_1(t) = [e^{tA}X, e^{tA}Y]$ and $y_2(t) = e^{tA}[X,Y]$ both satisfy the ordinary differential equation $y_i(t)' = Ay_i(t)$. □

Exponential Map

Def. (12.11.1.8) [One-Parameter Subgroup]. A **one-parameter subgroup** of a Lie group G over $\mathbb{K}$ is a Lie group homomorphism $\mathbb{K} \to G$. ⌟

Prop. (12.11.1.9). Let $X \in \mathfrak{g}$, then there exists a unique morphism of Lie groups $\gamma : \mathbb{K} \to G$ that $\gamma'(0) = X$. ⌟

Proof: If γ is such a group homomorphism, then $\gamma(s+t) = \gamma(s)\gamma(t)$. Differentiating for s, we get

$$\gamma(t)' = d(L_{\gamma(s)})_0(X).$$

Thus γ is an integral curve of the left-invariant vector field on G corresponding to X(12.11.3.3), which is unique.

Now to construct such a homomorphism, we use ODE theorems to construct a γ satisfying this for $|t| < \varepsilon$, and then check $\gamma(s+t) = \gamma(s)\gamma(t)$ because they are both integral curves for t starting at $\gamma(s)$. In particular, $d(L_{\gamma(t)})(X) = d(R_{\gamma(t)})(X)$. Now we can extend this γ to whole of $\mathbb{K}$ by defining $\gamma(2^n s) = \gamma(s)^{2^s}$, then we check by induction on n that

$$\gamma'(t) = \frac{1}{2}(d(R_{\gamma(\frac{t}{2})})\gamma'(\frac{t}{2}) + d(L_{\gamma(\frac{t}{2})})\gamma'(\frac{t}{2}))(X) = d(R_{\gamma(\frac{t}{2})})d(R_{\gamma(\frac{t}{2})})(X) = d(R_{\gamma(t)})(X).$$

□

Cor. (12.11.1.10) [One-Parameter Subgroup and Lie Algebras]. Let G be a Lie group, then the one-parameter subgroups of G correspond to maximal integral curves of left invariant vector fields starting at e. In particular, the one-parameter subgroups of G corresponds to $\mathfrak{g}$ and also $T_e(G)$.

Also, the flow of the right-invariant vector field R_X is given by $(g,t) \mapsto \exp(tX)g$, and the flow of the left-invariant vector field L_X is given by $(g,t) \mapsto g\exp(tX)$. ⌟

Def. (12.11.1.11) [Exponential Map]. Let G be a Lie group with Lie algebra $\mathfrak{g}$, then we can define an **exponential map** $\exp : \mathfrak{g} \to G$ that for any $X \in \mathfrak{g}$, $\exp(X) = \gamma_X(1)$, where γ_X is the one-parameter subgroup of G generated by X(12.11.1.10). It can be shown that $\gamma(sX)$ is the one-parameter subgroup of G generated by X. ⌟

Prop. (12.11.1.12) [Properties of Exponential Map].

1. $\exp : \mathfrak{g} \to G$ is a smooth map which is a local diffeomorphism near 0 that $\exp(0) = e, \exp_* = \mathrm{id}_{\mathfrak{g}}$.
2. $\exp(s+t) = \exp(s)\exp(t)$ for $s, t \in \mathbb{K}$.
3. For any group homomorphism $\varphi : G \to H$ and $X \in \mathfrak{g}$, $\varphi(\exp(X)) = \exp(\varphi_*(X))$.
4. $g\exp(tX)g^{-1} = \exp(\mathrm{Ad}(g)X)$. Also, $\mathrm{Ad}_* = \mathrm{ad}$, or equivalently by item3, $\mathrm{Ad}(\exp(X)) = \exp(\mathrm{ad}(x))$ as operators.

5. If we identify $\mathfrak{gl}_n(\mathbb{K})$ with $GL_n(\mathbb{K})$, then we can check directly that the exponential map of $GL_n(\mathbb{K})$ is
$$\exp(A)=\sum_{k=0}^\infty \frac{1}{k!}A^k.$$
┘

Proof: 1: The smoothness follows from the smoothness of the solution of ODE. The smooth inverse theorem shows it is a local diffeomorphism at identity.

2: trivial.

3: Both $\varphi(\exp(tX))$ and $\exp(t\varphi_*(X))$ are integral curves of the vector field $L_{\varphi_*(X)}$ and have the same initial point.

4: The first assertion is just item3 applied to the conjugate action C_g. For the Lie algebra homomorphism,
$$d(Ad)(X)Y=\frac{\partial}{\partial s}\frac{\partial}{\partial t}\exp(sX)\exp(tY)\exp(-sX)=[X,Y]$$
by(12.11.1.14). □

Prop. (12.11.1.13). Let G be a Lie group with Lie algebra $\mathfrak{g}$, and $\mathfrak{g}=A\oplus B$ a decomposition as subspaces, then the map
$$F:A\oplus B\to G:(X,Y)\mapsto \exp(X)\exp(Y)$$
is a local diffeomorphism at $0\in\mathfrak{g}$. ┘

Proof: Identify $\mathfrak{g}$ and the tangent space of G at e, then the differential F is identity, so it is a local diffeomorphism. □

Prop. (12.11.1.14)[Baker-Campbell-Hausdorff]. Let G be a Lie group with Lie algebra $\mathfrak{g}$, $X,Y\in\mathfrak{g}$, then
$$\exp(tX)\exp(tY)=\exp(\sum_{n=1}^\infty \frac{t^n}{n!}\mu_n(X,Y)).$$
where $\mu_n(X,Y)$ can be written as $\mathbb{Q}$-Lie polynomials of X and Y that is invariant of G.

In particular, $\mu_1(X,Y)=X+Y$, $\mu_2(X,Y)=\frac{1}{2}t^3([X,[X,Y]]+[Y,[Y,X]])$ and so on. ┘

Proof: By the Lie correspondence(12.11.3.15), we can first assume that G is simply-connected, then there is a mapping of G onto some subgroup of $GL(n,\mathbb{K})$ with discrete kernel. If we can prove the formula for $G=GL(n,\mathbb{K})$, then $\exp(\sum_{n=1}^\infty\frac{t^n}{n!}\mu_n(X,Y))\exp(tY)^{-1}\exp(tX)^{-1}$ is contained the kernel, but it is a smooth function in t, and its value is 1 for $t=0$, thus it holds for any t.

Now let $T\mathbb{K}^2=\mathbb{K}\langle x,y\rangle$ be the free non-commutative algebra in variables x,y, the series $\exp(x)=\sum_{n=0}^\infty\frac{x^n}{n!}$ can be viewed as an element in $\widehat{\mathbb{K}\langle x,y\rangle}$. Then we can define
$$\mu=\log(\exp(x)\exp(y))\in\widehat{\mathbb{K}\langle x,y\rangle},$$
where $\log(A)=-\sum_{n=1}^\infty\frac{(1-A)^n}{n!}$. Then $\mu=\sum_{n=1}^\infty\frac{\mu_n}{n!}$, where $\mu\in\mathbb{K}\langle x,y\rangle$ are polynomials in x,y of degree n with coefficients in $\mathbb{Q}$.

Then it remains to show that μ_n can be written as Lie polynomials in x,y. Notice $\Delta(x)=x\otimes 1+1\otimes x$, thus $\Delta(\exp(x))=\exp(x)\otimes\exp(x)$, thus $\Delta(\exp(x)\exp(y))=\exp(x)\exp(y)\otimes\exp(x)\exp(y)$, and
$$\Delta(\log(\exp(x)\exp(y)))=\log(\Delta(\exp(x)\exp(y)))=\log((\exp(x)\exp(y)\otimes 1)(1\otimes\exp(x)\exp(y)))$$

$$= \log(\exp(x)\exp(y)) \otimes 1 + 1 \otimes \log(\exp(x)\exp(y)).$$

then by separating degrees, each μ_n is primitive(3.11.2.4), thus they are contained in the free Lie-algebra generated by x, y, by(3.7.8.15) and(3.7.8.18).

The calculation is invariant of n in $GL(n, \mathbb{R})$, thus it is invariant of G. □

Cor. (12.11.1.15). Let G be a Lie group with Lie algebra $\mathfrak{g}$, $X, Y \in \mathfrak{g}$, then

$$\lim_{n\to\infty} (\exp(\frac{1}{n}X)\exp(\frac{1}{n}Y))^n = \exp(X + Y).$$

⌟

Proof:

$$(\exp(\frac{1}{n}X)\exp(\frac{1}{n}Y))^n = (\exp(\frac{1}{n}(X+Y) + O(\frac{1}{n^2})))^n = \exp(X + Y + O(\frac{1}{n})).$$

Taking $n \to \infty$, we get the desired result. □

Prop. (12.11.1.16). Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$ and H, G be Lie groups over $\mathbb{K}$, then

- A continuous homomorphism $\gamma : \mathbb{K} \to H$ is smooth.
- A continuous homomorphism between smooth Lie groups $F : G \to H$ is smooth.
- There is at most one smooth structure on a Lie gx1x10nianshao x1x10roup G that makes it a Lie group group.

⌟

Proof: 1: Let V be a nbhd of $0 \in \mathfrak{h}$ that exp is a diffeomorphism on $2V$(12.11.1.12). Choose t_0 small that $\gamma(t) \in \exp(V)$ for any $|t| \le t_0$, and let $X \in V$ that $\exp(X) = \gamma(t_0)$, then we can show $\gamma(t) = \exp(tX)$ for any $t = \frac{m}{2^n}$, so this holds for any t by continuity/analyticity, and γ is smooth.

2: By the proof of 1, we can construct a map(not necessary continuous) $F_* : \mathfrak{g} \to \mathfrak{h}$ with commutative diagram $\begin{array}{ccc} \mathfrak{g} & \xrightarrow{F_*} & \mathfrak{h} \\ \downarrow{\scriptstyle\exp} & & \downarrow{\scriptstyle\exp} \\ G & \xrightarrow{F} & H \end{array}$. Now using(12.11.1.15) and the continuity of F, we can show F_* is linear:

$$\begin{aligned}\exp(F_*(X+Y)) = F(\exp(X+Y)) &= F(\lim_{n\to\infty} \exp(\frac{1}{n}X)\exp(\frac{1}{n}Y))^n] \\ &= \lim_{n\to\infty} (\exp(\frac{1}{n}F_*X)\exp(\frac{1}{n}F_*Y))^n = \exp(F_*(X+Y))\end{aligned}$$

Thus F is smooth at a nbhd of G, and smooth everywhere by translation. □

Group Aspects

Def. (12.11.1.17) [Lie Subgroup]. A **Lie subgroup** of a Lie group G is a subgroup that is also an immersed submanifold(12.1.1.14).

An **embedded Lie subgroup** of a Lie group G is a subgroup that is also an immerse submanifold(12.1.1.14). ⌟

Prop. (12.11.1.18) [Lie subgroup is Weakly Embedded]. Any Lie subgroup of a Lie group G is weakly embedded. ⌟

Proof: Cf.[Lee13]P506. □

Lemma (12.11.1.19). Let G be a Lie group and H a subgroup that is also an embedded submanifold, then H is an embedded Lie subgroup. ⌟

Proof: We need to show the multiplication and inverse on H is smooth: $H \times H \to G$ is smooth and has image in H, thus $H \times H \to H$ is also smooth, by(12.1.1.22). □

Lemma (12.11.1.20). Let G be a Lie group and $H \subset G$ a Lie subgroup, if H is an embedded submanifold of G, then H is closed in G. ⌟

Proof: Assume H is an embedded submanifold of G, then it is locally compact in the induced topology, so(11.10.1.7) shows H is closed in G. □

Lemma (12.11.1.21). Let G be a Lie group and H a subgroup of G that is also a closed subset of G, then H is an embedded Lie subgroup. ⌟

Proof: By(12.11.1.20), it suffices to show that H is an embedded submanifold of G. Let $\mathfrak{g}$ be the Lie algebra of G, and define a subspace $\mathfrak{h} \subset \mathfrak{g}$ that $\mathfrak{h} = \{X \in \mathfrak{g} | \exp(tX) \in H, \forall t \in \mathbb{R}\}$. By(12.11.1.15) and the fact H is closed in G, $\mathfrak{h}$ is a linear subspace of $\mathfrak{g}$.

Next we show that there exists a nbhd U of $0 \in \mathfrak{g}$ that exp is a diffeomorphism and also $\exp(U \cap \mathfrak{h}) = \exp(U) \cap H$: Let U be any open nbhd of $0 \in \mathfrak{g}$ that exp is a diffeomorphism $U \to \exp(U)$, then $\exp(U \cap \mathfrak{h}) \subset \exp(U) \cap H$ by definition.

Let $\mathfrak{b} \subset \mathfrak{g}$ be chosen s.t. $\mathfrak{h} \oplus \mathfrak{b} = \mathfrak{h}$, then $F : \mathfrak{h} \oplus \mathfrak{b} \to G : (X, Y) \mapsto \exp(X)\exp(Y)$ is a local diffeomorphism. Choose nbhd U of $0 \in \mathfrak{g}$ and $\widetilde{U}$ of $0 \in \mathfrak{h} \oplus \mathfrak{b}$ that both $\exp|_U$ and $F|_{\widetilde{U}}$ are diffeomorphisms, and choose a countable nbhd basis $\{U_i\}$ of $0 \in \mathfrak{g}$. Denote $V_i = \exp(U_i)$ and $\widetilde{U}_i = F^{-1}(V_i)$, then V_i is a nbhd basis of $e \in G$ and $\widetilde{U}_i$ is a nbhd basis of $0 \in \mathfrak{h} \oplus \mathfrak{b}$. We may assume $U_i \subset U$ and $\widetilde{U}_i \subset \widetilde{U}$.

If $\exp(U_i \cap \mathfrak{h}) \subset \exp(U_i) \cap H$ for any i, then we can choose $h_i = \exp(Z_i) \in H$ that $h_i \notin \exp(U_i \cap \mathfrak{h})$. Because $\exp(U_i) = F(\widetilde{U}_i)$, set $h_i = \exp(X_i)\exp(Y_i)$, where $(X_i, Y_i) \in \widetilde{U}_i$. Now $Y_i \neq 0$, otherwise $\exp(Z_i) = \exp(X_i)$, which implies $Z_i = X_i$ and $h \in \exp(U_i \cap \mathfrak{h})$. Notice $\exp(Y_i) = \exp(X_i)^{-1} h_i \in H$.

Because $\widetilde{U}_i$ is a basis of $\mathfrak{h} \oplus \mathfrak{b}$, $Y_i \to 0$, Choose an inner product on $\mathfrak{b}$, and let $c_i = |Y_i|$, then $c_i^{-1} Y_i$ lies on the unit sphere of $\mathfrak{b}$. Replacing by a subsequence, we can assume $c_i^{-1} Y_i \to Y$ for some $Y \in \mathfrak{b}$. Then $|Y| = 1$ by continuity.

For any $t \in \mathbb{R}$, let $n_i = [\frac{t}{c_i}]$, then $|nc_i - t| \leq c_i \to 0$, which means $n_i Y_i \to tY$, so $\exp(n_i Y_i) \to \exp(tY)$. But $\exp(n_i Y_i) = \exp(Y_i)^{n_i} \in H$, so $\exp(tY) \in H$ because H is closed. Thus $Y \in \mathfrak{h}$, contradiction.

Thus in this way we can construct a slice chart φ of H at e, and for any $h \in H$, because

$$L_h((\exp(U) \cap H)) = L_h(\exp(U)) \cap H,$$

$\varphi \circ L_{h^{-1}}$ is a slice chart of H at h. Thus H is an embedded submanifold of G by(12.1.1.17). □

Prop. (12.11.1.22) [Closed Subgroup Theorem]. Let G be a Lie group and H a subgroup of G, then the following are equivalent:

- H is closed in G.
- H is an embedded submanifold.
- H is an embedded Lie subgroup.

⌟

Proof: $3 \to 2$ is trivial, $3 \to 1$ is(12.11.1.20). $1 \to 3$ is(12.11.1.21), $2 \to 3$ is(12.11.1.19). □

Remark (12.11.1.23). The dense line of the torus is a Lie subgroup that is not a closed Lie subgroup. ⌟

Lemma (12.11.1.24) [One-Parameter subgroup of Subgroups]. Let $H \subset G$ be a Lie subgroup, then the one-parameter subgroups of H are exactly those of G with initial velocity in $T_e(H)$. ⌟

Proof: This is because a one-parameter subgroup of H is naturally a one-parameter subgroup of G, and two one-parameter subgroups with the same initial velocity is identical. □

Prop. (12.11.1.25). Let $H \subset G$ be a Lie subgroup, then the exponential map of H is the exponential map of G restricted to $\mathfrak{h}$, and

$$\mathfrak{h} = \{X \in \mathfrak{g} | \exp(tX) \in H, \forall t \in \mathbb{R}\}.$$

⌟

Proof: The first assertion is an immediate corollary of(12.11.1.24). Now if $X \in \mathfrak{h}$, then the first assertion shows $\exp(tX) \in H$ for all t. Conversely, if $\exp(tX) \in H$ for all t, then $\exp(tX)$ is a smooth map to H, by(12.11.1.18), thus its derivative at e is in $\mathfrak{h}$, which means $X \in H$. □

Prop. (12.11.1.26) [Semidirect Product]. Let G acts via τ on H, then the Lie algebra of $G \ltimes_\tau H$ is $\mathfrak{g} \ltimes_{d\tau} \mathfrak{h}$. ⌟

Proof: Notice the differential of the action $\tau(g)$ on H defines a map $G \to GL(\mathfrak{h})$, and then the differential of this map gives a map $d\tau : \mathfrak{g} \to \mathrm{Der}(\mathfrak{h})$, so we can form $\mathfrak{g} \ltimes_{d\tau} \mathfrak{h}$(3.7.1.6).

For the rest, Cf.[Knapp, P60]. □

Prop. (12.11.1.27). Let G, H be simply-connected Lie groups with Lie algebra $\mathfrak{g}, \mathfrak{h}$, and let $\pi : \mathfrak{g} \to \mathrm{Der}(\mathfrak{h})$ be a Lie algebra homomorphism, then there is an action τ of G on H by automorphisms that $d\overline{\tau} = \pi$, and $G \ltimes_\tau H$ is a simply-connected Lie group with Lie algebra $\mathfrak{g} \ltimes_\pi \mathfrak{h}$. ⌟

Proof: Cf.[Knapp, P60]. □

Prop. (12.11.1.28) [Quotient Theorem for Lie Groups]. Let G be a Lie group and H a normal closed Lie subgroup, then the quotient G/H is a Lie group, and the quotient map π is a surjective Lie group homomorphism with kernel H. ⌟

Proof: By(12.11.2.6), G/H is a smooth manifold that the quotient map is surjective, smooth, and is a group homomorphism with kernel H. It suffices to show the multiplication of G/H is smooth, which is easy by(12.1.1.8). □

Prop. (12.11.1.29) [First Isomorphism Theorem for Lie Groups]. Let $\varphi : G \to H$ be a Lie group homomorphism, then there kernel of F is an closed Lie subgroup of G with Lie algebra $\ker(\varphi_*)$. The image of φ has a unique smooth structure making it a Lie subgroup of H that $G/\ker(F) \to \mathrm{Im}(\varphi)$ is a diffeomorphism, and it is a closed Lie subgroup when it is embedded in H, e.g. when φ induces a proper action(12.11.2.3). ⌟

Proof: This follows from(12.11.2.2) and(12.11.1.22). □

Def. (12.11.1.30) [Adjoint Group]. For a Lie group G, the center $Z(G)$ of G is a closed Lie subgroup because it the kernel of Ad(12.11.1.29). We call the group $G/Z(G)$ the **adjoint group** of G, which is an immersed subgroup of $GL(\mathfrak{g})$ by(12.11.1.29). ⌟

Lie Groups and Analytic Groups

Prop. (12.11.1.31). What condition makes a Lie group a complex Lie group**?** ⌟

Prop. (12.11.1.32). Any connected Lie group has a compact subgroup as deformation retraction. ⌟

Proof: □

Prop. (12.11.1.33) [Gleason; Montgomery-Zippin]. A real topological group G admits a (unique) Lie group structure iff the underlying topological space G is a topological manifold. ⌟

Proof: Cf.https://terrytao.wordpress.com/2011/06/17/hilberts-fifth-problem-and-gleason-metrics/
□

Prop. (12.11.1.34) [Lie Groups and Analytic Groups]. A real Lie group admits a unique real analytic structure, So it is not important to distinguish between a Lie group and an analytic Lie group, and call it **analytic group** if it is a connected Lie group. The uniqueness follows from(12.11.1.16). ⌟

Proof: Use(12.11.1.14) to show that in a local exp char (U,φ) of 1, $U\times U\to U$ is analytic, then we can choose an analytic atlas on G given by $\{(gU,\varphi\circ L_{g^{-1}})$. This is an analytic atlas, because the transition function is $\varphi L_{g^{-1}h}\varphi^{-1}$ on $U\cap h^{-1}gU$. Because $hU\cap gU\neq\varnothing$, let $x=hu_1=gu_2$, then $L_{g^{-1}h}=L_{u_2u_1^{-1}}$, which is analytic.

To show multiplication is analytic w.r.t. this atlas: **?** □

Cor. (12.11.1.35). The proof above can be used to show that any C^k-group manifold be upgraded uniquely to a Lie group structure. So basically the study of C^0-Group manifold and analytic groups are the same. ⌟

2 Homogeneous Spaces

Actions of Lie Groups

Prop. (12.11.2.1)[Fundamental Theorem on Lie Group Actions]. Let θ be a right smooth action of a Lie group G on a smooth manifold M, then we can define a complete Lie algebra homomorphism

$$\widetilde{\theta}:\mathfrak{g}\to\mathfrak{X}(M):\theta(X)_p=\frac{d}{dt}|_{t=0}p\cdot\exp(tX)=d(\theta^{(p)})_e(X_e),$$

called the **infinitesimal generator** of θ. where a Lie homomorphism $\widetilde{\theta}:\mathfrak{g}\to\mathfrak{X}(M)$ is called complete iff for any $X\in\mathfrak{g}$, $\widetilde{\theta}(X)$ is a complete vector field(12.1.5.3).

Conversely, if G is simply-connected and $\widetilde{\theta}:\mathfrak{g}\to\mathfrak{X}(M)$ is a complete Lie algebra homomorphism, then there exists a unique smooth right action θ of G on M with infinitesimal generator $\widetilde{\theta}$. ⌟

Proof: $\theta(X)$ is smooth because it is the infinitesimal generator of the smooth flow $\mathbb{R}\times M\to M:(t,p)\mapsto p\exp(tX)$(12.1.5.4). $\widetilde{\theta}$ is a Lie algebra homomorphism by(12.1.2.13).**?** □

Prop. (12.11.2.2) [Isotropy Group and Orbits]. Let θ be an action of G on a manifold M, let $\widetilde{\theta}_x:\mathfrak{g}\to T_xM$ be given by $\widetilde{\theta}_x(X)=\widetilde{\theta}(X)_x$. Then

- The stabilizer G_x is a closed subgroup of G with Lie subalgebra $\mathfrak{g}_x=\ker(\widetilde{\theta}_x)$.

- Gx has a unique smooth structure making it an immersed subgroup of M that $G/G_x \to Gx$ is a diffeomorphism, and $T_x(Gx) \cong \mathrm{Im}(\widetilde{\theta}_x) \cong \mathfrak{g}/\mathfrak{g}_x$.

⌟

Proof: Cf.[Eti21]P48. □

Prop. (12.11.2.3). If a Lie group G acts properly on a manifold M, then each orbit is a closed submanifold of M, and each isotropy group is compact, by(4.12.1.15) and(4.12.1.17). ⌟

Prop. (12.11.2.4) [Quotient Map Theorem]. Let G be a Lie group that acts smoothly, freely and properly on a manifold M, then the quotient space M/G is a topological manifold with dimension $\dim M - \dim G$, and it has a unique smooth structure that $M \to M/G$ is a smooth submersion. ⌟

Proof: Cf.[Lee13]P544. □

Homogeneous Spaces and Fiber Bundles

Def. (12.11.2.5) [Homogeneous Spaces]. Let G be a Lie group, then a **homogeneous space** for G is a smooth manifold M with a smooth transitive G-action. ⌟

Prop. (12.11.2.6) [Characterizing Homogeneous Spaces]. Let G be a Lie group.

- if H is a closed subgroup of G, then the left coset space G/H is a topological manifold of dimension $\dim G - \dim H$, and has a unique smooth structure that the quotient map $G \to G/H$ is a smooth submersion. With this smooth structure, the left action of G on G/H turns it into a homogeneous space.
- If M is a homogeneous G-space, and $p \in M$, then the isotropy group G_p of M is a closed subgroup of G, and $G/G_p \to M$ is a diffeomorphism of G-spaces.

⌟

Proof: Cf.[Lee13]P551, P552. □

Cor. (12.11.2.7) [Homogeneous Space Structure on Sets]. Suppose X is a set with a transitive action of a Lie group G that for some point $p \in X$, the isotropy group G_p is closed in G. Then X has a unique smooth manifold structure with respect to which the given action is smooth. With this structure, $\dim X = \dim G - \dim G_p$. ⌟

Proof: This is because G/G_p is a smooth manifold that is G-equivariantly isomorphism to X, and the uniqueness also follows from the proposition. □

Prop. (12.11.2.8) [Quotients of Lie Groups by Discrete Subgroups]. Let G be a Lie group and Γ a discrete subgroup of G, then G/Γ is a smooth manifold, and the quotient map $G \to G/\Gamma$ is a smooth normal covering. ⌟

Proof: (12.11.1.4) and the proof of(12.11.2.6) shows Γ acts smoothly, freely, and properly on G on the right. Then the theorem is a consequence of(12.1.1.10). □

Prop. (12.11.2.9) [Contractible Homogeneous Space]. If X is a homogeneous G-manifold that is contractible, $x \in X$, then G is diffeomorphic to $G_x \times X$. ⌟

Proof: □

Prop. (12.11.2.10) [Orientability of Homogenous Spaces]. Let G be a Lie group and X be a homogeneous manifold of G. Let $x \in X$ and $H = \mathrm{Stab}_G(x)$.

1. X is orientable iff values of $\mathrm{Ad}(h_i)$ are of the same sign for any two element $h_1, h_2 \in H$ lying in a same connected component of G.
2. Show that when H is connected, X is orientable.
3. There exist a G-invariant volume form on X iff $\mathrm{Ad}(H) \subset SL(\mathfrak{g}/\mathfrak{h})$.

⌟

Prop. (12.11.2.11) [Fiber Bundle of Homogenous Spaces]. Let $G \in \mathcal{L}\mathrm{ie}\mathcal{G}\mathrm{rp}_{\mathrm{cpct}}$, $K \leq H \leq G$ be closed subgroups, then the map $G/K \to G/H$ is a G- locally trivial fiber bundle. ⌟

Proof: ? □

Prop. (12.11.2.12) [Examples of Homogeneous Spaces]. Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$.

- The **Grassmannian manifold** $\mathrm{Gra}(k, \mathbb{K}^n)$ is defined to be the set of k-dimensional spaces in $\mathbb{K}^n$. $U(n, \mathbb{K})$ acts transitively on $\mathrm{Gra}(k, \mathbb{K}^n)$, and the stabilizer is $U(k, \mathbb{K}) \times U(n-k, \mathbb{K})$. Thus $\mathrm{Gra}(k, \mathbb{K}^n)$ is a homogeneous $U(n, \mathbb{K})$-space by(12.11.2.7), and $U(n, \mathbb{K}) \to \mathrm{Gra}(k, \mathbb{K}^n)$ is a fiber bundle with fiber $U(k, \mathbb{K}) \times U(n-k, \mathbb{K})$ by(12.11.2.11).
- The **Stiefel manifold** $V_k(\mathbb{K}^n)$ of orthonormal k-frames in $\mathbb{K}^n$ is defined to be the set of tuples $(v_1, \ldots, v_n)$ in $\mathbb{K}^n$ that $(v_i, v_j) = \delta_{ij}$. $U(n, \mathbb{K})$ acts transitively on $V_k(\mathbb{K}^n)$ with stabilizer $U(n-k, \mathbb{K})$, Thus $V_k(\mathbb{K}^n)$ is a homogeneous $U(n, \mathbb{K})$-space by(12.11.2.7), and $U(n, \mathbb{K}) \to V_k(\mathbb{K}^n)$ is a fiber bundle with fiber $U(n-k, \mathbb{K})$, and $V_k(\mathbb{K}^n) \to \mathrm{Gra}(k, \mathbb{K}^n)$ is a fiber bundle with fiber $U(k, \mathbb{K})$.
- The **flag Variety**.

⌟

Proof: 1: Let $\dim X = n$. X is orientable iff there is a non-vanishing n-form on X. Because $o_x : G \to X$ is submersive, choose n left invariant vector fields $X_1, \ldots, X_n$ that $(do_x)_e(v_i)$ generate $T_x(X)$, then by homogeneity, $(do_x)_g(X_{ig})$ generate $T_gx(X)$ for any $g \in G$. Thus X is orientable iff there is a n-form ω on G that satisfies $r_h^*\omega = \omega$, $\omega_g = \Delta(g) l_{g^{-1}}^* \omega_e$ for some $\Delta(g) \in \mathbb{R}*$, and for any $h \in H$, and $\omega(X_1, \ldots, X_n) \neq 0$.

If such a form exists, then $\Delta(gh) l_{(gh)^{-1}}^* \omega_e = r_h^* l_{g^{-1}}^* \omega_e$, which is equivalent to $\Delta(g)\,\mathrm{Ad}(h)^*\omega_e = \Delta(gh)\omega_e$ for any $h \in H$, thus values of $\mathrm{Ad}(h_i)$ are of the same sign for any two element $h_1, h_2 \in H$ lying in a same connected component of G.

Conversely, if values of $\mathrm{Ad}(h_i)$ are of the same sign for any two element $h_1, h_2 \in H$ lying in a same connected component of G, then we can define ω as above, where $\Delta(h) = \det(\mathrm{Ad}(h)|(\mathfrak{g}/\mathfrak{h}))$, and extend Δ to G that satisfy $\Delta(gh) = \Delta(g)\Delta(h)$. This can be because G is a fiber bundle over G/H.

2: When H is connected, clearly the values of $\mathrm{Ad}(H)$ are of the same sign.

3: The proof is the same as that of item1. In this case, all $\Delta(g) = 1$, thus the existence of G-invariant volume form on X is equivalent to $\mathrm{Ad}(H) \subset SL(\mathfrak{g}/\mathfrak{h})$. □

3 Lie Theory

Lie Algebras of Lie Groups

Def. (12.11.3.1) [Invariant Vector Fields]. Let G be a Lie group, then a smooth vector field X on G is called left-invariant if $d(L_g)_{g'}(X_{g'}) = X_{gg'}$ for any $g, g' \in G$. The set of left-invariant vector fields on G is denoted by $\mathrm{Lie}(G)$. ⌟

Prop. (12.11.3.2). If $X.Y$ are left-invariant vector fields over G, then $[X, Y]$ is also left-invariant, by(12.1.2.13). ⌟

Prop. (12.11.3.3)[Invariant Vector Fields and Tangent Spaces]. Let G be a Lie group, then the evaluation map $\mathrm{Lie}(G) \to \mathfrak{g} : X \mapsto X_e$ is a vector space isomorphism. ⌟

Proof: The inverse map is given by $X \mapsto (L_X)_g = d(L_g)_e(X)$. This is clearly a left-invariant vector field. It suffices to show that this $\widetilde{X}$ is smooth. By(12.1.2.10), it suffices to show $L_X(f)$ is smooth for any smooth function f.

$$L_X(f)(g) = d(L_g)_e(X)(f)(g) = X(L_g f)(0) = \frac{d}{dt}|_0 f(g\exp(tX))$$

which is a differential of a smooth map $\mathbb{R} \times G \to GL : (t, g) \mapsto f(g\exp(tX))$, so it is smooth in g. □

Cor. (12.11.3.4)[Lie Group is Parallelizable]. Every Lie group admits a left-invariant smooth global frame, thus any Lie group is parallelizable. ⌟

Prop. (12.11.3.5). If $X \in \mathfrak{g}$ corresponds to a left-invariant vector field L_X, then for any $g \in G$,

$$d(R_g)_p((L_X)_p) = (L_{\mathrm{Ad}(g^{-1})X})_{pg}.$$

⌟

Proof:

$$\begin{aligned} d(R_g)_p((L_X)_p)(f)(pg) &= (L_X)_p(R_g f) = d(L_p)_e(X)(R_g f) \\ &= X(L_p R_g(f)) = \frac{d}{dt}|_0 f(p\exp(tX)g) \\ &= \frac{d}{dt}|_0 f(p\exp(t\,\mathrm{Ad}(g^{-1})X)) = (\mathrm{Ad}(g^{-1}X)(L_p(f)) \\ &= (L_{\mathrm{Ad}(g^{-1})X})_{pg}(f)(pg) \end{aligned}$$

□

Def. (12.11.3.6) [Lie Algebra of a Lie Group]. If G is a Lie group, $\mathrm{Lie}(G)$ is a Lie algebra w.r.t. the Lie bracket(12.1.2.12). It is called the **Lie algebra associated to** G. ⌟

Proof: This is clear from the definition $[X, Y](f) = XY(f) - YX(f)$. □

Prop. (12.11.3.7) [Induced Map of Lie Algebras]. A homomorphism $F : G \to H$ of Lie groups induces a morphism of their Lie algebras via the tangent space. ⌟

Proof: For any $X \in \mathrm{Lie}(G)$, define $F_*(X)_g = (dL_g)_e(dF_e(X_e))$, then this is a left-invariant vector field, and it clearly corresponds to the tangent map via isomorphism in(12.11.3.3). This map is a Lie algebra map by a variant of(12.1.2.13). □

Cor. (12.11.3.8). If $H \subset G$ is a Lie subgroup, then there is a natural isomorphism

$$\mathfrak{h} \cong \{X \in \mathrm{Lie}(G) | X_e \in T_e H\}.$$

In particular, the tangent space $\mathfrak{h}$ of H is a Lie subalgebra of $\mathfrak{g}$. ⌟

Proof: There is a commutative diagram

$$\begin{array}{ccc} \mathrm{Lie}(H) & \xrightarrow{X\mapsto X_e} & \mathfrak{h} \\ \downarrow \iota_* & & \downarrow (\iota_*)_e \\ \mathrm{Lie}(G) & \xrightarrow{X\mapsto X_e} & \mathfrak{g} \end{array}.$$

□

Prop. (12.11.3.9) [Covering of Lie Groups]. Let $F : G \to H$ be a homomorphism of connected Lie groups, then the following are equivalent:

- F is surjective with discrete kernel.
- F is a smooth covering map.
- F is a local diffeomorphism.
- The induced homomorphism $F_* : \mathfrak{g} \to \mathfrak{h}$ is an isomorphism.

⌟

Proof: $1 \to 2$: F is surjective thus H is a homogeneous G-space, so(12.11.2.6) shows $H \cong G/\ker(F)$. And $G \to G/\ker(F)$ is a smooth covering map by(12.11.2.8).

$2 \to 3$ is trivial.

$3 \to 1$: If F is a local diffeomorphism, then $\ker(F)$ is discrete, and F is open. Thus $F(G)$ is an open subgroup of H, thus all of H because H is connected(4.12.1.3).

$3 \to 4$ is trivial. $4 \to 3$ is by inverse function theorem. □

Cor. (12.11.3.10) [Homomorphism with Discrete Kernel]. Let $G \to H$ be a homomorphism of Lie groups of the same dimension with discrete kernel and H connected, then it is a covering space map, and the kernel is in the center of G, by(12.11.1.6). ⌟

Proof: This homomorphism is locally injective at 1, so it has rank $\dim G = \dim H$, so it is local diffeomorphism. In particular, the image contains a nbhd of 1 in H, thus it contains all H by(4.12.1.3).
□

Prop. (12.11.3.11) [Universal Covering Lie Group]. If G is a connected Lie group, then its universal covering space $\widetilde{G}$ can be given a Lie group structure that the covering map is a group homomorphism. Moreover, the group structure is unique up to isomorphism over G. Moreover, the kernel of $\widetilde{G} \to G$ is a discrete central subgroup of $\widetilde{G}$. ⌟

Proof: Because $\widetilde{G}$ is simply connected, so does $\widetilde{G} \times \widetilde{G}$, let $\widetilde{e}$ be an element over e, we can lift the map $\widetilde{G} \times \widetilde{G} \to G \times G \xrightarrow{m} G$ to a map $\widetilde{m} : \widetilde{G} \times \widetilde{G} \to \widetilde{G}$ that $\widetilde{m}(\widetilde{e}, \widetilde{e}) = \widetilde{e}$. Similar we can lift an inverse map $\widetilde{i}$ that $\widetilde{i}(\widetilde{e}) = \widetilde{e}$. These maps are smooth because $\pi : \widetilde{G} \to G$ is a local diffeomorphism.

It's left to show that $(\widetilde{m}, \widetilde{i})$ makes $\widetilde{G}$ into a Lie group: For example, the map $L_{\widetilde{e}} : \widetilde{G} \to \widetilde{G}$ is a lift of id_G and it coincides with $\mathrm{id}_{\widetilde{G}}$ on a point $\widetilde{e}$, thus it is just $\mathrm{id}_{\widetilde{G}}$, which means $\widetilde{e}$ is a left identity. The rest is easy.

For the uniqueness: By the universal property of covering, if there are two coverings, we can lift it to a map connecting them that maps identity to identity, then show it is a group homomorphism.

The last assertion follows from(12.11.3.10). □

Prop. (12.11.3.12) [Lie Subalgebras and Subgroups]. For a Lie group G, for any lie subalgebra $\mathfrak{h} \subset \mathfrak{g}$, there exists uniquely a connected Lie subgroup H s.t. $\mathfrak{h}$ is the lie algebra of H. ⌟

Proof: By (12.1.3.1), there is a maximal connected manifold H corresponding to $\mathfrak{h}$, we only need to show that it is a group. But the left invariance of $\mathfrak{h}$ shows that $HH \subset H$ because H is maximal. Cf.[Lee13]P506.? □

Cor. (12.11.3.13). If G_1 is a simply connected Lie group and G_2 is a connected Lie group, then any Lie algebra homomorphism $\widetilde{h}:\mathfrak{g}_1\to\mathfrak{g}_2$ can be lifted to a unique Lie group homomorphism. ⌟

Proof: Consider the image of $\widetilde{h}$: $\Gamma(\widetilde{h})\subset\mathfrak{g}_1\times\mathfrak{g}_2$, which is a Lie subalgebra. First notice a Lie group homomorphism h is equivalent to a Lie subgroup G_h of $G_1\times G_2$ that $\pi_1|_{G_h}$ is a diffeomorphism onto G_1. And this Lie homomorphism induces the desired Lie algebra homomorphism iff the Lie algebra of G_h is just $\widetilde{h}$.

(12.11.3.12) shows that there exists a unique Lie group G in $G_1\times G_2$ with Lie subalgebra $\Gamma(\widetilde{h})$. The projection $\pi_1|_G$ is a diffeomorphism onto G_1, because the tangent map at e is an isomorphism, thus a local diffeomorphism and by(12.11.3.10) a covering map, so it must be an isomorphism because G_1 is simply connected and G is connected. □

Cor. (12.11.3.14) [Representations of Simply-Connected Lie Groups]. The category of representations of s simply-connected Lie groups is equivalent to the category of representations of its Lie algebra. ⌟

Thm. (12.11.3.15) [The Lie Correspondence].

- The category of finite dimensional Lie algebras is equivalent to the category of simply connected Lie groups.
- For a f.d. Lie algebra $\mathfrak{g}$, the connected Lie groups with Lie algebras isomorphic to $\mathfrak{g}$ corresponds to G/Γ, where G is a simply connected subgroup with Lie algebra $\mathfrak{g}$, and Γ is a discrete central subgroup of G.

⌟

Proof: 1: By(12.11.3.12)(12.11.3.13) together with Ado's theorem**??**.

2: (12.11.3.11) and(12.11.3.9) shows any Lie group is a quotient of its universal covering Lie group by a discrete central subgroup. Conversely, for any discrete central subgroup, G/Γ is a Lie subgroup and $\pi:G\to G/\Gamma$ is a homomorphism with kernel Γ by(12.11.1.4) and(12.11.1.28), thus $\mathrm{Lie}(G)=\mathrm{Lie}(G/\Gamma)\cong\mathfrak{g}$(12.11.1.28). □

Prop. (12.11.3.16) [Ideals and Normal Subgroups]. Let G be a connected Lie group and H a connected Lie subgroup, then H is a normal subgroup of G iff $\mathfrak{h}$ is an ideal of $\mathfrak{g}$. ⌟

Proof: Because G,H are both connected, (4.12.1.3) shows H is normal in G iff for any $X\in\mathfrak{g},Y\in\mathfrak{h}$, $\exp(X)\exp(Y)\exp(X)^{-1}\in H$. Taking derivative w.r.t. Y, this is equivalent to $d(\mathrm{Ad}(\exp(X)))(Y)=\mathrm{ad}(X)Y\in\mathfrak{h}$(12.11.1.12), by(12.11.1.25), which is equivalent to $\mathfrak{h}$ being an ideal of $\mathfrak{g}$. □

Prop. (12.11.3.17) [Center]. Let G be a connected subgroup with Lie algebra $\mathfrak{g}$ and Z the center of G, $\mathfrak{z}$ the center of $\mathfrak{g}$, then Z is a closed Lie subgroup of G with Lie algebra $\mathfrak{z}$. ⌟

Proof: Because G is connected, $g\in Z$ iff g commutes with all $\exp(tX),X\in\mathfrak{g}$. Thus $Z=\ker\mathrm{Ad}$. Now the assertion follows from(12.11.1.29). □

Prop. (12.11.3.18) [Chevalley's Theorem]. Let G be a complex connected Lie group and $\mathfrak{g}$ the Lie algebra of G, $\mathfrak{h}$ the Cartan subalgebra of $\mathfrak{g}$, and W the Weyl group, then the restriction of functions induces a graded algebra isomorphism

$$\mathbb{C}[\mathfrak{g}]^G\cong\mathbb{C}[\mathfrak{h}]^W.$$

⌟

Proof: **?** □

Classifications

Prop. (12.11.3.19) [Simply-Connected Compact Lie Groups]. Any simply connected compact Lie groups is a product of the following types:

- $\mathrm{Spin}(n)$ for $n \geq 3$.
- $\mathrm{SU}(2)$ for $n \geq 2$.
- $\mathrm{Sp}(n)$ for $n \geq 1$.
- E_6, E_7, E_8, F_4, G_2.

⌟

Proof: ? □

4 Compact Lie Groups and Representations

Prop. (12.11.4.1). Any compact connected complex Lie group is Abelian. And it is a complex tori. So we only consider only compact real Lie groups. ⌟

Proof: Mimic the proof that Abelian variety is commutative(15.7.1.5), using a similar rigidity lemma. □

Cor. (12.11.4.2). $U(n)$ is not a complex Lie group, in particular not a complex algebraic variety. ⌟

Prop. (12.11.4.3). Let G be a compact connected Lie group with Lie algebra $\mathfrak{g}$ and center Z. Let G_{ss} be the connected subgroup of G corresponding to the Lie subalgebra $[\mathfrak{g}, \mathfrak{g}]$(12.11.3.12), then G_{ss} has finite center, and Z^0, G_{ss} are closed in G, and $G = Z^0 G_{ss}$. ⌟

Proof: Cf.[Kna96]P198. □

Prop. (12.11.4.4)[Compact Lie Group and Representations]. A compact topological group G is a real Lie group iff it has a faithful real f.d. representation. And in this case, it is a closed subgroup of $U(n)$ for some n. ⌟

Proof: If it has a faithful f.d. representation, then $G \subset GL(n, \mathbb{R})$ compact hence closed, thus a Lie subgroup by(12.11.1.22).

Conversely, if G is a Lie group, then we can choose a small nbhd U of $e \in G$ that contains no non-trivial subgroup of G(choose $\exp(\frac{1}{2}V)$ where exp is an diffeomorphism on V). Consider kernel K_π for irreducible representations π of G, then $\cap_\pi K_\pi = \varnothing$ by Gelfand-Raikov(11.10.2.22), in particular $\cap_\pi (K_\pi - U) = \varnothing$. But $G - U$ is compact, hence there are f.m. π_i that $\cap_i K_{\pi_i} \in U$, but by definition of U, $\cap_i K_{\pi_i} = \{e\}$, which gives a f.d. faithful representation of G, by(11.10.4.4). □

Prop. (12.11.4.5)[Reduction to Faithful Representations]. Let V be a faithful f.d. representation of a compact Lie group G and Y is an irreducible f.d. representation of G, then Y is a direct summand of $V^{\otimes n} \otimes V^{*\otimes m}$ for some $m, n \geq 0$. Moreover, if G is unimodular, we can take $m = 0$. ⌟

Proof: Cf.[Etingof, P175]. □

Remark (12.11.4.6). Theory of Representations of compact Lie groups are a special case of abstract harmonic analysis11.10. ⌟

Maximal Tori

Prop. (12.11.4.7) [Tori]. Any connected compact Abelian real Lie group is a torus. ⌟

Proof: By(12.12.3.2), the exponential map realizes $\mathfrak{g}$ as the universal cover of G, and the kernel is then a complete lattice Λ in $\mathbb{R}^n$, so $G \cong \mathbb{R}^n/\Lambda \cong (S^1)^n$. □

Prop. (12.11.4.8). The maximal tori in a compact Lie group G corresponds to the maximal Abelian subalgebras of $\mathfrak{g}$. ⌟

Proof: Let T be a maximal tori, then $\mathfrak{t}$ is maximal Abelian by fundamental theorem of Lie(12.11.3.12). Conversely, if $\mathfrak{t}$ is a maximal tori, then the corresponding Lie subgroup T is Abelian, and $\overline{T}$ is also Abelian. The Lie algebra of $T, \overline{T}$ are the same by maximality of $\mathfrak{t}$, so $T = \overline{T}$, and it is a torus by(12.11.4.7), and it is clearly maximal. □

Prop. (12.11.4.9). Let G be a compact connected Lie group with Lie algebra $\mathfrak{g}$, then any two maximal Abelian subalgebra of $\mathfrak{g}$ are conjugate via $\mathrm{Ad}(G)$. ⌟

Proof: Let $\mathfrak{t}, \mathfrak{t}'$ be two maximal Abelian subalgebra of $\mathfrak{g}$. As $\mathfrak{g}$ is reductive(3.7.5.3), if we choose $X \in \mathfrak{t}, X' \in \mathfrak{t}'$ that are not zero for any roots, then $Z_{\mathfrak{g}}(X) = T, Z_{\mathfrak{g}}(X') = T'$. Let $(\cdot,\cdot)$ be a invariant inner product on $\mathfrak{g}$ defined in(12.11.7.2), choose a $g_0 \in G$ that $(\mathrm{Ad}(g_0)X, X')$ is maximal, then $0 = ([Z, \mathrm{Ad}(g_0)X, X') = (Z, [\mathrm{Ad}(g_0)X, X'])$ for any $Z \in \mathfrak{g}$, so $\mathrm{Ad}(g_0)X \in Z_{\mathfrak{g}}(X') = \mathfrak{t}'$. Thus $\mathfrak{t}' \subset Z_{\mathfrak{g}}(\mathrm{Ad}(\mathfrak{g}_0)X) = \mathrm{Ad}(g_0)Z_{\mathfrak{g}}(X) = \mathrm{Ad}(g_0)\mathfrak{t}$, and the equality holds as $\mathfrak{t}'$ is maximal. □

Cor. (12.11.4.10) [Maximal Tori are Conjugate]. Let G be a compact connected Lie group, then any two maximal tori of G are conjugate via $\mathrm{Ad}(G)$. ⌟

Prop. (12.11.4.11). Let G be a compact connected Lie group, then any element of G is connected in a maximal torus. ⌟

Proof: By(12.12.3.2), this element is contained in a 1-parameter subgroup T of G, and $\overline{T}$ is also Abelian, so is a torus by(12.11.4.7). Then choose a maximal torus containing $\overline{T}$. □

Cor. (12.11.4.12). The center of G is contained in any maximal torus, by(12.11.4.10). ⌟

Prop. (12.11.4.13). Let S be a torus in a compact Lie group G and $g \in G$ that commutes with elements in S, then there is a torus containing both S and g. ⌟

Proof: Let A be the closure of $\cup_{i\in\mathbb{Z}} g^i S$, and A_0 the identity component of A, then as A is compact, A_0 is open in A and compact, so $\cup_{i\in\mathbb{Z}} g^i A_0 = A$, and also A/A_0 is a cyclic group. As A_0 is a torus, we can find $a \in A$ that the closure of $\{a^n | n \in \mathbb{Z}\}$ is A. By(12.12.3.2), let $a = \exp_G(X)$, then the closure of the 1-parameter group generated by X is a torus containing both S and g. □

Cor. (12.11.4.14). In a compact connected Lie group G, then centralizer of a torus T is connected. In fact, it is the union of maximal tori containing T. In particular, a maximal torus is self-centralizing. ⌟

Highest Weight Theory

Cf.[Compact Lie Groups, Sepanski].Chap7.

Examples of Representations

Prop. (12.11.4.15) [Representations of $SU(2)$]. $SU(2) \cong S^3$ is simply connected with Lie algebra $\mathfrak{sl}_2(\mathbb{R})$(12.12.0.7), thus we can use(12.11.3.14) and(18.8.1.14) to see that the representations of $SU(2)$ are all of the form W_n, where W_n is the representation of $SU(2)$ on the space of homogenous polynomials of degree n in two variables x, y induced by $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax+by \\ cx+dy \end{bmatrix}$. ⌟

Proof: Check the central character of the induced representations of Lie algebra. □

Prop. (12.11.4.16). Let $G = SO(n)$ for $n \not\equiv 2 \mod 4$. Show that:

1. For any element $g \in G$, g and g^{-1} are conjugate in $SO(n)$.
2. Any irreducible finite-dimensional $\mathbb{C}$-representation V of G is isomorphic to its dual.

⌟

Proof: 1: By(3.5.10.7), if $n = 2m+1$, g is orthogonally diagonal to a matrix of the form $\mathrm{diag}\{SO(2,\mathbb{R}), \ldots, SO(2,\mathbb{R}), 1\}$. Notice $SO(2,\mathbb{R}) = \{k_\theta, \theta \in (0, 2\pi]\}$, where $k_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$, and $k_\theta^{-1} = k_{-\theta} = k_\theta^t$. If we take $W = \mathrm{diag}\{\begin{bmatrix} & 1 \\ 1 & \end{bmatrix}, \ldots, \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}, (-1)^m\}$, then $W \in SO(n,\mathbb{R})$ and $WgW^{-1} = g^{-1}$.

If $n = 4k$, then g is orthogonally diagonal to a matrix of the form $\mathrm{diag}\{SO(2,\mathbb{R}), \ldots, SO(2,\mathbb{R})\}$. If we take $W = \mathrm{diag}\{\begin{bmatrix} & 1 \\ 1 & \end{bmatrix}, \ldots, \begin{bmatrix} & 1 \\ 1 & \end{bmatrix}\}$, then $W \in SO(n,\mathbb{R})$ and $WgW^{-1} = g^{-1}$.

2: Because $\chi_{V^*}(g) = \chi_V(g^{-1}) = \chi_V(g)$ as g, g' are in the same conjugacy class, V and V^* are isomorphic, because f.d. representations are determined by characters(3.6.1.13)(applied to the group algebra $\mathbb{C}[G]$). □

Maximal Compact Subgroup

For maximal compact subgroup of general locally compact subgroups, Cf.1.

Prop. (12.11.4.17) [Uniqueness for Semisimple Lie group]. Maximal compact subgroup exists by(11.10.1.47), and for a semisimple Lie group G, the maximal compact subgroup is unique up to conjugation. ⌟

Proof: Cf.[Wiki]. □

Prop. (12.11.4.18) [Examples of Maximal Subgroups].

- $O(n)$ is the maximal compact subgroup of $GL(n,\mathbb{R})$.
- $SO(n)$ is the maximal compact subgroup of $SL(n,\mathbb{R})$.
- $SO(m,n)$ is the maximal compact subgroup of $S(O(m) \times O(n))$.
- $SO(n)$ is the maximal compact subgroup of $SL(n,\mathbb{R})$.
- $SU(n)$ is the maximal compact subgroup of $SL(n,\mathbb{C})$.
- $SU(m,n)$ is the maximal compact subgroup of $S(U(m) \times U(n))$.
- $SO(n)$ is the maximal compact subgroup of $SO(n,\mathbb{C})$.

- $U(n)$ is the maximal compact subgroup of $GL(n,\mathbb{C})$.
- $SU(n)$ is the maximal compact subgroup of $SL(n,\mathbb{C})$.
- $Sp(n)$ is the maximal compact subgroup of $Sp(n,\mathbb{C})$, by(12.12.0.16).
- $Sp(m,n)$ is the maximal compact subgroup of $Sp(m)\times Sp(n)$.
- $Sp(n)$ is the maximal compact subgroup of $SL(n,\mathbb{H})$, by(12.12.0.16).
- $U(n)$ is the maximal compact subgroup of $O^*(n)$, by(12.12.0.16).

And the above maximal compact subgroups are also deformation retractions. ⌟

Proof: This follows from polar decomposition(12.11.5.2), notice that the projection of a compact group is a compact group in $\mathbb{R}^n$, so it is trivial. □

5 Decompositions

Prop. (12.11.5.1) [Cartan Decomposition]. Let $G=GL(n,\mathbb{R}), K=O(n)$ or $G=GL(n,\mathbb{R})^+, K=SO(n)$, then every double coset $K\backslash G/K$ has a unique representation of diagonal matrix D with decreasing positive entries. ⌟

Proof: For the existence, given g, consider $S=g^tg=k_1^{-1}\operatorname{diag}(\lambda_1,\ldots,\lambda_n)k_1$, where $k_1\in SO(n)$(3.5.10.18). Then consider

$$k_2=gk_1^{-1}\operatorname{diag}(\lambda_1^{-1/2},\ldots,\lambda_n^{-1/2})$$

it is orthogonal and $g=k_2\operatorname{diag}(\lambda_1^{1/2},\ldots,\lambda_n^{1/2})k_1$.

For the uniqueness, consider $gk_1^{-1}\operatorname{diag}(\lambda_1^{-1/2},\ldots,\lambda_n^{-1/2})$ is orthogonal, thus $k_1Sk_1^{-1}$ is diagonal with decreasing positive entries, thus uniquely defined. □

Prop. (12.11.5.2) [Polar Decomposition for Linear Groups]. Let $G\subset GL(n,\mathbb{C})$ be a closed linear group that is defined by the a family of real valued polynomials in the real and imaginary parts of entries of G, and G is closed under conjugation. Let $K=G\cap U(n)$, and let $\mathfrak{p}$ be the subspace of Hermitian matrices in $\mathfrak{g}$, then the map $K\times\mathfrak{p}\to G:(k,X)\mapsto k\exp(X)$ is a homeomorphism. In particular, G has K as deformation retracts. ⌟

Proof: The $GL(n,\mathbb{C})$ case follows from(11.9.4.20) and(12.12.3.2), and for the general case, it suffices to show if $g\in G$ and $g=k\exp(X)$, then $X\in\mathfrak{g}$: By hypothesis, $g^*g=e^{2X}\in G$. Take a basis that $2X=\operatorname{diag}(a_1,\ldots,a_n)$ with a_i real, then $e^{2kX}=\operatorname{diag}(e^{ka_1},\ldots,e^{ka_n})$ are all in G. Then it can be easily shown any polynomial that vanishes at all such e^{2kX} vanishes on all e^{2tX}, thus $X\in\mathfrak{g}$. □

Cor. (12.11.5.3). $GL(n,\mathbb{R})\cong P\cdot O(n)$, where P is the set of positive symmetric matrix, by(12.12.3.2). ⌟

Prop. (12.11.5.4) [QR-Decomposition].

- Any real matrix A has the form $A=QR$ where Q is orthogonal and R is upper triangular with positive diagonal entries. Moreover, if A is invertible, then the decomposition is unique.
- Any complex matrix A has the form $A=QR$ where Q is unitary and R is upper triangular with positive diagonal entries. Moreover, if A is invertible, then the decomposition is unique.
- Any Quaternion matrix A has the form $A=QR$ where $Q\in U(n,\mathbb{H})$(12.12.0.16) and R is upper triangular with positive diagonal entries. Moreover, if A is invertible, then the decomposition is unique.

⌟

Proof: We only prove for $GL(n,\mathbb{R})$, the rest is similar. Use Gram-Schmidt orthogonalization: choose a basis $v = \{v_1,\dots,v_n\}$ of V and A acts on V, then A maps $\{v_1,\dots,v_n\}$ to a set $\{w_1,\dots,w_n\}$. Then we can define an orthonormal basis $\{e_1,\dots,e_n\}$ that $v_k \in span\{e_1,\dots,e_k\}$. Now let $\{w_1,\dots,w_n\} = \{e_1,\dots,e_n\}R$, then R is upper triangular, and $Q = [e_1,\dots,e_n]_v$ is orthogonal, and $A = QR$. We can make diagonal entries of R positive by left multiplying a diagonal orthogonal matrix.

To show the uniqueness when A is invertible, let $A = Q_1R_1 = Q_2R_2$, then $A^tA = R_1^tR_1 = R_2^tR_2$. Then $(R_2)^{-t}R_1^t = R_2R_1^{-1}$, where the LHS is lower-triangular and the RHS is upper-triangular, which means both of them are diagonal. Then if α_i are the diagonal entries of R_1 and β_i are the diagonal entries of R_2, then $\alpha_i/\beta_i = \beta_i = \alpha_i$, which means $\alpha_i = \beta_i$, and $R_2R_1^{-1} = 1$. □

Prop. (12.11.5.5) [Bruhat Decomposition]. Let K be a field, B be the set of upper-triangular matrices, N be the set of unipotent upper-triangular matrices, then

$$GL(n,K) = BWB = BWN$$

where W is the set of permutation matrices, B is the invertible upper triangular matrices, and the decomposition is a disjoint union w.r.t. W.

Moreover, if K is a topological field, there is a lexicographical stratification $0 = W_0 \subset W_1 \subset \dots \subset W_{n!}$ of $GL(n,K)$ that W_k is closed in W_{k+1} and each $W_{k+1}\backslash W_k$ is a double coset BwB. ⌟

Proof: For any matrix $M \in GL(n,K)$, consider the first column, then there is a lowest term a_{i_11} that are not zero, then we can left multiply an upper triangular matrix b_1 s.t. the first column of b_1M has only one nonzero entry $a_{i_11} = 1$, then consider the second column but ignore the k-th row, we can find a lowest term a_{i_22} that is non-zero, then left multiply an upper triangular matrix b_2 that the second column of b_2b_1M has only one non-zero entry $a_{2i_2} = 1$. Now continuing this way, we find a permutation σ that only the entries a_{ij} that $j \geq \sigma^{-1}(i)$ are non-zero. Then we can find an upper triangular matrix c that $b_nb_{n-1}\dots b_1Mc$ is a permutation matrix $M_{\sigma^{-1}}$.

So we proved $BWB = GL(n,K)$. Now it suffices to show if $M_{\sigma_1}^{-1}bM_{\sigma_2} \in B$ for some $b \in B$, then $\sigma_1 = \sigma_2$: Because $M_\sigma = \sum_i e_{\sigma(i)i} = \sum_i e_{i\sigma^{-1}(i)}$,

$$M_{\sigma_1^{-1}}bM_{\sigma_2} = \sum_{ij} b_{\sigma_1(i)\sigma_2(j)}e_{ij}.$$

This is an element in B, both its $(\sigma_1^{-1}(k),\sigma_2^{-1}(k))$-entry is $b_{kk} \neq 0$, thus $\sigma_1^{-1}(k) \leq \sigma_2^{-1}(k)$, which implies $\sigma_1 = \sigma_2$. □

Cor. (12.11.5.6). If N is the group of unipotent upper triangular matrices, then $GL(n,L) = BWN$. ⌟

Prop. (12.11.5.7) [Smith Normal Form]. Let R be a PID, and K its fraction field. Choose a representative $\mathcal{P}$ for associativity classes of any prime in R(to eliminate the distraction of units), then there is complete set of representatives for the double cosets of $GL(n,R)\backslash GL(n,K)/GL(n,R)$ consisting of diagonal matrices $\text{diag}(f_1,\dots,f_n)$, where $f_i \in K$ are products of elements in $\mathcal{P}$, and f_k divides f_{k+1}. Notice $GL(n,R)$ is the matrices with unit determinants in R. ⌟

Proof: For the uniqueness, clearly the row operators doesn't change the greatest common divisor of $k \times k$ minors of M for any k(change by a scalar but the diagonal entries are monic), thus the entries are determined by the minors of M.

For the existence, for any $g\in GL(n,K)$ there is an $r\in R$, that rg has coefficients in R, and also r is a product of elements in $\mathcal{P}$. let M be the submodule of R^n generated by the rows of rg, then by the elementary divisor theorem(3.2.4.24), there exists a basis ξ_i for R^n and $d_i\in R$ that $d_i|d_{i+1}$, and $\{d_i\xi_i\}$ form a basis of M. we may assume d_i are products of elements in $\mathcal{P}$. Then the matrix ξ with rows ξ_i are in $GL(n,R)$, and the rows of the matrix $\mathrm{diag}(d_1,\ldots,d_n)\xi$ span the same module as rg. Then

$$K_1rg=\mathrm{diag}(d_1,\ldots,d_n)\xi$$

for some $K_1\in GL(n,R)$, so g are in the same double coset as $\mathrm{diag}(r^{-1}d_1,\ldots,r^{-1}d_n)$. □

Prop. (12.11.5.8) [Iwasawa Decomposition]. ⌟

6 Semisimple Lie Groups

Def. (12.11.6.1) [Semisimple Lie Group]. A **semisimple/solvable/nilpotent/simple Lie group** is a Lie group with a semisimple/solvable/nilpotent/simple Lie algebra. ⌟

Def. (12.11.6.2) [Adjoint Lie Group]. An **adjoint Lie group** is a semisimple real Lie group(12.11.6.1) with trivial center. ⌟

Prop. (12.11.6.3). Let G be a semisimple complex Lie group, then the center Z of G is contained in G^c, thus the restriction of f.d. representations of G to G^c is an equivalence of categories. ⌟

Proof: Cf.[Etingof, P209] □

Maximal Tori

Prop. (12.11.6.4). Let G be a complex semisimple Lie group with Lie algebra $\mathfrak{g}$, compact form $\mathfrak{g}^c$ and compact part G^c, then ⌟

7 Analysis

Lemma (12.11.7.1). Let H be a Lie subgroup of G and $g\notin H$, then there is a smooth function Φ on G that $\Phi(xh)=\Phi(x)$ for any $x\in G,h\in H$, and $\Phi(H)=0$, yet $\Phi(g)\neq 0$. ⌟

Proof: Because H is closed, there is a nbhd U of g disjoint from H and a function φ supported in U. Then $\Phi(x)=\int_H\varphi(xh)dh$ satisfies the desired condition. □

Bi-Invariant Metric

Lemma (12.11.7.2). Bi-invariant metric exists in a compact Lie group. ⌟

Proof: Because the Haar measure on a compact metric is bi-invariant. Choose a Riemann metric and set

$$\langle V,W\rangle=\int_{G\times G}\langle L_{\sigma*}R_{\tau*}(V),L_{\sigma*}R_{\tau*}(W)\rangle d\mu(\sigma)d\mu(\tau).$$

Note that L_* and R_* commute. □

Prop. (12.11.7.3). For a left-invariant metric on a connected Lie group G, if it is bi-invariant, then the inner product at the origin e is invariant under $\mathfrak{g}$(3.7.1.13), and the converse is also true if G is connected. ⌟

Proof: If the metric is invariant, then for any $X, Y, Z \in \mathfrak{g}$, $\langle \mathrm{Ad}(\exp(tX))Y, \mathrm{Ad}(\exp(tX))Z\rangle = \langle X, Y\rangle$, so we take derivation w.r.t. t to get

$$\langle \mathrm{ad}(X)Y, Z\rangle + \langle Y, \mathrm{ad}(X)Z\rangle = 0$$

by(12.11.1.12).

Conversely, if this is invariant, then using $\exp(tX) = \exp((t-t_0)X)\exp(t_0X)$, we get $\partial(\langle \mathrm{Ad}(\exp(tX))Y, \mathrm{Ad}(\exp(tX))Z\rangle)/\partial t = 0$ for all t, thus $\langle \mathrm{Ad}(\exp(tX))Y, \mathrm{Ad}(\exp(tX))Z\rangle = \langle X, Y\rangle$, and it is invariant under right actions by $\exp(tX)$ also. As G is generated by the elements $\exp(X)$(4.12.1.3), it is right-invariant under G. □

Prop. (12.11.7.4). If G is a Lie group with a bi-invariant metric, then

$$\nabla_X Y = 1/2[X, Y], \quad R(X, Y)Z = 1/4[[X, Y], Z], \quad K(\sigma) = 1/4\Big|[X, Y]\Big|^2.$$

So it has non-positive sectional curvature, and its curvature is non-negative, and all 1-parameter subgroups are geodesics from e. ⌟

Proof: It suffices to show that $\langle Z, \nabla_X Y\rangle = 1/2\langle Z, [X, Y]\rangle$ for any Z, and this follows from(12.3.3.16). The second follows from the first and the definition(12.3.3.11). □

Cor. (12.11.7.5). A bi-invariant Lie group with $\mathfrak{g}$ having trivial center is compact and $\pi_1(G)$ finite. ⌟

Proof: The Ricci curvature has a positive lower bound, otherwise for some X, $[X, Y] = 0$ for all Y, thus X is in the center. Hence we use Myer theorem(12.3.5.20). □

Cor. (12.11.7.6). If G has a bi-invariant metric, then the exp map $\mathfrak{g} \to G$ is surjective. ⌟

Proof: Because exp is defined for any $X \in \mathfrak{g}$, and for any $g \in G$ and $v \in T_g(G)$, $\exp_p(v) = L_g(\exp(dL_{g^{-1}})_g(v))$ because L_g is an isomorphism of Riemann manifolds. So by Hopf-Rinow(12.3.3.46), G is complete. Thus for any q, there is a geodesic connecting e, q, which is a 1-parameter subgroup, thus $q = \exp(X)$ for some $X \in \mathfrak{g}$. □

Prop. (12.11.7.7) [Structure of bi-invariant Lie groups]. A simply-connected Lie group with a bi-invariant metric is equal to $G' \times R^k$, G' compact. ⌟

Proof: Because the orthogonal complement of the center of $\mathfrak{g}$ is a Lie algebra, G is like $G' \times R^k$, and a simply connected abelian Lie group is R^k **?**. □

12.12 Classical Groups

In this subsection, classical groups(9.3.5.1) over Archimedean fields and related Lie groups are studied.

References are [Symmetry, Representations and Invariants]

For more classical groups, Cf.[Classical Groups Baker].

Notation (12.12.0.1).

- Use notations as in Lie Groups.

⌟

Def. (12.12.0.2) [Examples of Classical Groups]. Let $\mathbb{K}$ be either $\mathbb{R}, \mathbb{C}$,

- For any associative algebra $\mathbb{K}$ over a field, the **general linear group** $GL(n, \mathbb{K})$ is the subgroup of $M_n(\mathbb{K})$ consisting of invertible matrices.
- The **unitary group** $U(n)$ is the subgroup of $GL_n(\mathbb{C})$ consisting of matrices fixing a non-degenerate Hermitian form.
- The **special unitary group** $SU(n) = U(n) \cap SL_n(\mathbb{C})$.
- The **pseudo-unitary groups** $U(p, q, \mathbb{K})$: If $\mathbb{K} = \mathbb{R}$, it is the subgroup of $GL(n, \mathbb{R})$ consisting of matrices preserving a bilinear form of signature (p, q). If $\mathbb{K} = \mathbb{C}$, it is the subgroup of $GL(n, \mathbb{C})$ consisting of matrices preserving a Hermitian form of signature (p, q). If $\mathbb{K} = \mathbb{H}$, it is the subgroup of $GL(n, \mathbb{H})$ consisting of matrices preserving a non-degenerate quoternionic Hermitian form of signature (p, q)(3.5.12.7).
- The **quoternionic orthogonal group** $O^*(2n)$ is the subgroup of $GL(n, \mathbb{H})$ consisting of matrices preserving a non-degenerate quoternionic skew-Hermitian form(3.5.12.7). $SO^*(2n)$ is the subgroup of $O^*(2n)$ consisting of elements of determinant 1.
- $PU(n)$ is the quotient group of $SU(n)$(or $U(n)$) by scalar matrices.

⌟

Proof: $GL_n(\mathbb{K})$ has a natural smooth structure as an open subset of $\mathbb{K}^{n^2}$, and the multiplication map is clearly smooth, so it is a Lie group by(12.11.1.1). The other groups are closed subgroups of $GL_n(\mathbb{K})$, so they have unique smooth manifold structure making them Lie subgroups of $GL_n(\mathbb{K})$, by(12.11.1.22)(12.11.1.16). Finally the quotient group by normal closed subgroups have natural Lie group structure by(12.11.1.28). □

Prop. (12.12.0.3)[Classification of Transformations]. Let $\alpha \in SL(2, \mathbb{R})$ and $\alpha \neq \mathbf{I}$, then by Jordan decomposition, α is conjugate to a matrix of one the two following types:

$$\begin{bmatrix} \lambda & 1 \\ & \lambda \end{bmatrix}, \quad \begin{bmatrix} \lambda & \\ & \mu \end{bmatrix}, \lambda \neq \mu$$

according as it has repeated eigenvalues or distinct eigenvalues. In the first case, α is called **parabolic**, and in the second case, if $|\lambda/\mu| = 1$, it is called **elliptic**, If λ/μ is real and positive, it is called **parabolic**, and called **loxodromic** otherwise.

- If $\alpha \in SL_2(\mathbb{R})$ is parabolic, then it has a unique real eigenvector, which means it has a unique fixed point in $\mathbb{R} \cup \infty$.
- If $\alpha \in SL_2(\mathbb{R})$ is elliptic, then α has two conjugate eigenvectors, which means it has exactly one fixed point z in $\mathscr{H}$, and a second fixed point, namely $\overline{z}$, in the lower half plane.

- If $\alpha \in SL_2(\mathbb{R})$ is hyperbolic, then it has two real eigenvectors, which means it has two distinct fixed points in $\mathbb{R} \cup \infty$.

⌟

Prop. (12.12.0.4)[Iwasawa-Decomposition]. Any element of $GL(2,\mathbb{R})^+$ has a unique representation of the form(12.11.5.4):

$$g = \begin{bmatrix} u & \\ & u \end{bmatrix} \begin{bmatrix} y^{1/2} & xy^{-1/2} \\ & y^{-1/2} \end{bmatrix} k_\theta$$

where $k_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$. So by(11.10.1.39) and(11.10.1.19) the Haar measure is calculated to be $\mathrm{d}g = \frac{1}{2\pi}\frac{\mathrm{d}u}{u}\frac{\mathrm{d}x\mathrm{d}y}{y^2}\mathrm{d}\theta$, and it is unimodular by(11.10.1.22). (Notice the upper triangular matrix group $B \subset GL(2,\mathbb{R})^+$ is not unimodular). ⌟

Proof: For the calculation of Haar measure, notice that it suffices to calculate for u, x, y and it is

$$\frac{\mathrm{d}(uy^{1/2})\mathrm{d}(uy^{-1/2})\mathrm{d}(uxy^{-1/2})}{(uy^{1/2})^2 uy^{-1/2}} = \frac{\mathrm{d}x\mathrm{d}(uy^{1/2})\mathrm{d}(uy^{-1/2})}{u^2 y} = \frac{\mathrm{d}x\mathrm{d}y\mathrm{d}u}{uy^2}$$

□

Cor. (12.12.0.5). Any element of $SL(2,\mathbb{R})$ has a unique representation of the form

$$g = \begin{bmatrix} e^{\frac{u}{2}} & 0 \\ 0 & e^{-\frac{u}{2}} \end{bmatrix} \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} k_\theta.$$

And the Haar measure is given by $\mathrm{d}g = \frac{1}{2\pi}\mathrm{d}u\mathrm{d}x\mathrm{d}\theta$ by similar calculation, which is unimodular. ⌟

Prop. (12.12.0.6). $\mathscr{H}$ is a homogenous space for $\mathrm{PGL}(2,\mathbb{R})$, and $\mathrm{Stab}_{\mathrm{PGL}(2,\mathbb{R})}(\mathrm{i}) = SO(2,\mathbb{R})$. Also it fixes the hyperbolic metric $\mathrm{d}s^2 = y^{-2}\mathrm{d}x\mathrm{d}y$. ⌟

Proof: This follows from the Iwasawa decomposition(12.12.0.4). □

Prop. (12.12.0.7)[$SU(2)$].

$$SU(2) = \{A_{\alpha,\beta} = \begin{bmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{bmatrix}, \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1\}$$

is isomorphic to the group of unit quaternions and diffeomorphic to S^3. The Lie algebra of $SU(2)$ is isomorphic to $\mathfrak{sl}_2(\mathbb{R})$. ⌟

Proof: Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SU(2)$, then

$$a\overline{a} + b\overline{b} = 1, \quad a\overline{c} + b\overline{d} = 0, \quad c\overline{c} + d\overline{d} = 1, ac - bd = 1.$$

So $(c,d) = \lambda.(-\overline{b}, \overline{a})$, and we can calculate $\lambda = 1$. So the first assertion follows.

By(3.5.12.4), $SU(2)$ is isomorphic to the group of unit quaternions, which is clearly isomorphic to S^3. □

Prop. (12.12.0.8)[Actions of $SU(2)$].

- There is a double covering of Lie groups $SU(2) \to SO(3)$ with kernel $\{\pm 1\}$.
- There is a double covering of Lie groups $SU(2) \times SU(2) \to SO(4)$ with kernel $\{\pm 1\}$.

⌟

Proof: 1: Regard $SU(2)$ as the unit quaternions and $SO(3)$ the transformation group of pure unit quaternions, then $SU(2) \to SO(3)$ is given by

$$u \mapsto (v \mapsto uv\overline{u}).$$

Because $u \cdot \overline{u}$ preserves orthogonality relations, it preserves the space of pure quaternions, so it has image in $O(3)$. But it has image in $SO(3)$ because $SU(2) \cong S^3$ is connected. Its kernel is in the center of $\mathbb{H}$, so must be ± 1. Now(12.11.3.10) shows this is a covering space map.

2: Consider the action $SU(2) \times SU(2)$ on the section of unit vectors of $\mathbb{H}$: $(u,v)(z) = uzv^{-1}$. if (u,v) is in the kernel of this map, then $uv^{-1} = 1$, so $u = v$,and u is in the center of $\mathbb{H}$, so $u = v = \pm 1$. Because $\dim SU(2) = 3$ and $\dim SO(4) = 6$, (12.11.3.10) shows this is a double cover. □

Prop. (12.12.0.9).

- There is a double cover $SU(4) \to SO(6, \mathbb{R})$ with kernel $\{\pm 1\}$.
- There is a double cover $SL(4, \mathbb{C}) \to SO(6, \mathbb{C})$ with kernel $\{\pm 1\}$.
- There is a double cover $Sp(4, \mathbb{C}) \to SO(5, \mathbb{C})$ with kernel $\{\pm 1\}$.

⌟

Proof: 1: $SU(4)$ acts on a 4-dimensional Hermitian space V. Then it acts on the Hermitian space $\wedge^2 V$. Consider the Hodge star operator $* : \wedge^2 V \to \wedge^2 V$(12.1.3.9), it is an anti-linear operator, $*^2 = \mathrm{id}$ and $*$ commutes with $SU(4)$ action. Then $W = \ker(* - \mathrm{id})$ is a real vector space of dimension 6 that $SU(4)$ acts on. This kernel of this action is the same as the kernel of the action $\wedge^2 V$, which is $\{\pm 1\}$.

The Hermitian form induces a symmetric form on W: Take a conjugation on V, because $V = W \oplus iW$, $W = \mathrm{Im}(* + \mathrm{id})V$. So for $a, b \in W$, let $a = *c + c, b = *d + d$, then $(a,b)\omega = ((*a, *b) + (*a, b) + (a, *b) + (a,b))\omega = *a \wedge b + \overline{a \wedge b} + a \wedge b + \overline{*a \wedge b}$ is a real form. Then this representation induces a map $SU(4) \to SO(6)$(because $SU(4)$ is connected). Because $\dim SU(4) = \dim SO(6) = 6$, it is a double cover by(12.11.3.10).

2: $SL(4, \mathbb{C})$ acts on a 4-dimensional complex vector space V, then it acts on the space $W = \wedge^2 V^*$. We construct a non-degenerate bilinear form on W given by $\wedge : W \times W \to \wedge^4 V^* \cong \mathbb{C}$. Then $SL(4, \mathbb{C})$ preserves this bilinear form, thus induces a map $SL(4, \mathbb{C}) \to SO(6, \mathbb{C})$. The kernel of this map is $\{\pm 1\}$, because if A preserves all $v_1^* \wedge v_2^*$, then $Av_1^* \wedge Av_2^* = v_1^* \wedge v_2^*$, so $Av_1^* \wedge Av_2^* \wedge v_i^* = 0$, so $Av_1^* \in \{v_1^*, v_2^*\}$, or $Av_2^* \subset \{Av_1^*, v_1^*\} \cap \{Av_1^*, v_2^*\} = Av_1^*$, then $Av_1^* \wedge Av_2^* = 0$, contradiction. So $Av_1^* \subset \{v_1^*, v_2^*\}$. v_1, v_2 is arbitrary, thus A is diagonal, and it is clear $A = \pm 1$. Finally, $SL(4, \mathbb{C}) \to SO(6, \mathbb{C})$ is a double cover by(12.11.3.10).

3: The representation of $SL(4, \mathbb{C})$ on $W = \wedge^2 V^*$ restricts to a representation of $Sp(4, \mathbb{C})$, and it fixes the vector $\sigma = v_1^* \wedge v_2^* + v_3^* \wedge v_4^*$ by definition, so it also fixes the orthogonal $\{\sigma\}^\perp$, thus inducing a map $Sp(4, \mathbb{C}) \to SO(5, \mathbb{C})$ with kernel $\{\pm 1\}$, which is a double cover by(12.11.3.10). □

Prop. (12.12.0.10) [$SU(1,1)$ and $SL(2, \mathbb{R})$]. Let $SL(2, \mathbb{C})$ act continuously on $\mathbb{P}^1(\mathbb{C})$ by $\gamma(z) = \frac{az+b}{cz+d}$ where $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then

- The stabilizer of the unit disk $\mathbb{D}$ is
$$SU(1,1)=\{\begin{bmatrix}a & b\\ \overline{b} & \overline{a}\end{bmatrix}||a|^2-|b|^2=1\}.$$
- $SU(1,1)$ is conjugate to $SL(2,\mathbb{R})$ in $SL(2,\mathbb{C})$.
- The subgroup of $SU(1,1)$ fixing $0\in\mathbb{D}$ is the subgroup of rotations $\{\mathrm{diag}(e^{\mathrm{i}\,\theta/2},e^{-\mathrm{i}\,\theta/2})\}$.

⌟

Proof: 3: This follows from Schwartz lemma(11.5.1.3).

1, 2: We first describe $SU(1,1)$:
$$SU(1,1)=\{\begin{bmatrix}a & b\\ c & d\end{bmatrix}:|a|^2-|c|^2=1,\quad a\bar{b}-c\bar{d}=0,\quad |b|^2-|d|^2=-1,\quad ad-bc=1\}$$
which means $(b,d)=\lambda(\overline{c},\overline{a})$, and $\lambda=1$.

Let $C=\frac{1}{\sqrt{2}e^{2\pi i/4}}\begin{bmatrix}1 & -i\\ 1 & i\end{bmatrix}$, then C induces an isomorphism between $\mathscr{H}$ and $\mathbb{D}$, because $\frac{z-i}{z+i}\in\mathbb{D}$ iff $|z-i|<|z+i|$ iff z is in the upper half plane. By this isomorphism and item 3, the element of $SL(2,\mathbb{C})$ stabilizing $\mathbb{D}$ and fixing i is of the group $SO(2,\mathbb{R})\subset SL(2,\mathbb{R})$.

Notice that $SL(2,\mathbb{R})$ preserves $\mathcal{H}$ by(11.4.1.9), and it acts transitively on it because $\sqrt{y}\begin{bmatrix}y & x\\ & 1\end{bmatrix}$ maps i to $x+iy\in\mathcal{H}$. Now if $\gamma\in SL(2,\mathbb{C})$ stabilizes $\mathscr{H}$, then γg fixes i for some $g\in SL(2,\mathbb{R})$, thus $\gamma g\in SL(2,\mathbb{R})$, thus $\gamma\in SL(2,\mathbb{R})$. Thus we have shown the stabilizer of $\mathcal{H}$ is $SL(2,\mathbb{R})$. Then the stabilizer of $\mathbb{D}$ is
$$\begin{aligned}C\cdot SL(2,\mathbb{R})C^{-1}&=\{\frac{1}{2i}\begin{bmatrix}1 & -i\\ 1 & i\end{bmatrix}\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}i & i\\ -1 & 1\end{bmatrix}|a,b,c,d\in\mathbb{R},ad-bc=1\}\\ &=\{\frac{1}{2}\begin{bmatrix}a+d+(b-c)i & a-d-(b+c)i\\ a-d+(b+c)i & a+d-(b-c)i\end{bmatrix}|a,b,c,d\in\mathbb{R},ad-bc=1\}\end{aligned}$$
which is exactly $SU(1,1)$. So we get 1 and 2. □

Cor. (12.12.0.11) [Upper Half Plane $\mathscr{H}$]. By(11.4.7.8), the groups $GL(2,\mathbb{R})$ preserves the upper plane $\mathscr{H}$, by(11.4.1.9). The action of SL(2; $\mathbb{R}$) on $\mathscr{H}$ is transitive and the stabilizer of i is $SO(2,\mathbb{R})$, thus we have $\mathcal{H}\cong SL(2;\mathbb{R})/SO(2;\mathbb{R})$. ⌟

Prop. (12.12.0.12)[$Sp(2,\mathbb{K})$ and $SL(2,\mathbb{K})$]. For any field $\mathbb{K}$, $Sp(2,\mathbb{K})\cong SL(2,\mathbb{K})$: They both consists of linear maps preserving the differential form $dx\wedge dy$. ⌟

Prop. (12.12.0.13) [Center of $SU(p,q)$]. $Z_{U(p,q)}(SU(p,q))$ are all scalar matrices. ⌟

Proof: Firstly we consider $Z_{U(2)}(SU(2))$, if $A\in Z(SU(2))$, then it commutes with $\mathrm{diag}(i,-i)$, so A is a scalar. Similarly, If $A\in Z_{U(1,1)}(SU(1,1))$, then A commutes with $\mathrm{diag}(i,-i)$, thus A is a scalar.

If $X\in Z(SU(p,q))$ is not a scalar matrix, then it has two eigenvectors s,t with different eigenvalues. Consider the space V generated by s,t and its orthogonal complement, then X restricted to this space is in the center of $U(V)$. Now $SU(V)\cong SU(1,1)$ or $SU(2)$, both have the set of scalar matrices as center, so X cannot have different eigenvalue, contradiction. Thus X is a scaler matrix. □

Prop. (12.12.0.14)[$PGL(2,\mathbb{C})\cong SO(3,\mathbb{C})$]**.** $V\cong\mathbb{C}^2$ has a natural symmetric form $(x,y)\mapsto x\wedge y\cong\mathbb{C}$, and this form is preserved by $SL(2,\mathbb{C})$ by definition. The kernel of this map is $\{\pm 1\}$. Thus $SL(2,\mathbb{C})$ acts on $\mathrm{Sym}^2(V)$, thus induces a map $PGL(2,\mathbb{C})\to SO(3)$, which an isomorphism by(12.11.3.10). ⌟

Prop. (12.12.0.15) [Real and Complex Matrices]. $GL_n(\mathbb{C})$ can be embedded into $GL_{2n}(\mathbb{R})$, with determinant $|\det|^2$. And in this way, $U(n)$ is mapped into $O(2n,\mathbb{R})$. Also, $O(n,\mathbb{R})$ embeds into $U(n)$ diagonally. ⌟

Proof:

$$X+iY\mapsto\begin{bmatrix}X & -Y\\ Y & X\end{bmatrix}\sim\begin{bmatrix}X & -Y\\ iX+Y & X-iY\end{bmatrix}\sim\begin{bmatrix}X+iY & Y\\ 0 & X-iY\end{bmatrix}$$

□

Prop. (12.12.0.16) [Symplectic Groups].

- $U(p,q,\mathbb{H})=Sp(2n,\mathbb{C})\cap U(2p,2q,\mathbb{C})$. $U(n,\mathbb{H})=U(n,0,\mathbb{H})$ is also denoted by $Sp(n)$, called the **compact symplectic group**.
- $O^*(2n)=U(n,n)\cap O(2n,\mathbb{C})$.
- $Sp(2n,\mathbb{C})=SL(n,\mathbb{H})$.
- $Sp(2n,\mathbb{R})\cap O(2n,\mathbb{R}) = Sp(2n,\mathbb{R})\cap GL(n,\mathbb{C}) = O(2n,\mathbb{R})\cap GL(n,\mathbb{C}) = U(n) = \{\begin{bmatrix}X & -Y\\ Y & X\end{bmatrix},\quad X+iY\in U(n)\}$.

⌟

Proof: 1: By(3.5.12.9), notice that any $\mathbb{C}$-linear automorphism preserving B_1 and B_2 is $\mathbb{H}$-linear.

2: By(3.5.12.9), notice that any $\mathbb{C}$-linear automorphism preserving B_1 and B_2 is $\mathbb{H}$-linear.

3: If $A\in Sp(2n,\mathbb{R})\cap O(2n,\mathbb{R})$, then $AA^t=A^tA=1, A^tJA=1$, then $AJ=JA$. The rest and the other identities are easy by(12.12.0.15). □

1 Spin Groups

Prop. (12.12.1.1). Let $\mathrm{Cl}_{r,s}$ denote the real Clifford algebra of signature $r-s$, then

$$\mathrm{Cl}_{1,0}\cong\mathbb{C},\quad Cl_{0,1}\cong\mathbb{R}\oplus\mathbb{R},\quad \mathrm{Cl}_{2,0}\cong\mathbb{H}\subset M(2,\mathbb{C}),\quad Cl_{0,2}\cong R(2)=M(2,\mathbb{R}),$$

And we have

$$Cl_{n+2,0}\cong Cl_{0,n}\otimes Cl_{2,0},\quad Cl_{0,n+2}\cong Cl_{n,0}\otimes Cl_{0,2}.$$

by the mapping $e_i\to e_i\otimes e_1'e_2'$, $e_{n+j}\to 1\otimes e_j'$.

So we have

$$Cl_{n+8,0}\cong Cl_n\otimes\mathbb{R}(16),\quad \mathbb{C}l_{n+2,0}=Cl_{n+2,0}\otimes\mathbb{C}=\mathbb{C}l_{n,0}\otimes\mathbb{C}(2).$$

because $\mathbb{H}\otimes\mathbb{C}=\mathbb{C}(2)$, and

$$\begin{bmatrix} n & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7\\ Cl_{n,0} & \mathbb{R} & \mathbb{C} & \mathbb{H} & \mathbb{H}\oplus\mathbb{H} & \mathbb{H}(2) & \mathbb{C}(4) & \mathbb{R}(8) & \mathbb{R}(8)\oplus\mathbb{R}(8)\\ \mathbb{C}l_{n,0} & \mathbb{C} & \mathbb{C}\oplus\mathbb{C} \end{bmatrix}$$

The Clifford algebra is a $\mathbb{Z}_2$-graded algebra, $Cl=Cl^0\otimes Cl^1$ and $Cl_{n-1}\cong Cl_n^0$ by the mapping $e_i\to e_i\otimes e_{n+1}$. This is in fact the decomposition of the chirality operator $\Gamma=(-1)^{\lfloor\frac{n+1}{2}\rfloor}e_1e_2\dots e_n, \Gamma^2=1$. ⌟

Prop. (12.12.1.2). For n even, $\mathbb{C}(V)$ is naturally isomorphic to $\mathrm{End}_{\mathbb{C}}(\Lambda^* W)$, where $W = \{\frac{1}{\sqrt{2}}(e_{2i-1} - ie_{2i})\}$. This isomorphism is not obvious and restrict to a Spinor representation of $\mathrm{Spin}(n)$ and $\rho(\Gamma)^2 = 1$ induce two representations of $Cl(n)^0$, in particular $\mathrm{Spin}(n)$, called the **(half Spinor representations)**. This has a unique extension to representation of Spin^c. $\wedge^* W$ comes with a Hermitian metric which is preserved by the action of $\mathrm{Pin}(n)$ (check). So the image is $\mathrm{SO}(n)$ is in $SO(\wedge^* W)$. Cf.[Jost Geometric analysis P72]. ⌟

Def. (12.12.1.3) [Spin(n)]. denote $\mathrm{Pin}(n)$ as the group in Cl_n generated by v_i of norm 1. Because $v_i \cdot v_i = -1$, it is a group. And denote $\mathrm{Spin}(n)$ as the subgroup of $\mathrm{Pin}(n)$ generated by even number of v_is. ⌟

Prop. (12.12.1.4) [Action of Spin(n)]. The conjugation action $Ad(v) = v(-)v$ =reflection w.r.t v, maps $\mathrm{Pin}(n)$ to $O(n)$ and $\mathrm{Spin}(n)$ to $SO(n)$. The kernel of this mapping is $\{\pm 1\}$ when n is even. This is a double covering of $SO(n)$ and $O(n)$, it is nontrivial because $1, -1$ is connected by $(\cos te_1 + \sin te_2)(\cos te_1 - \sin te_2)$.

In particular, $\mathrm{Spin}(n)$ is a universal covering of $SO(n)$ and thus simply-connected for $n \geq 3$. ⌟

Proof: Let $\alpha = e_i\beta + \gamma$, then $\beta, \gamma \in Cl^0$ and so $\alpha = ce_1 \dots e_n + d$, and c can happen only when n is odd. □

Prop. (12.12.1.5) [Center of Spin(n)]. $$Z(\mathrm{Spin}(n)) = \begin{cases} S^1 & n = 2 \\ \mathbb{Z}/2\mathbb{Z} & n = 2k+1, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & n = 4k, \\ \mathbb{Z}/4\mathbb{Z} & n = 4k+2, \end{cases}.$$ ⌟

Proof: □

Prop. (12.12.1.6) [Low Dimensional Accidental Isomorphisms].

- $\mathrm{Spin}(2) \cong SO(2) \cong U(1)$.
- $\mathrm{Spin}(3) \cong SU(2) \cong Sp(1)$
- $\mathrm{Spin}(4) \cong SU(2) \times SU(2)$ because they are both universal coverings of $SO(4)$, by(12.12.2.1) and(12.12.1.4).
- $\mathrm{Spin}(5) \cong \mathrm{Sp}(2)$.
- $\mathrm{Spin}(6) \cong SU(4)$.

⌟

Proof: 2: because $\mathrm{Spin}(3), SU(2)$ are both universal covering of $SO(3)$, by(12.12.2.1) and(12.12.1.4), and $Sp(1)$ acts transitively on the set of unit vectors in $\mathbb{H}$ with trivial kernel. □

2 Fundamental Groups

Prop. (12.12.2.1).

- $SU(n-1) \to SU(n) \to S^{2n-1}$ shows $SU(n)$ are connected and simply connected. Also $\pi_2(SU(n)) \cong \pi_2(SU(2)) \cong \pi_2(S^3) = 0$.
- $SO(n-1) \to SO(n) \to S^{n-1}$ shows $SO(n)$ are connected and $\pi_1(SO(n)) \cong \pi_1(SO(3)) = \mathbb{Z}/2\mathbb{Z}$ for $n \geq 3$ by(12.12.0.8)and(12.12.0.7). And $\pi_1(SO(2)) = \mathbb{Z}$.
- $U(n-1) \to U(n) \to S^{2n-1}$ shows $U(n)$ are connected and $\pi_1(U(n)) \cong \mathbb{Z}$.

- $SO(n,\mathbb{R})$ is a deformation retraction of $SL(n,\mathbb{R})$, and $SU(n)$ is a deformation retraction of $SL(n,\mathbb{C})$.
- $\pi_1(PSO(n)) = \begin{cases} \mathbb{Z} & n=2 \\ \mathbb{Z}/2\mathbb{Z} & n=2k+1, \\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z} & n=4k, \\ \mathbb{Z}/4\mathbb{Z} & n=4k+2, \end{cases}$. Because for $n\geq 3$, its universal covering is $\mathrm{Spin}(n)$, so $\pi_1(PS(n)) = Z(\mathrm{Spin}(n))$(12.12.1.5).
- $\pi_1(PU(n)) = \mathbb{Z}/n\mathbb{Z}$.
- $Sp(n-1)\to Sp(n)\to S^{4n-1}$ shows $Sp(n)$ are connected and simply connected.
- $\pi_1(Sp(2n,\mathbb{R})) = \pi_1(U(n)) = \mathbb{Z}$ and the determinant induces an isomorphism onto $\pi_1(S^1)$. In fact, this is used to define the Maslov index.

⌟

3 Generals

Prop. (12.12.3.1) [Finite Subgroups of SO(3, ℝ)]. Every finite subgroup of $\mathrm{SO}(3,\mathbb{R})$ is conjugate to one of the following:

- the cyclic group C_n generated by rotation.
- the dihedral group D_{2n} generated by adjoining a reflection to the rotation.
- the group A_4 of rotation of the tetrahedron.
- the group S_4 of rotations of the octahedron.
- the group A_5 of rotations of the icosahedron.

⌟

Proof: Cf.[Dornhoff, Group Representation Theory, 1971 Part A, Chap26]. □

Prop. (12.12.3.2) [Image of Exponential Maps].

- The exponential map for $\mathrm{GL}_n(\mathbb{C})$ is surjective.
- The image of the exponential map for $\mathrm{GL}_n(\mathbb{R})$ is $\mathrm{GL}_n(\mathbb{R})^2$.
- The image of exponential map for B_+ which is the subgroup of $\mathrm{GL}(n,\mathbb{R})$ consisting of upper-triangular matrices with positive entries, is surjective.
- The exponential defines a diffeomorphism from the space of Hermitian(symmetric) matrices to positive definite Hermitian(resp. symmetric) matrices in $\mathrm{GL}(n,\mathbb{C})$(resp. $\mathrm{GL}(n,\mathbb{R})$).
- The exponential for a compact Lie group is surjective, by(12.11.7.6) and(12.11.7.2).

⌟

Proof: 1: Use Jordan forms. Notice the logarithm of $(cI+N), c\neq 0$ is definable for N nilpotent, and it is a polynomial function of the matrix itself.

2: It is clear the image is contained in $GL(n,\mathbb{R})^2$, conversely, we see from the complex case that any $B\in GL(n,\mathbb{R})$ is of the form $\exp(P(B))$ for some polynomial $P\in\mathbb{C}[X]$, then $T=B^2=\exp(P(B)+\overline{P}(B))\in\exp(GL(n,\mathbb{R}))$.

3: Use Jordan forms. Notice the logarithm of $(cI+N), c\neq 0$ is definable for N nilpotent and $c>0$, and it is a polynomial function of the matrix itself, so it is also upper-triangular.

4: By(3.5.10.18) it is clearly surjective. For injectivity, consider $\exp(X) = \exp(Y)$, then at least X, Y are both unitarily conjugate to the same diagonal matrix $\mathrm{diag}(d_1, \ldots, d_n)$, and we may assume $Y = \mathrm{diag}(d_1, \ldots, d_n)$, then

$$X = \tau^{-1} Y \tau, \quad \mathrm{diag}(D_1, \ldots, D_n) = \tau^{-1}\,\mathrm{diag}(D_1, \ldots, D_n)\tau$$

where $D_i = e^{d_i}$. Consequently, $\mathrm{diag}(D_1^k, \ldots, D_n^k) = \tau^{-1}\,\mathrm{diag}(D_1^k, \ldots, D_n^k)\tau$, and we can choose c_i that $\sum c_i D_j^i = d_j$ for any j, because the Vandermonde matrix is nonsingular. Hence $\mathrm{diag}(d_1, \ldots, d_n) = \tau^{-1}\,\mathrm{diag}(d_1, \ldots, d_n)\tau$, so $X = Y$. □

4 Metaplectic Groups

Def. (12.12.4.1) [Metaplectic Groups]. The group $\mathrm{SL}(2, \mathbb{R})$ has a double cover $\mathrm{Mp}(2, \mathbb{R})$ called the **metaplectic group**

$$\mathrm{Mp}(2, \mathbb{R}) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \pm\sqrt{c\tau + d}\} \in \mathrm{SL}(2, \mathbb{R}) \rtimes \mathcal{O}(\mathscr{H}),$$

where $\mathrm{SL}(2, \mathbb{R})$ acts on $\mathcal{O}(\mathscr{H})$ as usual.

And $\mathrm{Mp}(2, \mathbb{Z}) \subset \mathrm{Mp}(2, \mathbb{R})$ is the subgroup consisting of elements of the form

$$\mathrm{Mp}(2, \mathbb{Z}) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \pm\sqrt{c\tau + d}\} \in \mathrm{SL}(2, \mathbb{Z}) \rtimes \mathcal{O}(\mathscr{H}).$$

And for any subgroup $H \subset SL(2, \mathbb{R})$, denote $\widetilde{H}$ the inverse image of H in $\mathrm{Mp}(2, \mathbb{R})$. Also denote $\mathrm{Mp}(2, \mathbb{Z}) = \widetilde{\mathrm{SL}(2, \mathbb{Z})}$, called the **metaplectic modular group**. ⌟

12.13 Locally Symmetric Spaces

1 Symmetric Spaces

Main references are[Hel78], [Mil17b] and [Lan20].

Def. (12.13.1.1) [Symmetric Spaces]. A Riemannian manifold is called **locally symmetric** at p if $\nabla R(p) = 0$. Locally symmetric is equivalent to the fact that every local reversing map is an isometry.

A **symmetric space** is a Riemannian manifold that $\nabla R = 0$ everywhere.

A symmetric space is complete because two folding is an extension of geodesics. In particular, a symmetric space is homogenous, and to check symmetrically, it suffices to show it is homogenous and locally symmetric at a point. ⌟

Proof: □

Prop. (12.13.1.2). A Lie group with a bi-invariant metric is a symmetric space. ⌟

Proof:

□

Prop. (12.13.1.3). The conjugate points in a symmetric space is easy to calculate, they are $\exp(\frac{\pi k}{\sqrt{e_i}}V)$, counting multiplicity, where e_i is the eigenvalue of the self-adjoint operator $K_V(W) = R(V, W)V$ at p. ⌟

Prop. (12.13.1.4) [Lie Group of Isometries]. Let M be a symmetric space, then the group of isometries $\mathrm{Isom}(M^\infty, g)$ of M has a natural structure of a Lie group. ⌟

Proof: Cf.[Helgason, homogenous Spaces, 4.3.2]. □

Prop. (12.13.1.5) [Symmetric Space is a Homogenous Space]. Let (M, g) be a symmetric space, and $p \in M$, then the subgroup $K_p \subset \mathrm{Aut}(M, g)^0$ fixing p is compact, and the natural map

$$\mathrm{Isom}(M, g)^0 / K_p \to M^\infty$$

is an isomorphism of smooth manifolds, where $\mathrm{Isom}(M, g)^0 / K_p$ is given the homogenous space structure(12.13.1.4). In particular, $\mathrm{Isom}(M, g)^0$ acts transitively on M. ⌟

Proof: Cf.[Mil17c]P12. □

2 Decompositions of Symmetric Spaces

3 Non-Compact Type

4 Compact Type

5 Hermitian Symmetric Spaces

Def. (12.13.5.1) [Hermitian Symmetric Spaces]. A **Hermitian symmetric space** is a Hermitian manifold that is a symmetric space(12.13.1.1) and that the local symmetries are all holomorphic. ⌟

Prop. (12.13.5.2) [Lie Group of Isometries]. For a Hermitian symmetric space, the group of holomorphic symmetries $\mathrm{Aut}(M, g)$ is closed in the group of isometries $\mathrm{Aut}(M^\infty, g)$, which is a Lie group by(12.13.1.4), so it is also a Lie group. ⌟

Prop. (12.13.5.3) [Basic Hermitian Symmetric Spaces]. There are three different families of Hermitian symmetric spaces(but not complete):

- (Non-compact Type): These spaces are non-compact and simply connected, with negative curvatures, and $\mathrm{Isom}(M,g)^0$ is adjoint and non-compact.
- (Compact Type): These spaces are compact and simply-connected, with positive curvatures, and $\mathrm{Isom}(M,g)^0$ is adjoint and compact.
- (Euclidean Type): These spaces have constant curvature 0.

⌟

Proof: Cf.Helgason 1978, Chap8. □

Prop. (12.13.5.4) [Decomposition]. Any Hermitian symmetric space M decomposes into a product $M^0 \times M^+ \times M^-$ of Hermitian symmetric spaces with M^0 Euclidean, M^- of non-compact type and M^+ of compact type. ⌟

Proof: □

Prop. (12.13.5.5). Any Hermitian symmetric space of Euclidean type is a quotient of $\mathbb{C}^g$ by a discrete subgroup of translations. ⌟

Proof: □

Example (12.13.5.6). The projective space $\mathbb{P}^n(\mathbb{C})$ with the Fubini-Study metric is a Hermitian symmetric space. For any p, the (descent of) the rotation through π about the axis through p and its polar opposite is the geodesic isomorphism at p. ⌟

Proof: See(12.9.1.6). □

6 Hermitian Symmetric Domains

Def. (12.13.6.1) [Hermitian Symmetric Domain]. A Hermitian symmetric space(12.13.5.1) of non-compact type(12.13.5.3) is called a **Hermitian symmetric domain**. in particular, a Hermitian symmetric domain is simly-connected. A **bounded symmetric domain** is a bounded open connected symmetric subset of $\mathbb{C}^n$. ⌟

Prop. (12.13.6.2) [Hermitian Symmetric Domains are Bounded]. Every Hermitian symmetric domain can be embedded into $\mathbb{C}^n$ for some n, and the image is bounded. ⌟

Proof:

□

Prop. (12.13.6.3) [Bergman Metric]. Every bounded symmetric domain has a canonical Hermitian metric called the **Bergman metric**, it is invariant under holomorphic automorphisms, and it has negative curvatures. ⌟

Proof: Cf.[Mil17]P11 and [Hel78]8.3.3. □

Cor. (12.13.6.4). Every Hermitian symmetric domain D has a unique Hermitian metric that maps to the Bergman metric under any isomorphism of D onto a bounded symmetric domain. ⌟

Cor. (12.13.6.5). A complex manifold is a a symmetric Hermitian domain iff it is biholomorphic to a bounded symmetric domain. ⌟

Proof: □

Def. (12.13.6.6) [Siegal Upper Half Plane $\mathscr{H}_g$]. For $g \in \mathbb{Z}_+$, the **Siegal upper half space** $\mathscr{H}_g$ is defined to be

$$\mathscr{H}_g = \{Z \in \mathrm{Mat}(n, \mathbb{C}) | Z^t = Z, \mathrm{Im}(Z) \in \mathrm{Pos}(g, \mathbb{C})\}.$$

It is identified with an open subset of $\mathbb{C}^{g(g+1)/2}$. The symplectic group $\mathrm{Sp}(2g; \mathbb{R})$(12.12.0.2) acts transitively on $\mathscr{H}_g$ via

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} Z = (AZ+B)(CZ+D)^{-1}$$

The matrix $\begin{bmatrix} 0 & -I \\ I & 0 \end{bmatrix}$ acts as an involution on $\mathscr{H}_g$, and has iI_g has its fixed point, so $\mathscr{H}_g$ is homogenous and symmetric.

The injection into $\mathbb{C}^g$ is not holomorphic, so we cannot see from this that $\mathscr{H}_g$ is holomorphic, but we can see from**?** ⌟

Proof: **?** □

Cor. (12.13.6.7) [Upper Half Plane]. By(12.12.0.11), the group $GL(2; \mathbb{R})$ acts continuously on $\mathbb{C}$ by $\gamma(z) = \frac{az+b}{cz+d}$ where $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

The groups $GL(2, \mathbb{R})$ preserves the upper plane $\mathscr{H}$, by(11.4.1.9). The action of $\mathrm{SL}(2; \mathbb{R})$ on $\mathscr{H}$ is transitive and the stabilizer of i is $SO(2, \mathbb{R})$, thus we have $\mathcal{H} \cong SL(2; \mathbb{R})/SO(2; \mathbb{R})$, and $\mathrm{PSL}(2; \mathbb{R})$ is the group of holomorphic automorphisms of $\mathcal{H}$ by(11.4.7.8).

Also, the Riemannian metric $\frac{\mathrm{d}x\mathrm{d}y}{y^2}$ on $\mathscr{H}$ is fixed by the action of $GL(2; \mathbb{R})$. ⌟

Def. (12.13.6.8) [Siegal Unit Disk $\mathbb{D}_g$]. Let $\mathbb{D}_g$ be the set of symmetric complex matrixes that $I - Z^*Z$ is positive definite, then it is identified with an open subset of $\mathbb{C}^{g(g+1)/2}$, this is a holomorphic embedding.

There is an isomorphism from $\mathcal{H}_g$(12.13.6.6) to $\mathcal{D}_g$:

$$Z \mapsto (Z - iI_g)(Z + iI_g)^{-1}.$$

This is an isomorphic, so D_g is symmetric, and $\mathcal{H}_g$ has an invariant metric, so they are both Hermitian symmetric domains**?**. ⌟

Proof: **?**. □

Prop. (12.13.6.9). Let (M, g) be a Hermitian symmetric domain, then the inclusions

$$\mathrm{Aut}(M^\infty, g) \supset \mathrm{Aut}(M, g) \subset \mathrm{Aut}^{\mathrm{Hol}}(M)$$

induce equalities

$$\mathrm{Aut}(M^\infty, g)^0 = \mathrm{Aut}(M, g)^0 = \mathrm{Hol}(M)^0$$

Then $\mathrm{Hol}(M)^0$ acts transitively on M, the stabilizer K_p of p in $\mathrm{Aut}^{\mathrm{Hol}}(M)^0$ is compact, and

$$\mathrm{Hol}(D)^0/K_p \cong M^\infty.$$

⌟

Proof: Cf.[Mil17b]P12. □

Prop. (12.13.6.10). The Lie group $\mathrm{Aut}^{\mathrm{Hol}}(M)$ in(12.13.6.9) is a real semisimple Lie group with only f.m. connected components and trivial center.?

If G is a connected simple real algebraic group with trivial center s.t. $D = G(\mathbb{R})^0/K$ for some maximal compact subgroup $K \subset G(\mathbb{R})^0$, then $\mathrm{Aut}(D) \cap G(\mathbb{R}) = G(\mathbb{R})^0$, and $G(\mathbb{R})$ has one or two connected components. ⌟

Proof: ? □

Prop. (12.13.6.11) [Rotation at a Point]. Let D be a Hermitian symmetric domain and $p \in D$, then there is a unique homomorphism $u_p : U_1 \to \mathrm{Hol}(D)$ that $u_p(z)$ fixes p and acts on $T_p(D)$ as multiplication by z. ⌟

Prop. (12.13.6.12) [Classification of Hermitian Symmetric Domains]. The isomorphism classes of irreducible Hermitian symmetric domains are classified by the special nodes on connected Dynkin diagrams. ⌟

Proof: Cf.[Mil17]P20. □

7 Locally Symmetric Varieties

Prop. (12.13.7.1) [$D(\Gamma)$]. Let D be a Hermitian symmetric domain, and let Γ be a discrete subgroup of $\mathrm{Aut}^{\mathrm{Hol}}(D)^0$. If Γ is torsion-free, then Γ acts freely on D, and there is a unique complex manifold structure on $\Gamma\backslash D$ that the quotient map $\pi : D \to \Gamma\backslash D$ is a holomorphic covering space.

In this case, denote $D(\Gamma) = \Gamma\backslash D$, and D is a universal covering of $D(\Gamma)$, by(12.13.5.3) and(12.13.6.1). ⌟

Proof: Cf.[Mil17b]P32. □

Prop. (12.13.7.2). Let D be a Hermitian symmetric domain and $\Gamma \subset \mathrm{Hol}(D)^0$ is a discrete subgroup, then by(12.13.6.9), Γ has finite covolume in $\mathrm{Hol}(D)^0$ iff $\Gamma\backslash D$ has finite covolume, ⌟

Proof: □

Prop. (12.13.7.3). $D(\Gamma)$ has only f.m. automorphisms, as a complex manifold. ⌟

Proof: Cf.[Mil17b]P41. □

Thm. (12.13.7.4) [Satake-Baily-Borel Compactifications]. Let D be a locally symmetric Hermitian space and $\Gamma \subset \mathrm{Hol}(D)^0$ an arithmetic subgroup(15.5.2.1), then $D(\Gamma)$ can be realized as an open subset of a projective variety $\overline{D(\Gamma)}$ over $\mathbb{C}$, and it is a normal algebraic variety. If moreover Γ is torsion-free, then it is smooth, by(12.13.7.1).

Such a projective variety $D(\Gamma)$ is called a **locally symmetric variety**. ⌟

Proof: Cf. [BAILY-BOREL, Compactification of arithmetic quotients of bounded symmetric domains. 84:442–528. 1966] and [CASSELMAN, Geometric rationality of Satake compactifications, pp. 81–103.1997].

Cf.[Mil17b]P38 for a history. □

Thm. (12.13.7.5) [Borel]. Let $D(\Gamma)$ be a quotient variety(12.13.7.4) of a Hermitian symmetric domain by a torsion-free arithmetic subgroup Γ in $\mathrm{Aut}^{\mathrm{Hol}}(D)^0$, then for any other smooth quasi-projective variety V over $\mathbb{C}$, any holomorphism map $V^{\mathrm{an}} \to D(\Gamma)^{\mathrm{an}}$ comes from a morphism. ⌟

Proof: □

Cor. (12.13.7.6) [Algebraic Structure is Unique]. The algebraic variety structure on $D(\Gamma)$ is unique. Any variety of the form is called a **locally symmetric variety**. ⌟

Proof: If there is another structure, then by GAGA it is a smooth variety, then the holomorphic map extends to a bijective morphism, which must be an isomorphism, by [Milne, Algebraic Geometry, P188]?. □

Cor. (12.13.7.7) [Borel]. The Satake-Baily-Borel compactification(12.13.7.4) $\overline{D(\Gamma)}$ is minimal in the sense that it factors through any compactification $D(\Gamma) \subset V$ s.t. $V \backslash D(\Gamma)$ is a divisor with only normal crossings as singularities. ⌟

Proof: Cf.[Borel 1972]? □

12.14 Compactifications of Locally Symmetric Spaces

Main references are [Smooth compactifications of locally symmetric varieties, Rapoport-Scholze](contains a lot of references), [Toroidal Compactification of Siegel Spaces (1980).pdf], [Goresky, M. 2005. Compactifications and cohomology of modular varieties, pp. 551−582. In Harmonic analysis, the trace formula, and Shimura varieties] and [SATAKE, 2001. Compactifications, old and new].

Def. (12.14.0.1) [Toroidal Compactifications]. Cf. [BOREL, A. AND JI, L. 2006. Compactifications of symmetric and locally symmetric spaces]. ⌟

For Siegel modular varieties, there is a short note in [Conrad, Mordell conjecture seminar].

12.15 Calabi-Yau Manifolds

12.16 Knots and Links

References are [Ada04], [Knot Theory, Lickorish].

Def. (12.16.0.1) [Knots and Links]. For $M \in \mathcal{M}\mathrm{ani}^3$, a **knot** K in M is an embedding $K : \mathbb{S}^1 \hookrightarrow M$, and a **link** is a collection of disjoint unions in M. If M is piecewise-smooth or piecewise-linear, K is also assumed to be smooth or piecewise-linear.

If M is not specified, then it is assumed to be $\mathbb{R}^3$. If we talk about two knots, then it is assumed that they are disjoint. ⌟

Def. (12.16.0.2) [Unknots]. An **unknot**(or a **trivial knot**) is a knot $K \subset M$ that is (piecewise-smoothly/linearly) null-homotopic. Two knots/links are called **equivalent knots**/links if they are isotopic.

If we consider the knots in $\mathbb{R}^3$, we tacitly assume that the links are piecewise-linear. ⌟

Prop. (12.16.0.3). There are no knot diagrams with exact two crossings. ⌟

Proof: □

Def. (12.16.0.4) [Knot Diagrams]. For a piecewise-linear knot $K \subset \mathbb{R}^3$, a **knot diagram** is given by a linear projection $\mathrm{pr} : \mathbb{R}^3 \to \mathbb{R}^2$ s.t.

- $\#p^{-1}(x) \leq 2$ for any $x \in \mathbb{R}^2$.
- $\#p^{-1}(x) = 2$ for only f.m. $x \in \mathbb{R}^2$.
- For any vertex x of K, $\mathrm{pr}^{-1}(\mathrm{pr}(x)) = \{x\}$.

together with a labeling of overcrossing and undercrossing at each pair $(x, y) \in K$ s.t. $p(x) = p(y)$, according to their height w.r.t. the projection. ⌟

Def. (12.16.0.5) [Crossing Numbers]. The **crossing number** $\mathrm{Cr}(L)$ of a link L is the minimal number of crossings for any link diagram of L. ⌟

Def. (12.16.0.6) [Unknot Numbers]. The **unknot number** of a knot K is the minimal number of crossings needed to change on some knot diagram of it to make it an unknot. Why does such an unknot always exists**?**. ⌟

Def. (12.16.0.7) [Sign of Crossing and Writhe]. There are three kinds of crossing relation between two oriented strands: L_+, L_-, L_0. Cf.[Lickorish]P11Figures. ⌟

Def. (12.16.0.8) [Reidemeister Moves]. There are three **Reidemeister moves** on a knot diagram:

1. A local untwist/twist(i.e. $\looparrowright$ changed to $\to$).
2. A local strand passing over or under a strand.
3. A local strand passing over or under a crossing.

⌟

Thm. (12.16.0.9). Given two knots K, K' and two projections of them, then they are equivalent iff they are connected by a finite series of Reidemeister moves. ⌟

Proof: **?** □

Def. (12.16.0.10) [Connected Sums of Knots]. Given two knots $K, K \in \mathbb{S}^3$, we can consider their connected sum. And a **prime knot** is a non-trivial knot that is not a connected sum of two non-trivial knots. ⌟

Def. (12.16.0.11) [Knot Invariants]. A **knot invariant** is a function on the set of knots that has the same value on equivalent knots. By(12.16.0.9), a knot invariant is equivalent to a function on knot diagrams that is invariant under Reidemerster moves. ⌟

Def. (12.16.0.12) [Knot Groups]. For any knot $K \subset \mathbb{R}^3$, the **knot group** $\Pi(K)$ is defined to be $\Pi(K) = \pi_1(\mathbb{R}^3 \setminus K)$. This is a knot invariant. ⌟

Def. (12.16.0.13) [Tricolorable Knots]. A **tricoloring of a knot diagram** is a tricoloring of each stand of the diagram s.t.

- Every color is used.
- At each crossing, the three strands are either of the same color or pairwise different colors.

having a tricoloring is a property that is invariant under Reidemeister moves, so it is a knot invariant. A **tricolorable knot** is a knot that has a tricolorable knot diagram. ⌟

Def. (12.16.0.14) [Alternating Knots]. An **alternating knot** is a knot that has a diagram s.t. if one travels thought the knot, the 'up' and 'down' nature of the crossing alternates. ⌟

Knots and Braids

Def. (12.16.0.15) [Braids]. For $n \in \mathbb{Z}_+$, let A be the set of n points in $\mathbb{R}^3$ with coordinates $y = 0, z = 1, x = 1, 2, \ldots, n$, and B the set of n points in $\mathbb{R}^3$ with coordinates $y = 0 = z, x = 1, 2, \ldots, n$. Then an n-strand braid is a set of n piecewise-smooth non-intersecting paths with descending z-coordinates connecting the points in A bijectively to points in B. Two braids are called **equivalent** if there is an isotopy of $\mathbb{R}^3$ taking one into another with the endpoints fixed.

The n-strand **braid group** is the set of equivalent classes of n-strand braids with the group structure such that: For any two braids X, Y, $X \circ Y$ is the braid with the bottom of X connected to the top of Y. It is easy to check that the braids form a group under this multiplication. ⌟

Def. (12.16.0.16) [Closure of Braids]. Given any braid B, the **closure of braid** of B is the oriented link $L(B)$ generated by connecting each $(k, 0, 0)$ with $(k, 0, 1)$ by a smooth path contained in the plane $x = k$ and non-intersecting with B, where the orientation of $L(B)$ is given by going through the braid from the top to the bottom. ⌟

Prop. (12.16.0.17). For $n \in \mathbb{Z}_+$, the following three groups are equivalent:

- The n-strand braid group.
- The fundamental group of the unordered n-configuration space for $\mathbb{R}^2$.
- The free group generated by words $\sigma_1, \ldots, \sigma_{n-1}$ under the relations:

$$\sigma_i \sigma_j = \sigma_j \sigma_i, \forall 1 \leq i \leq j - 2 \leq n - 1,$$

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}, \forall 1 \leq i \leq n - 2.$$

⌟

Proof: 1 and 3: Any braid can be projected along the y-direction, and we can perturb it s.t. this is a link diagram, and for each z_0, there is at most one crossing with $z = z_0$. In this way, we can decompose any braid into a composite of braids s.t. each braid is a swap of two consecutive vertices i and $i + 1$. Then there is a map from the free group $\langle \sigma_1, \ldots, \sigma_{n-1} \rangle$ to the n-strand braid group mapping σ_i to the swap of vertices i and $i + 1$ with i at front, and σ^{-1} mapped to the swap of vertices

i and $i+1$ with $i+1$ at front. Then it can be checked that it is truly a map, and it factors through the relations

$$\sigma_i\sigma_j = \sigma_j\sigma_i, \forall 1 \le i \le j-2 \le n-1,$$
$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \forall 1 \le i \le n-2.$$

So it remains to prove that any two equivalent braids are connected by a sequence of moves according to these relations. This proof is similar to that of Riedemeister moves(12.16.0.9)**?**.

1 and 2: Connecting the top and bottom of each braid gives a loop in the n-configuration space of $\mathbb{R}^2$. □

Def. (12.16.0.18) [Markov Moves]. There are three kinds of **Markov moves** on a braid:

1. Conjugation by σ_i for some i.
2. Make an n-strand braid to an $n+1$-strand braid by adding a straight strand at the end and multiply by σ_n or σ_n^{-1} on the right.

⌟

Prop. (12.16.0.19) [Markov]. For two braids B, B'(may have different number of strands), their closure represent equivalent links iff they are connected by a finite number of Markov moves(12.16.0.18). ⌟

Proof: Cf.[A study of Braids]P148.**?** □

Thm. (12.16.0.20) [Alexander]. Any oriented link L is equivalent to the closure of a braid. ⌟

Proof: We only prove for piecewise-linear links. Take a link diagram D of L and take a point $P \in \mathbb{R}\backslash D$ that is not on the lines generated by any segment of D. Then we can observe each segment is clockwise or counter-clockwise w.r.t. P. We can make them all clockwise: For counter-clockwise segments we draw a general triangle that include P, and then use Reidemeister moves to make a new diagram for L. Then in this way, projection clockwise from P gives us a braid whose closure is equivalent to L. □

Cor. (12.16.0.21) [Braid Indices]. The **braid index** of an oriented link L is the minimal $n \in \mathbb{Z}_+$ s.t. L is equivalent to the closure of an n-strand braid. ⌟

Braid Groups

Cor. (12.16.0.22) [Pure braids]. Due to the covering map $\mathbb{C}^n\backslash \cup \{z_i = z_j\} \to \mathbb{C}^n\backslash \cup \{z_i = z_j\}/S^n$ with fiber S^n, there is a map $B_n \to S_n$ which is easily seen to be surjective and with kernel $P_n = \pi_1(\mathbb{C}^n\backslash \cup \{z_i = z_j\})$, called the group of **pure braids**. ⌟

Prop. (12.16.0.23). There is a group homomorphism $B_3 \to \mathrm{PSL}(2;\mathbb{Z})$ that maps $a = \sigma_1\sigma_2\sigma_1$ to S and $b = \sigma_1\sigma_2$ to T. The kernel of this map is the group generated by $c = a^2 = b^3$. ⌟

Coding of Knots

Def. (12.16.0.24) [Chessboard Coloring of Knots]. Given a knot diagram K, we can chessboard 2-color the components of the complements of K, s.t. two adjacent components have different colors. (This is because each vertex has order 4). ⌟

Def. (12.16.0.25) [Dowker-Thistlethwaite Notations]. Given a knot diagram, the **Dowker-Thistlethwaite notation** is given as follows: **?** ⌟

Def. (12.16.0.26) [Conway Notations]. ⌟

Stick Numbers

Def. (12.16.0.27) [Stick Numbers]. For a knot $K \in \mathbb{R}^3$, the **stick number** $s(K)$ is the minimal number $n \in \mathbb{Z}_+$ s.t. K is equivalent to a piecewise-linear knot with n vertices. ⌟

Prop. (12.16.0.28). For any non-trivial knot K, $s(K) \geq 6$. ⌟

Proof: Use the fact that any knot diagram with ≤ 2 crossings is an unknot(12.16.6.1). □

Prop. (12.16.0.29). For any non-trivial knot K,

$$\frac{5 + \sqrt{8\,\mathrm{Cr}(K) + 9}}{2} \leq s(K) \leq \frac{3}{2}(\mathrm{Cr}(K) + 1).$$

⌟

Proof: Cf.https://en.wikipedia.org/wiki/Stick_number. □

Prop. (12.16.0.30) [Jin]. If K_1, K_2 are knots, then

$$s(K_1 \# K_2) \leq s(K_1) + s(K_2) - 3.$$

Is it possible to make it -4(which would be optimal in the case K_1, K_2 being trefoil)**?**. ⌟

Proof: Cf.[Jin, Polygon Indices and Superbridge Indices of Torus Knots and links]. □

Bridge Numbers

Def. (12.16.0.31)[Bridge Numbers]. The **bridge number** $b(K)$ of a knot K is the minimal number of strands that overpass at least one other strands in some knot diagram of it. Clearly, $b(K) \leq \mathrm{Cr}(K)$. ⌟

Prop. (12.16.0.32). For any non-trivial knots, $b(K) \geq 2$. ⌟

Proof: **?** □

Prop. (12.16.0.33) [Schburt]. If K_1, K_2 are knots, then

$$b(K_1 \# K_2) \leq s(K_1) + s(K_2) - 1.$$

⌟

Proof: **?**[Schburt1954]. □

Def. (12.16.0.34)[Two-Bridged Knots]. A **two-bridged knot** is a knot $K \in \mathbb{R}^3$ with $b(K) = 2$. In particular, by(12.16.0.33), two-bridged knots are all prime knots. ⌟

Prop. (12.16.0.35). Two-bridged knots are just rational knots. ⌟

Proof: **?** □

Slice Knots

Def. (12.16.0.36) [Slice Knots]. A **slice knot** is a knot $K \in \mathbb{S}^3 = \partial\mathbb{D}^4$ that is the boundary of an embedding $M : \mathbb{D}^2 \hookrightarrow \mathbb{D}^4$. ⌟

Def. (12.16.0.37) [Ribbon Knots]. A **ribbon knot** is a slice knot $K \in \mathbb{S}^3$ which is a boundary of an embedding $M : D^2 \hookrightarrow \mathbb{D}^4$ s.t. the function $||x||$ on $\mathbb{D}^4$ restricted to M has no interior local maximum on M. ⌟

1 Seifert Surfaces

Def. (12.16.1.1) [Siefert Surfaces]. A **Siefert surface** of an oriented link $L \subset \mathbb{S}^3$ is a connected compact oriented surface with boundary in $\mathbb{S}^3$ that has L as its oriented boundary. ⌟

Thm. (12.16.1.2). Any oriented link $L \subset \mathbb{S}^3$ has a Siefert surface. ⌟

Proof: Cf.[Lickorish]P16. □

Cor. (12.16.1.3) [Genus of Knots]. For any knot K, the **genus of knot** $g(K)$ of K is defined to be the minimal genus of a Siefert surface of K. ⌟

Prop. (12.16.1.4). For any two disjoint knots K_1, K_2, $g(K_1 + K_2) = g(K_1) + g(K_2)$. ⌟

Proof: Cf.[Lickorish]P17. □

Thm. (12.16.1.5) [Schönflies Theorem]. For any piecewise-linear embedding $e : \mathbb{S}^2 \to \mathbb{S}^3$, $\mathbb{S}^3 \setminus e(\mathbb{S}^2)$ has two connected components, and the closure of each of them is a piecewise-linear $\mathbb{D}^2$. ⌟

Proof: Cf.[Lickorish. The irreducibility of the three-sphere]. □

2 Polynomial Invariants

HOMFLY Polynomails

Thm. (12.16.2.1) [HOMFLY]. There exists a unique knot invariant P on the equivalent classes of tame oriented links to the set of homogenous Laurent polynomials of degree 0 in x, y, z, s.t.

- $P_{\bigcirc} = 1$.
- $xP_{L_+}(x, y, z) + yP_{L_-}(x, y, z) + zP_{L_0}(x, y, z) = 0$, which means a local surgery of the crossing according to(12.16.0.7).

⌟

Prop. (12.16.2.2). Given two oriented links L, L',

$$P_{L\#L'}(x, y, z) = P_L(x, y, z) \cdot P_{L'}(x, y, z).$$

⌟

Example (12.16.2.3). $P_{\coprod^n \bigcirc}(x, y, z) = (-\frac{x+y}{z})^{n-1}$. ⌟

Kauffman Polynomials

Alexander-Conway Polynomials

Def. (12.16.2.4). ⌟

Prop. (12.16.2.5). The Alexander-Conway polynomial is just

$$\Delta_L(t) = P_L(1, -1, t^{1/2} - t^{-1/2}).$$

⌟

Jones Polynomials

Cf.[STATE MODELS AND THE JONES POLYNOMIAL, Kauffman].

Def. (12.16.2.6) [Kauffman Brackets]. The **Kauffman bracket** is a function from unoriented link diagrams in $\mathbb{S}^2$ to $\mathbb{Z}[T][\frac{1}{T}]$ defined inductively by the following rules:

- $\langle \bigcirc \rangle = 1$.
- $\langle D \amalg \bigcirc \rangle = -(T^{-2} + T^2)\langle D \rangle$.
- $\Big\langle L_+ \Big\rangle = T.\Big\langle \big)\big(\Big\rangle + T^{-1}.\Big\langle \asymp \Big\rangle$, which means a local surgery of the crossing according to(12.16.0.7).

The Kauffman bracket of a diagram is invariant under type2,3 Reidemeister moves, but changed by type1 Reidemeister moves. ⌟

Def. (12.16.2.7) [Writhes]. The **Writhe of a link diagram** $w(D)$ of an oriented link diagram D is the sum of sign of crossings of D. The writhe of a diagram is invariant under type2,3 Reidemeister moves, but changed by type1 Reidemeister moves. ⌟

Thm. (12.16.2.8) [Jones]. Let D be a diagram of an oriented link L, then the expression

$$X_L(T) = (-T)^{3w(D)}\langle D \rangle \text{(12.16.0.7)(12.16.2.6)}$$

is a link invariant(12.16.0.11) of the oriented link L. The **Jone polynomial** of D is defined to be

$$V_L(t) = X_L(t^{-1/4}) \in \mathbb{Z}[t^{1/2}, t^{-1/2}].$$

⌟

Proof: Cf.[Lickorish]P26.

It suffices to show that this $X_L(T)$ is invariant under Reidemeister moves, and this is easy to verify(Cf. [Ada04]). □

Prop. (12.16.2.9). The Jones polynomial is just

$$V_L(t) = P_L(t, -t^{-1}, t^{1/2} - t^{-1/2}).$$

⌟

Prop. (12.16.2.10) [Properties of Jones Polynomials].

- If K is a knot, then $V_K(\omega) = 1$.
- $V_L(1) = (-2)^{\pi_0(L)-1}$.

- if K is a knot, then $\frac{\partial}{\partial t}V_K(1) = 0$.
- If K is a knot, then the Arf invariant of K is just $Arf = (1 - V_K(\mathrm{i}))/2$.
- $\Delta_K(-1) \equiv 1, 5 (\mathrm{mod}\ 8)$, according to $Arf = 0$ or 1.

⌟

Proof: Cf.[Jones]. □

Prop. (12.16.2.11). If K is a knot and $|\Delta_K(\mathrm{i})| > 3$, then K cannot be represented as a closed 3-braid.
If K is a knot and $\Delta_K(e^{2\pi\,\mathrm{i}/5}) > 6.5$, then K cannot be represented as a closed 4-braid. ⌟

Proof: Cf.[Jones]. □

Conj. (12.16.2.12). If K is a non-trivial knot, then $X_K(T) \neq \mathbf{1}$. ⌟

Proof: □

Arf Invariants

Def. (12.16.2.13) [Pass Moves]. A **Pass move** on an oriented knot diagram is a local strand move by passing two strands of the opposite orientation across two strands of the opposite orientation at the same time. Notice that the orientation of K doesn't influence the definition of this pass move. Two knots are called **pass-equivalent** if they can be connected by a sequence of pass moves. ⌟

Def. (12.16.2.14) [Arf Invariants]. Any knot is pass-equivalent to either the unknot or a trefoil knot(Notice the two trefoil knots are pass-equivalent), and a trefoil knot is not pass-equivalent to the unknot.

The **Arf invariant** $\mathrm{Arf}(K) \in \mathbb{Z}/(2)$ of a knot K is defined to 0 if it is pass-equivalent to the unknot, and 1 otherwise. ⌟

Proof: Cf.[Ada04]P223.? □

Prop. (12.16.2.15). On a local crossing, if $\langle L_+ \rangle$ and $\langle L_- \rangle$ are all knots and $\langle)(\rangle$ is a link with two components, then

$$\mathrm{Arf}(\langle L_+ \rangle) = \mathrm{Arf}(\langle L_- \rangle) + \mathrm{lk}\left(\langle)(\rangle\right).$$

Notice the orientation on $\langle)(\rangle$ doesn't matter to the parity. ⌟

Proof: This may be done using invariant polynomials.? □

3 Chirality

Def. (12.16.3.1)[Chirality]. A knot $K \subset \mathbb{R}^3$ is called **chiral** if it is not equivalent to its mirror image. It is called **achiral** or **amphicheiral** otherwise. ⌟

Prop. (12.16.3.2). Any alternating knot diagram with an odd number of crossings is chiral. ⌟

Proof: □

4 Links

Def. (12.16.4.1) [Linking Numbers]. For an oriented link $L \subset \mathbb{R}^3$ with two component, let D be a link diagram of it, then the **linking number** of L is defined to be half of the sum of crossing signs(12.16.0.7) between two components of L, where 'up' is $+1$ and 'down' is -1. Then this number is an integer, and it is independent of the diagram chosen by checking Reidemeister moves(12.16.0.8), so it is a link invariant of L.

If $L = K \amalg K'$, this number is denoted by $\mathrm{lk}(K, K')$. ⌟

Prop. (12.16.4.2). Suppose K be an oriented knot in $\mathbb{S}^3$. Let N be a tubular nbhd of K, and $X = \mathbb{S}^3 \backslash X$. Then $H_1(X)$ is isomorphic to $\mathbb{Z}$ by Alexander duality, and it is generated by a class represented by a simply closed curve $\mu \subset \partial N$ that bounds a disk in N meeting K at a single point. Let C be another oriented simple closed curve in X, then $\mathrm{lk}(C, K)$ equals $[C] = \mathrm{lk}(C, K).\mu \in H_1(X)$. ⌟

Proof: Cf.[Lickorish]P12. □

5 Links and Graphs

Def. (12.16.5.1) [Intrinsically Linked Graphs]. An **intrinsically linked graph** is a graph K s.t. any embedding of K in $\mathbb{R}^3$ contains a non-trivial link. ⌟

Def. (12.16.5.2) [Intrinsically Knotted Graphs]. An **intrinsically knotted graph** is a graph K s.t. any embedding of K in $\mathbb{R}^3$ contains a knotted cycle. ⌟

Prop. (12.16.5.3) [Conway-Gordon]. Any embedding of the graph K_6 in $\mathbb{R}^3$ contains two triangles with odd linking number. In particular, K_6 is intrinsically linked. ⌟

Proof: In the embedding shown as in [Ada04]P216Figure8.2, it is easy to see that sum of linking numbers between the 10 pairs of 3-cycles in K_6 is odd. Then the assertion follows from(12.16.5.6). □

Lemma (12.16.5.4). The parity of the sum of linking numbers of all the 10 pairs of 3-cycles in K_6 under any embedding is invariant under a crossing change. ⌟

Proof: Clearly a crossing of an edge with itself or a crossing of two adjacent edges doesn't change the sum. And a crossing of two non-adjacent edges changes two linking number by 1, so the parity of the sum is unchanged.

For a crossing of two adjacent edges, □

Prop. (12.16.5.5) [Conway-Gordon]. Any embedding of the graph K_7 in $\mathbb{R}^3$ contains a Hamilton cycle with non-zero Arf invariant. ⌟

Proof: In the embedding shown as in [Ada04]P230Figure, all Hamilton cycles except one is unknotted, and the rest one is a trefoil, so the total sum of Arf invariants of all 360 Hamilton cycles in K_7 under this embedding is 1. Then the assertion follows from(12.16.5.6). □

Lemma (12.16.5.6). The sum of Arf invariants of all 360 Hamilton cycles in K_7 under any embedding is invariant under a crossing change. ⌟

Proof: Cf.[C-G83]P448. □

Prop. (12.16.5.7). $K_{5,5}$ is intrinsically knotted. ⌟

Proof: Cf.[Miki Shimabara1988]. □

Prop. (12.16.5.8). Intrinsically linked graphs are intrinsically knotted. ⌟

Proof: Cf.[RST93]. □

Def. (12.16.5.9) [Peterson Graphs]. A **Peterson graph** is a graph connected to K_6 through $Y - \Delta$ transforms. There are exactly 7 Peterson graphs, Cf.[Ada04]P222.? ⌟

Thm. (12.16.5.10) [Robertson-Seymour-Thomas]. A graph is intrinsically knotted iff it contains a Peterson graph(12.16.5.9). ⌟

Proof: One direction is trivial, for the other, Cf.[RST93]?. □

Conj. (12.16.5.11). Any intrinsically knotted graph contains a subgroup that is an extension(splitting of vertices) of K_7 or $K_{5,5}$. ⌟

Proof: □

6 Tables of Knots

For a table of knots, Cf.[Ada04]P280.

Prop. (12.16.6.1) [2 Crossings]. Any knot diagram with ≤ 2 crossings determine an unknot. ⌟

Proof: ? The only way I can think is to enumerate. □

12.17 Geometric and Combinatorial Group Theory

Cf.[Princeton Companion].

Mednykh's Formula

Thm. (12.17.0.1). For $G \in \mathcal{A}\mathrm{b}^{\mathrm{fin}}$, and Σ_g the oriented closed surface of genus g, then

$$\#\,\mathrm{Hom}(\pi_1(\Sigma_g), G) = \#G \sum_i \Big(\frac{\#G}{\dim V_i}\Big)^{2g-2}.$$

⌟

Prop. (12.17.0.2). For any oriented triangulated surface Σ and $G \in \mathcal{A}\mathrm{b}^{\mathrm{fin}}$, we can associate a rational number in the following way:

1. Let $V = \mathbb{Q}[G]$ which is a non-commutative $\mathbb{Q}$-algebra.
2. Let $a = \frac{1}{\$G^2} \sum_{g,h,k\in G, ghk=1} g \otimes h \otimes k \in V^{\otimes 3}$.
3. Let $N \in (V^{\otimes 2})^*$ be given by $N(g,h) = \#G\delta_{gh,1}$.
4. Label the edges $e_1, \ldots, e_E$ and given each of them an arbitrary orientation, and faces $f_1, \ldots, f_F$ with orientation given by the orientation of Σ.
5. For each face f_i, let the orientation on the boundary be given by the ordered pair $(f_i(1), f_i(2), f_i(3))$(which subjects to a 3-cycle permutation).
6. Consider the element
$$\otimes_i a \in \otimes_i (V^{\otimes 3}),$$
and for each edge $e_j = f_x(a) = f_y(b)$, use the element $N \in (V^{\otimes 2})^*$ to contract the (x,a)-th and (y,b)-th component of $\otimes_i(V^{\otimes 3})$. Then the image of $\otimes_i a$ under this contraction is an element in $\mathbb{Q}$.

Then this element is invariant under isogenies of Σ and Pachner moves of the triangulations. In particular, this element only depends on Σ, by(4.4.11.9). ⌟

Proof: ? □

Prop. (12.17.0.3). Situation as in(12.17.0.2), the number we get is just

$$(\#G)^{\chi(G)-1} \cdot \#\,\mathrm{Hom}(\pi_1(\Sigma), G).$$

⌟

Proof: ? □

13 Theoretical Physics

13.1 Field Theory

Def. (13.1.0.1) [Field Theories]. A **field theory** consists of the following:

- A differentiable manifold M called the **space-time**.
- A target space $V \in \mathcal{V}\text{ect}/\mathbb{R}$.
- A **Lagrangian** $\mathcal{L}$ which is a differential functional on $C^\infty(M, V)$(11.13.1.2).

Moreover, it is called a **field theory of order**$\leq k$ if $\mathcal{L} = \mathcal{L}(\{\partial_I \varphi\}_{|I|\leq k})$ is smooth function on the k-th jet space of M w.r.t. V.

A field theory of order≤ 1 is also called a **classical field theory**. A field theory of order≤ 2 is called a **semi-classical field theory**. ⌟

1 Classical Field Theory

2 Semi-Classical Field Theory

TBA

Prop. (13.1.2.1). Yang-Mills Field. ⌟

3 Perturbative Field Theory

Remark (13.1.3.1) [Path Integrals]. ⌟

4 Conformal Field Theory

5 Dualities

Def. (13.1.5.1). Two field theory are called **equivalent field theories** if expectation values in both theories equal. In particular, the partition function should equal.? ⌟

13.2 Gauge Theory

13.3 Statistical Mechanics

1 Ising Models and Potts Models

Cf.[The Knot Book, Adams].

Prop. (13.3.1.1) [Potts Models and Tutte Polynomials]. Let G be a planer graph and $q \in \mathbb{Z}_+$, then the Potts model on G with q-state and interaction energy $E(S_i, S_j) = \delta_{i,j}$ has partition function

$$Z = T_G(q, e^{-\frac{1}{kT}} - 1),$$

where $T_G(q,t)$ is the Tutte polynomial of G. ⌟

Proof: Cf.[Adams, P240].? □

Prop. (13.3.1.2) [Potts Models and Jones Polynomials]. Any knot diagram can be turned into a signed planer graph G. Then for $q \in \mathbb{Z}_+$, there is aa Potts model on G with q-state and suitable choice of signed interaction energies $E_\pm(S_i, S_j)$ s.t. the partition function is just

$$Z = V_G(t)$$

where $V_G(t)$ is the Jones polynomial, and $t \in \mathbb{C}$ satisfies $q = 2 + t + t^{-1}$. ⌟

Proof: Cf.[Adams, P213].? □

13.4 Quantum Field Theory

Main references are [Witten, Super-symmetry and Morse Theory]. [Witten, Topological Quantum Field Theory, 1988]. [Witten, Elliptic Genera and Quantum Field Theory], [Quantum Field Theory and the Jones Polynomial, Witten], [Supersymmetry and Morse Theory, Witten], [Etingof's notes], [Skinner's notes, https://www.damtp.cam.ac.uk/user/dbs26/AQFT.html].

Def. (13.4.0.1) [Quantum Field Theory]. A **quantum field theory** consists of the following:

- A Riemannian manifold M.
- A field, which is a map $M \to N$ where N is also a manifold.
- A space $\mathcal{C}$ of configurations on M, each $\varphi \in \mathcal{C}$ corresponds to a field.

⌟

Def. (13.4.0.2) [Actions of Quantum Field Theory]. An action of a quantum field theory is a map $S : \mathcal{C} \to \mathbb{R}$. The critical points of S corresponds to classical Euler-Lagrangian equations. Usually S is assumed to be local, i.e. can be written as functions of φ and its derivatives.

The main tool to study QFT is the path integral

$$\int_{\mathcal{C}} g(\varphi) e^{-S(\varphi)/\hbar} \mathrm{d}\varphi.$$

If $g = \mathbf{1}$, this is called the path integral $Z(M, g, S)$, and if $\mathcal{O}_i$ are some operators(functions on $\mathcal{C}$), the integral

$$\langle \prod_i \mathcal{O}_i(\varphi) \rangle = \int_{\mathcal{C}} \prod_i \mathcal{O}_i(\varphi) e^{-S(\varphi)/\hbar} \mathrm{d}\varphi$$

is called the correlation function between the $\mathcal{O}_i$s.

For example, ?analogous as in Brownian Motion, the motion $q = q(t)$ of a quantum particle in $\mathbb{R}^N$(1-dimensional QFT) is determined by the **correlation functions**

$$\mathrm{Cor}(q_{j_1}(t_1), \ldots, q_{j_n}(t_n)) = \int_{P_{a,b}} q_{j_1}(t_1) \cdot \ldots \cdot q_{j_n}(t_n) e^{-\mathrm{i}\, S(q)/\hbar} \mathrm{D}q, \quad S(q) = \int_a^b (\frac{1}{2}\dot{q}^2 - U(q)) \mathrm{d}t.$$

⌟

Def. (13.4.0.3) [Path Integral on Manifolds with Boundaries]. If M has boundaries, for each boundary component B_i, the possible fields form a Hilbert space $\mathcal{H}_i$. Thus Path integral defines a map

$$\otimes \mathcal{H}_i \to \mathbb{C} : \otimes \psi_i \mapsto \int_{\varphi, \varphi|_{B_i} = \psi_i} e^{-S(\varphi)/\hbar} \mathrm{d}\varphi.$$

In particular if $M = N \times \mathbb{I}$, then by duality it defines a map

$$U : \mathcal{H} \to \mathcal{H} : (U\psi_0, \psi_1) = \int_{\varphi, \varphi|_{N\times\{0\}} = \psi_0, \varphi|_{N\times\{1\}} = \psi_1} e^{-S(\varphi)/\hbar} \mathrm{d}\varphi.$$

⌟

1 Perturbative QFT

0-dimensional QFT, Feynman Calculus

Remark (13.4.1.1). Here we are interested in the case that $M = \mathrm{pt}$, and the fields are maps $M \to V \cong \mathbb{R}^n$. ⌟

Remark (13.4.1.2) [Situations]. Situation as in(11.11.2.26), with $S(x) = f(x)$, we get a smooth function $I(x) \in C^\infty([0,\infty))$ s.t.

$$I(\hbar) = \hbar^{\frac{-d}{2}} e^{\frac{S(c)}{\hbar}} \int_D g(x) e^{-\frac{S(x)}{\hbar}} \mathrm{d}x,$$

and by(11.11.2.23), the expansion of $I(\hbar)$ at $\hbar = 0$ only depends on derivatives of g at c. Thus to understand the expansion of $I(\hbar)$, it suffices to understand the **correlation functions**:

$$\langle l_1, \ldots, l_N \rangle = \hbar^{-\frac{d}{2}} \int_D l_1(x). \ldots . l_N(x) e^{-\frac{S(x)}{\hbar}} \mathrm{d}x$$

for any $N \in \mathbb{N}, l_1, \ldots, l_N \in V^*$. When $N = 0$, this is called the **partition function**.

Notice in view of the expansion of $\hbar$, we may replace D with V(by reason as in the proof of(11.11.2.26)), and WLOG, we may assume that $c = 0$, and the Taylor expansion of $S(x)$ at $x = 0$ is

$$S(x) = S(0) + \frac{B(x,x)}{2} - \sum_{i\geq 3} \frac{B_i(x, \ldots, x)}{i!}, B_i = \partial^i f(0),$$

where B^{-1} is called the **propagator**, and $B_i/i!$ are called the **interaction terms**. ⌟

Def. (13.4.1.3) [Feynman Graphs]. A **Feynman graph** is a finite multi-graph s.t. there are no vertices of valence 2. For $N \in \mathbb{N}$, let $\mathrm{Feyn}_{\geq 3}(N)$ be the isomorphism classes of Feynman graphs with N fixed vertices of valence 1 with a labeling of them.

And if $\underline{n} = (n_0, \ldots, n_k, \ldots)$, let $\mathrm{Feyn}(\underline{n})$ be the isomorphism classes of finite multi-graphs s.t. for any $k \in \mathbb{N}$, there are exactly n_k-many vertices of valence k. ⌟

Def. (13.4.1.4) [Feynman Amplitudes]. Situation as in (11.11.2.21), given

- $B_k \in \mathrm{Sym}^k(V^*)$ for each $k \in \mathbb{Z}_{\geq 3}$,
- $N \in \mathbb{N}$, and $l_1, \ldots, l_N \in V^*$,
- a Feynman graph $\Gamma \in \mathrm{Feyn}(N)$,

let the **Feynman amplitude** $\mathrm{Feyn}_\Gamma(l_1, \ldots, l_N)$ to be defined by the following procedure:

- For $i \in [N]_+$, put l_i on the i-th labeled vertex of Γ of valence 1,
- For $k \in \mathbb{Z}_+$, put B_k on each unlabeled vertex of Γ of valence k.
- Put B^{-1} on each edge of Γ.
- Tensor the tensors on the vertices together, and contract them using the B^{-1} on the edges. The resulting tensor is a real number.

⌟

Lemma (13.4.1.5) [Wick's Theorem]. Situation as in(11.11.2.21), if $N \in \mathbb{Z}_+$ and $l_1, \ldots, l_N \in V^*$, then

$$\int_V l_1(x). \ldots . l_N(x) e^{-\frac{B(x,x)}{2}} \mathrm{d}x = \begin{cases} \frac{(2\pi)^{d/2}}{\det B} \sum_{\sigma \in \Pi_{N/2}} \prod_{i \in \{1,\ldots,n\}/\sigma} B^{-1}(l_i, l_{\sigma(i)}) & 2|N \\ 0 & 2 \nmid N \end{cases},$$

where $\Pi_{N/2}$ is the set of matching on $[N/2]_+$. ⌟

Proof: If $2 \nmid N$, this is obvious because the integrand is an odd function. Suppose $n = 2k$, then both sides are symmetric and multilinear in $(l_1, \ldots, l_N)$, so it suffices to show for $l_1 = l_2 = \ldots = l_n = l$. And by change of variable, we may assume that there is a basis $\{x_1, \ldots, x_n\}$ of V s.t. $l(x) = x_1$, and $B(x_1, \ldots, x_n) = x_1^2 + \ldots + x_n^2$. Then by integrating out $x_2, \ldots, x_n$ using(11.11.2.23), it suffices to show that

$$\int_{-\infty}^{\infty} x^{2k} e^{-x^2/2} \mathrm{d}x = \sqrt{2\pi}(2k-1)!!,$$

which is true by integration by part and **??**. □

Thm. (13.4.1.6) [Feynman Calculus, Variational Form]. Suppose

$$S(x) = \frac{B(x,x)}{2} + \widetilde{S}(x),$$

where $\widetilde{S}(x) = -\sum_{i \in \mathbb{N}} g_i B_i(x, \ldots, x)/i!$, g_i being formal parameters(g_0 is called the **vacuum energy**, g_1 is called the **tadpole**, g_2 is called the **mass**), and consider the partition function

$$Z = \hbar^{-\frac{d}{2}} \int_V e^{-S(x)/\hbar}.$$

Then

$$Z_S = \frac{(2\pi)^{\frac{d}{2}}}{\sqrt{\det B}} \sum_{\underline{n} \in (\mathbb{N})^{\mathbb{N}}} \Big(\prod_i g_i^{n_i}\Big) \sum_{\Gamma \in \mathrm{Feyn}(\underline{n})} \frac{\hbar^{b(\Gamma)}}{\# \mathrm{Aut}(\Gamma)} \mathrm{Feyn}_\Gamma,$$

where $b(\Gamma) = \#E(\Gamma) + N - \#V(\Gamma)$.

And by decomposing Γ into connected components, there is also a logarithmic form:

$$\log \frac{Z_S}{Z_0} = \sum_{\underline{n} \in (\mathbb{N})^{\mathbb{N}}} \Big(\prod_i g_i^{n_i}\Big) \sum_{\Gamma \in \mathrm{Feyn}_{\mathrm{cntd}}(\underline{n})} \frac{\hbar^{b(\Gamma)}}{\# \mathrm{Aut}(\Gamma)} \mathrm{Feyn}_\Gamma, \quad Z_0 = \frac{(2\pi)^{\frac{d}{2}}}{\sqrt{\det B}}.$$

This is called the **loop expansion**, because for Γ connected, $b(\Gamma) + 1$ is the number of loops in Γ. ⌟

Cor. (13.4.1.7) [Feynman Calculus, Taylor Expansion Form]. Situation as in(13.4.1.2), for any $N \in \mathbb{N}$ and $l_1, \ldots, l_N \in V^*$, we have

$$\langle l_1, \ldots, l_N \rangle = \frac{(2\pi)^{\frac{d}{2}}}{\sqrt{\det B}} \sum_{\Gamma \in \mathrm{Feyn}(N)} \frac{\hbar^{b(\Gamma)}}{\# \mathrm{Aut}(\Gamma)} \mathrm{Feyn}_\Gamma(l_1, \ldots, l_N)$$

as a formal power series in $\hbar$, . ⌟

Proof: As both sides are symmetric and multilinear in $(l_1, \ldots, l_N)$, it suffices to show for $l_1 = \ldots = l_n = l$. Then it suffices to calculate the Taylor expansion of

$$\langle e^{l(x)}, \ldots, e^{l(x)} \rangle = \hbar^{-\frac{d}{2}} \int_V e^{l(x) - \frac{S(x)}{\hbar}} \mathrm{d}x$$

which is exactly calculated by(13.4.1.6). And the conclusions match, noticing that one is labeled and one is unlabeled so there is a multiple by $N!$. □

Matrix Integrals

Remark (13.4.1.8) [Situations]. For $N \in \mathbb{Z}_+$, let Herm^N be the set of Hermitian matrices of size N, with the inner product form $(A_1, A_2) = \mathrm{tr}(A_1 A_2)$, with a Lebesgue measure $\mathrm{d}\mu$ normalized s.t.

$$\int_{\mathrm{Herm}^N} e^{-\frac{\mathrm{tr}(A^2)}{2}} \mathrm{d}\mu A = 1.$$

Consider the path integral

$$Z_N = \hbar^{-N^2/2} \int_{\mathrm{Herm}_N} e^{-\frac{S(A)}{\hbar}} \mathrm{d}\mu A,$$

where the action functional is

$$S(A) = \frac{\mathrm{tr}(A^2)}{2} - \sum_{m \in \mathbb{N}} g_m \frac{\mathrm{tr}(A^m)}{m}.$$

We are intersected in the behavior of the coefficients of the expansion of Z_N in g_i for large N. ⌟

2 Supersymmetric QFT

Main references are [Supersymmetry and Morse Theory, Witten].

3 Topological QFT

Main references are [Ati88], [On the Classification of Topological Field Theories, Lurie].

Remark (13.4.3.1). It now seems clear that the way to investigate the subtleties of low-dimensional manifolds is to associate to them suitable infinite-dimensional manifolds (e.g. spaces of connections) and to study these by standard linear methods (homology, etc.). In other words we use quantum field theory as a refined tool to study low-dimensional manifolds. ——Atiyah. ⌟

Def. (13.4.3.2) [Topological Quantum Field Theory]. A **topological quantum field theory** or TQFT in dimension d defined over a ground ring $\Lambda \in \mathcal{CA}\mathrm{lg}$ consists of the following data:

- For any $\Sigma \in \mathcal{D}\mathrm{iff}^d_{\mathrm{orntd,cpct}}$, there is a finite Λ-module $Z(\Sigma)$, called the **states of particles of** Σ.
- For any $M \in \mathcal{D}\mathrm{iff}^{d+1}_{\mathrm{orntd},\partial}$, there is an element $Z(M) \in Z(\partial M)$, called the **vacuum state defined by** M.

s.t.

- Z are functorial in orientation-preserving diffeomorphisms of Σ or M.
- Z are involutary, i.e. $Z(\Sigma^*) = Z(\Sigma)^*$, where Σ^* is Σ with the dual orientation and $Z(\Sigma)^*$ is the dual module of $Z(\Sigma)$.
- Z is multiplicative, i.e. $Z(\Sigma_1 \coprod \Sigma_2) = Z(\Sigma_1) \otimes Z(\Sigma_2)$, and if $\partial M_1 = \Sigma_1 \coprod \Sigma_3, \partial M_2 = \Sigma_3 * \coprod \Sigma_2, M = M_1 \coprod_{\Sigma_3} M_2$, then
$$Z(M) = \langle Z(M_1), Z(M_2) \rangle$$
where the pairing is the natural pairing $Z(\Sigma_3) \times Z(\Sigma_3)^* \to \Lambda$.
- $Z(\varnothing^d) = \Lambda$, and $Z(\varnothing^{d+1}) = 1 \subset \Lambda = Z(\varnothing^d)$.

⌟

Prop. (13.4.3.3) [Cobordisms]. If For $M \in \mathfrak{Diff}^{d+1}_{\text{orntd},\partial}$, if $\partial M = \Sigma_1^* \coprod \Sigma_2$, then $Z(M) \in Z(\Sigma_1)^* \otimes Z(\Sigma_2)$ can be regarded as a homomorphism $Z(M) : Z(\Sigma_1) \to Z(\Sigma_2)$, and this is compatible with composition of cobordisms. In particular, if $\Sigma \in \mathfrak{Diff}^{d}_{\text{orntd,cpct}}$, $M = \Sigma \times [0,1]$, then $Z(M) = \text{id} \in \text{End}(Z(\Sigma))$.

In particular, the states of particles and the vacuum states(13.4.3.2) can be calculated by cut-and-paste. ⌟

Def. (13.4.3.4) [Vacuum-Vacuum Expectation Values]. For $M \in \mathfrak{Diff}^{d+1}_{\text{orntd,cpct}}$, $Z(M) \in Z(\partial M = \varnothing) = \Lambda$ is an element, called the **vacuum-vacuum expectation value** of M. ⌟

Prop. (13.4.3.5) [Homotopy Invariance]. Let $\Sigma, \Sigma' \in \mathfrak{Diff}^{d}_{\text{orntd,cpct}}$, $M = \Sigma \times [0,1]$, $M' = \Sigma' \times [0,1]$, and $F : M \to M'$ is a homotopy of morphisms between $f_1, f_2 : \Sigma \to \Sigma'$, then $Z(f) = Z(f') : Z(\Sigma') \to Z(\Sigma)$, by(13.4.3.3). ⌟

Examples of Topological QFT

Remark (13.4.3.6). For $d = 1$, there are Floer/Gromov theory and holomorphic conformal field theories. ⌟

Remark (13.4.3.7). For $d = 2$, there are Jones/Witten theory, Casson theory, Johnson theory, and "Thurston" theory. ⌟

Remark (13.4.3.8). For $d = 3$, there are Floer/Donaldson theory. ⌟

4 Vector Operator Algebras

Cf.[Princeton Companion].

13.5 Renormalization

13.6 Mirror Symmetry

Cf.[Princeton Companions].

14 Algebraic Number Theory

14.1 Additive Number Theory

References are [Introduction to the theory of numbers, Hardy-Wright]. [Some Results in the Additive prime-number theory, Long-Keng Hua].

1 Circle Methods

Prop. (14.1.1.1). For any $\alpha \in \mathbb{R} \setminus \mathbb{Z}$ and $M \in \mathbb{Z}_+$,

$$\sum_{n=1}^{M} e^{2\pi\,\mathrm{i}\,\alpha n} \leq \frac{1}{2\{\{\alpha\}\}}.$$

⌟

Proof:

$$|\sum_{n=1}^{M} e^{2\pi\,\mathrm{i}\,\alpha n}| = |\frac{e^{2\pi\,\mathrm{i}\,\alpha M} - 1}{e^{2\pi\,\mathrm{i}\,\alpha} - 1}| \leq |\frac{2}{2\sin(\pi\alpha)}| \leq \frac{1}{2\{\{\alpha\}\}}(11.3.7.2)$$

□

14.2 p-adic Analysis

References are [Non-Archimedean Analysis Part A] and [p-adic numbers, p-adic analysis and zeta functions, Koblitz].

This section should only contain theorems that are only applicable to non-Archimedean valuations. Theorems that are applicable to both Archimedean and non-Archimedean valuations should be put into11.7.

As far as I know, all properties proved in Functional Analysis independent of complex analysis is applicable to the non-Archimedean case, and in fact, the goal of this section is to build an analytic theory parallel to complex analysis.

1 (Ultranormed) Valuation Theory

Ultranormed Rings

Def. (14.2.1.1) [Normed Groups]. A **semi-normed group** is a group with a non-Archimedean valuation, it is called a **normed group** iff the valuation has kernel 0, which is equivalent to Hausdorff.

A normed group is totally connected, because open balls at 0 are subgroups hence closed. ⌟

Def. (14.2.1.2) [Normed Ring]. A **(semi-)normed ring** is a (semi-)normed additive group that

- $|1| = 1$. or the valuation is trivial.
- $|ab| \leq |a||b|$.

A **valued ring** is a normed ring with $|ab| = |a||b|$. It is called **degenerate** if all non-zero valuation value≥ 1. ⌟

Prop. (14.2.1.3). A valuation on a ring is non-Archimedean iff $\{|n|\}$ is bounded. Thus any valuation on a field with finite characteristic is non-Archimedian. ⌟

Prop. (14.2.1.4). In a normed ring, every triangle is an acute isosceles triangle. (This is because the biggest is smaller than the maximal of the other two, thus the biggest two are equal). Hence we have, for a circle $B(O, r)$, any interior point P is a center of circle, because $OP < r$. ⌟

Def. (14.2.1.5) [Bald Rings]. A normed ring R is call a **B-ring** if elements of valuation 1 is invertible, it is called **bald** if there is a ε that no elements has valuation in $(1 - \varepsilon, 1)$. ⌟

Def. (14.2.1.6) [Uniform Rings]. A non-Archimedean ring A is called **uniform** if the set of topologically nilpotent elements are bounded in A. ⌟

Prop. (14.2.1.7). If K is a normed field with valuation ring R, the smallest subring containing a zero sequence $a_0, a_1, \ldots$ is bald(14.2.1.5). ⌟

Proof: Cf.[Formal and Rigid Geometry P25]. □

Def. (14.2.1.8) [Topologically Nilpotent Elements]. An element a in a normed ring A is called **topologically nilpotent** iff $\lim a^n = 0$. The set of all topological nilpotent elements in A are denoted by A^0. ⌟

Prop. (14.2.1.9). $\check{A}$ is a subgroup of A^+, which is multiplicatively closed, then A^0 is clopen in A. In particular, A^0 is complete if A is complete. ⌟

Proof: Cf.[Non-Archimedean analysis P27]. □

Prop. (14.2.1.10) [Nakayama's Lemma]. If A is complete normed ring and M is a A-module, if there are f.m. elements x_i of M that $M = N + \sum x_i M$, then $M = N$. ⌟

Proof: The proof is verbatim as the proof of the usual Nakayama lemma. □

Normed Modules

Def. (14.2.1.11) [Ultranormed Module]. A module M over a normed ring A is called **normed module** iff it is a normed additive group and $|ax| \leq |a||x|$ for $a \in A, x \in M$. If A is valued and the equality always holds, we call it **faithfully normed** or **valued module**.

If A is a valued field, any normed module is valued. ⌟

Prop. (14.2.1.12) [Ultranormed Algebra]. A normed algebra is an A algebra B with $A \to B$ bounded of norm 1. ⌟

Prop. (14.2.1.13). For two valued module over A, if A is non-degenerate, a morphisms is bounded iff it is continuous. This is because we can multiply by elements of A to reduce to a nbhd of 0.

This applies to the case when A contains a field where the valuation is non-trivial, because we can use(14.2.1.11). ⌟

Def. (14.2.1.14) [Completed Tensor Product]. For two normed modules over a normed ring R, there is a complete normed R-module $M\widehat{\otimes}N$ called the **completed tensor product**, satisfying the following universal properties: $M \times N \to M\widehat{\otimes}N$ is bounded by 1, and for any complete normed R-module T and a R-map $M \times N \to T$ bounded by a, then it factor through a R-map $M\widehat{\otimes}N \to T$ bounded by a.

It satisfies many universal properties as you can imagine. ⌟

Proof: Cf.[Formal and Rigid Geometry P238]. □

Cor. (14.2.1.15). By(14.2.1.13), when A is non-degenerate, then the amalgamated sum is just the fibered pushout when restricted to the category of complete valued module over A with continuous maps as morphisms, because it satisfies the universal property. ⌟

Prop. (14.2.1.16)[Amalgamated Sum]. For two normed R-algebras there is an operation of **amalgamated sum** which satisfies universal properties similar to(14.2.1.14). In fact, it is just the completed tensor product when seen as modules. ⌟

Proof: Cf.[Formal and Rigid Geometry P242]. □

Weakly Cartesian Space

Def. (14.2.1.17) [Weakly Cartesian Vector Spaces]. A normed K-vector space over a valued field K is called **weakly Cartesian** if**?** ⌟

Prop. (14.2.1.18). If K is a complete valued field, then each normed K-vector space V is weakly Cartesian. ⌟

Proof: Cf.[Non-Archimedean Analysis P92]. □

Completeness

Prop. (14.2.1.19) [Cauchy Sequence of Non-Archimedean field]. For a sequence $\sum a_i$ in a non-Archimedean field, it is a Cauchy sequence iff $\lim |a_i| = 0$.

In particular, convergent sequence are all absolutely convergent and for a Cauchy sequence not converging to 0, the valuations of the terms stabilize. ⌟

Proof: One way is easy, the other way, notice $|\sum_{v=i}^{j} a_i| \leq \max_{i,i+1,\ldots j} |a_v| < \varepsilon$. □

Prop. (14.2.1.20) [Completion of a Field]. The completion of a non-Archimedean field is preferred to choose the definition of Cauchy sequence, so we see by(14.2.1.19) that $v(\widehat{K}) = v(K)$. ⌟

Prop. (14.2.1.21). For a complete field K and any finite vector space L, L has only one norm up to equivalence and it is complete. ⌟

Proof: Cf.[Formal and Rigid Geometry P230]. □

Prop. (14.2.1.22). A complete valuation on a field can extend uniquely to a valuation on its alg.closure. And in the finite case, it is $|\alpha| = |N(\alpha)|^{\frac{1}{d}}$. This is an immediate consequence of(14.2.1.33) and(14.2.1.30), and $|\alpha| \leq 1$ iff it is integral over valuation ring R of K. ⌟

Prop. (14.2.1.23). Any infinite separable algebraic extension of a complete field is never complete. ⌟

Proof: We use Krasner's lemma(14.2.1.34). By Ostrowski theorem(11.2.3.18), we can assume it is non-Achimedean, otherwise it cannot by infinite dimensional. Choose an infinite linearly independent basis of decreasing value rapidly enough, then we can see the field generated by the limit contains all the partial sums, contradiction. □

Prop. (14.2.1.24). If $K = \overline{K}$, then $\widehat{K} = \overline{\widehat{K}}$. ⌟

Proof: Let $L = \overline{\widehat{K}}$, then we can extend to a valuation on L, now let f be a monic polynomial with coefficients in $\widehat{K}$, we show its root $\alpha \in L$ can be approximated by elements in K, now let g monic in $K[X]$ be an approximation of f that $|g(\alpha)| \leq \varepsilon^n$, then there is a root β of g that $|\alpha - \beta| < \varepsilon$, and $\beta \in K$ by alg.closedness. □

Prop. (14.2.1.25). If K is a complete, then K^{sep} is dense in $\overline{K}$. ⌟

Proof: Assume F is non-Archimedean, then for $y \in F^{alg}$, there is a n that $y^{p^n} = \alpha \in F^{sep}$. We may assume $|\alpha| \leq 1$, then let π be an element that $|\pi| < 1$, then if y_i is a root of the separable polynomial $Y^{p^n} - \pi^i Y - \alpha = 0$, then $(y - y_i)^{p^n} = \pi^i y_i$. So $|y - y_i| \to 0$. □

Def. (14.2.1.26) [$\mathbb{Q}_p$, Hensel1897]. For $p \in \mathbf{P}$, $\mathbb{Q}_p$ is defined to be the p-adic completion of $\mathbb{Q}$, called the **field of p-adic numbers**. Its ring of integer is $\mathbb{Z}_p$, which equals the p-adic completion of $\mathbb{Z}$, called the **ring of p-adic integers**. ⌟

Prop. (14.2.1.27). There is a non-canonical isomorphism $\overline{\mathbb{Q}_p} \cong \mathbb{C}$, not compatible the topology. ⌟

Proof: This follows from(3.2.7.5) and the fact they both have the same cardinality $\aleph_1$. □

Cor. (14.2.1.28). The p-adic valuation on $\mathbb{Q}$ can be extended to $\mathbb{C}$ non-canonically. ⌟

Henselian Valued Fields

Def. (14.2.1.29) [Henselian Valued Field]. A **Henselian valued field** is a valued field K that the valuation ring $\mathcal{O}_K$ is a Henselian local ring(5.3.10.1). ⌟

Prop. (14.2.1.30). A valued field K is Henselian(14.2.1.29) iff the valuation of K has a unique extension to any finite extension L/K. ⌟

Proof: Cf.[Algebraic Number Theory Neukirch P144]. □

Def. (14.2.1.31) [Ramification Degrees]. If L/K is a finite extension of valued field of degree n, then v extends uniquely to $w(\alpha) = \frac{1}{n}v(N_{L/K}(\alpha))$, now we define the **ramification degree** as $[w(L^*) : v(K^*)]$, and the **inertia degree** as the degree of the residue field extension.

Thus for a normal extension, x and $\sigma(x)$ has the same valuation. Hence any polynomial in $K[X]$ has a decomposition into polynomials where all their roots has the same valuation. ⌟

Prop. (14.2.1.32) [Hensel's Lemma Generalized]. Let K be a complete valued non-Archimedean field and $\mathcal{O}_K$ be the valuation ring. If $P, Q, R \in \mathcal{O}_K[X]$ and $0 \le \lambda < 1$ that $\deg P = m + n, \deg Q = n, \deg R = m$, and

$$\deg(P - QR) \le m + n - 1, \quad |P - QR|_G \le \lambda |\operatorname{res}(Q, R)|^2$$

Where $|-|_G$ is the induced Gauss norm on $K[X]$. Then there exist polynomials U, V that

$$|U|_G, |V|_G \le \lambda |\operatorname{res}(Q, R)|^2, \deg U \le n - 1, \deg V \le m - 1$$

and $P = (Q + U)(R + V)$. ⌟

Proof: If $\rho = |\operatorname{res}(Q, R)| = 0$, then $P = QR$. Otherwise, the map $\theta_{Q,R} : W_m \oplus W_n \to W_{m+n}$ is invertible(3.3.1.9). Then we let $\varphi(U, V) = \theta_{Q,R}^{-1}(P - QR - UV)$, then If $U, V \in B(0, \lambda\rho)$, then $|\varphi(U, V)|_G \le \lambda\rho$. And it can be proved φ is a contraction map from $B(0, \lambda\rho)^2$ to itself with contraction factor λ, so it has a fixed point (U, V) by(4.4.8.9). So $QU + RV = P - QR - UV$. □

Cor. (14.2.1.33) [Hensel's Lemma]. Let K be a complete field, $P(X) \in \mathcal{O}_K[X]$ and $\alpha_0 \in \mathcal{O}_K$ s.t. $|P(\alpha_0)| < |P'(\alpha_0)|^2$, then there exists a $\alpha \in \mathcal{O}_K$ that $P(\alpha) = 0$ and $|\alpha - \alpha_0| \le |P(\alpha_0)/P'(\alpha_0)|$.

In particular, this holds when $|P'(\alpha_0)| = 1$ and $|P(\alpha_0)| < 1$, in which case we can pass to the residue field. Equivalently, a complete valued field is Henselian(14.2.1.29). ⌟

Proof: Let $\lambda = |P(\alpha_0)/P'(\alpha_0)|$ and $\operatorname{res} = P'(\alpha_0)$. Notice If $P(X) = Q(X)(X - \alpha_0) + P(\alpha)$, then $\operatorname{res}(Q(X), X - \alpha_0) = Q(\alpha_0) = P'(\alpha_0)$(3.3.1.11). **?** □

Prop. (14.2.1.34) [Krasner's Lemma]. If $\alpha, \beta \in \overline{K}$ that $|\alpha - \beta| < |\alpha - \sigma(\alpha)|$ for all σ, then $K(\alpha, \beta)/K(\beta)$ is purely inseparable. So when α is separable over K, $K(\alpha) \in K(\beta)$. ⌟

Proof: It suffice to prove that for all field morphism $\tau : K(\alpha, \beta) \to \overline{K}$ fixing $K(\beta)$, $\tau(\alpha) = \alpha$. This is because $|\tau(\alpha) - \beta| = |\alpha - \beta| < |\alpha - \sigma(\alpha)|$, thus $|\tau(\alpha) - \alpha| \le \max\{|\tau(\alpha) - \beta|, |\beta - \alpha|\} < |\alpha - \sigma(\alpha)|$. □

Cor. (14.2.1.35). If f is a separable irreducible polynomial and α is a root, then for g closed enough to f, there is a root β of g that $K(\beta) = K(\alpha)$. (Immediate consequence of(11.2.3.19)). ⌟

Cor. (14.2.1.36). Any finite separable extension $\mathcal{L}/\widehat{K}$ is of the form $L_0\widehat{K}$ for some finite separable extension L_0/K. (Because of primitive element theorem **?**). ⌟

Cor. (14.2.1.37). $K \subset \overline{K}$ is dense, then $K = \overline{K}$. ⌟

2 Extensions of Henselian Valued Fields

Notation (14.2.2.1).
- Let $(K, v, \mathcal{O}_K, \mathfrak{p}_v, \varpi, k)$ be a Henselian non-Archimedean valued field of residue characteristic p, and $\varpi \in K^\times, |\varpi| < 1$ a uniformizer. If $\mathcal{O}_K$ is DVR, assume $(\pi) = \mathfrak{p}_v$.

⌟

Lemma (14.2.2.2) [Extension is Monogenous]. For a finite extension of CDVR, if the residue field extension λ/k is separable, then there exists a $x \in \mathcal{O}_L$ that $\mathcal{O}_K[x] = \mathcal{O}_L$. ⌟

Proof: If $\overline{x}$ is an element of λ that generate λ over k, by primitive element theorem, then let $\overline{f}$ be the minipoly of $\overline{x}$, then let f, x be lifting of them, then $f(x)$ is a uniformizer, otherwise $f'(x)$ has valuation 0, so $f(x + \pi_L)$ is a uniformizer. Now we see that $x^i f(x)^j$ is a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$, □

Prop. (14.2.2.3). If L/K is a finite separable extension and if I is an ideal of $\mathcal{O}_L$, then $v_K(\mathrm{tr}_{L/K}(I)) = \lfloor v_K(I.\mathfrak{D}_{L/K}) \rfloor$. ⌟

Proof: By definition, $\mathrm{tr}_{L/K}(x\mathcal{O}_L) \subset \mathcal{O}_K$ iff $x \in \mathcal{D}^{-1}_{L/K}$, thus $\mathrm{tr}_{L/K}(I) \subset J$ iff $I \subset \mathcal{D}^{-1}_{L/K} J$, i.e. $\mathrm{tr}_{L/K}(I)$ is the smallest ideal J of $\mathcal{O}_K$ that contains $I \cdot \mathcal{D}_{L/K}$, thus the result. □

Unramified Extensions

Def. (14.2.2.4) [Unramified Extensions]. A finite extension L/K is called **unramified extension** if the residue field extension λ/k is separable and $[L : K] = [\lambda : k]$. Any algebraic extension is called **unramified** iff any finite extension is unramified.

This is compatible because unramified extensions form a distinguished class. So we can talk about the **maximal unramified extension** T of K, and a field extension L/K is called **unramified** if all finite subextensions are unramified. ⌟

Proof: It is faithfully transitive because the field extension degree is transitive, and for base change, as the residue field is separable, we let $\lambda = k[\overline{\alpha}]$, and choose a lift $\alpha \in \mathcal{O}_L$, the minipoly of α is $f(X) \in \mathcal{O}_K[X]$. Then we have

$$[\lambda : k] \leq \deg \overline{f} = \deg f = [K(\alpha) : K] \leq [L : K] = [\lambda : k]$$

So $L = K(\alpha)$ and $\overline{f}$ is the minipoly of $\overline{\alpha}$. Then $L' = K'(\alpha)$, and let $g(X)$ be the minipoly of α over K', then $\overline{g}$ is a factor of $\overline{f}$ so separable, hence irreducible by Hensel's lemma. Noe:

$$[\lambda' : k'] \leq [L' : K'] = \deg g = \deg \overline{g} = [k'(\alpha) : k'] \leq [\lambda' : k].$$

So $[\lambda' : k'] = [L' : K']$. □

Prop. (14.2.2.5) [Maximal Unramified Extension]. The residue field of the maximal unramified extension K^{ur}/K is $\overline{k}$, and the value group is the same as K. ⌟

Proof: The first assertion is because for any separable polynomial, it has a lift which is irreducible has a root lifting $\overline{\alpha}$, contradicting the maximality. For the second, look at finite subextensions, then it results from the fundamental inequality(11.2.3.20). □

Tamely Ramified Extensions

Def. (14.2.2.6) [Tamely Ramified Extension]. For K a Henselian non-Archimedean valued field, a finite field extension L/K is called a **tamely ramified extension** if the residue field extension is separable and $([L:T],p)=1$, where T is the maximal unramified subextension. ⌟

Prop. (14.2.2.7). Tamely unramified extensions form a distinguished class, so we can talk about the maximal tamely unramified extensions, and a field extension L/K is called **tamely ramified** if all finite subextensions are tamely unramified. ⌟

Proof: Cf.[Algebraic Number Theory Neukirch P156]. □

Prop. (14.2.2.8). A finite extension L/K is tamely ramified iff the extension is generated by radicals over the maximal unramified extension: $L=K^{\mathrm{ur}}(\sqrt[m]{a_i}),(m,p)=1$, where $a_i\in K^{\mathrm{ur}}$, (WARNING: make sure if $a_i\in K$ or not?). ⌟

Proof: Cf.[Algebraic Number Theory Neukirch P155]. □

Prop. (14.2.2.9). The value field of tamely ramified extensions. Cf.[Neukirch P157]. ⌟

Totally Ramified Extensions

Def. (14.2.2.10) [Eisenstein Polynomial]. Let $(R,\mathfrak{m})$ be a DVR, an **Eisenstein polynomial** in $R[T]$ is a polynomial of the form

$$f(T)=T^n+a_{n-1}T^{n-1}+\ldots+a_1T+a_0$$

where $a_i\in\mathfrak{m}$ for any i and $a_0\in\mathfrak{m}\backslash\mathfrak{m}^2$. ⌟

Prop. (14.2.2.11) [Totally Ramified Extensions via Eisenstein Polynomials]. If $e(T)$ is an Eisenstein polynomial in $\mathcal{O}_K[T]$ and Π is a root of $e(T)$ in $\overline{K}$, then $L=K(\Pi)$ is a totally ramified extension of K with uniformizer Π. Conversely, if L/K is a totally ramified and $\Pi\in L$ is a uniformizer, then $L=K(\Pi)$ and the minimal polynomial of Π is an Eisenstein polynomial. ⌟

Proof:

□

Remark (14.2.2.12). More about totally ramified extensions are discussed in Totally Ramified Extensions. ⌟

Ramification Groups

Def. (14.2.2.13) [Ramification Groups]. For a Galois extension L/K of CVDRs, denote λ/k residue fields extension of $w|v$, and denote $\mathfrak{p}_w,\mathfrak{p}_v$ by $\mathfrak{P},\mathfrak{p}$. Define:

The **inertia group** is $I(L/K)=\{\sigma\in\mathrm{Gal}(L/K)|\sigma(x)\equiv x\mod\mathfrak{P}\}$.

The **ramification group** is $R(L/K)=\{\sigma\in\mathrm{Gal}(L/K)|\sigma(x)/x\equiv 1\mod\mathfrak{P}\}$. ⌟

Prop. (14.2.2.14). For local fields, the ramification degree e equals the order of inertia group $|I_{L/K}|$. ⌟

Prop. (14.2.2.15). The residue field extension λ/k is normal and there is an exact sequence

$$1\to I(L/K)\to\mathrm{Gal}(L/K)\to\mathrm{Gal}(\lambda/k)\to 1.$$

⌟

Proof: Cf.[Neukirch P172]. □

Prop. (14.2.2.16). $R(L/K)$ is the unique pro-p-Sylow subgroup of $\mathrm{Gal}(L/K)$(3.1.13.11). ⌟

Proof: Cf.[Neukirch P174]. □

Prop. (14.2.2.17). There is an exact sequence

$$1 \to R(L/K) \to I(L/K) \to \chi(L/K) \to 0$$

where $\chi_v(L/K) = \mathrm{Hom}(\Delta/\Gamma, \lambda^\times)$ and $\Delta = w(L^\times), \Gamma = v(K^\times)$. Moreover, in case L/K is a finite extension, this exact sequence splits. ⌟

Proof: For any $\sigma \in I_w$, define the map $\chi_\sigma : \Delta/\Gamma \to \lambda^*$ as follows: for any $\delta \in \Delta/\Gamma$, let $\delta = w(x)$ for some $x \in L^*$, let $\chi_\sigma(\overline{\delta}) = \frac{\sigma(x)}{x} \mod \mathfrak{P}_w$. This is independent of x chosen, because if $w(x) \equiv w(x') \mod \Gamma$, then $w(x) = w(ax)$ for some $a \in K^*$, thus $x = axu$ for some $u \in \mathcal{O}_w^*$. Now $\frac{\sigma(u)}{u} \equiv 1 \mod \mathfrak{P}$ as $\sigma \in I_w$, so $\frac{\sigma(x)}{x} = \frac{\sigma(x')}{x'} \in \lambda^*$. And the kernel of this map is R_w by definition.

The sequence is exact on the right by [Neukirch P175].**?** □

Higher Ramification Groups

Notation (14.2.2.18).

- Let L/K be a finite Galois extension of CDVRs.

⌟

Def. (14.2.2.19) [Higher Ramifications]. For $s \in \mathbb{R}_+$, define the **s-th ramification group** $G_s(L/K) = \{\sigma \in G | v_L(\sigma(x) - x) \geq s+1 \text{ for all } a \in \mathcal{O}_L\}$.

Then we have $G = G_{-1} \supset G_0 \supset G_1 \supset \ldots$. And G_0 is the inertia group. ⌟

Prop. (14.2.2.20). When K has finite residue field, G_1 is the ramification group R_w(14.4.1.16). In this case, we have

$$G_s(L/K) = \{\sigma \in G_0 | \frac{\sigma(\pi_L)}{\pi_L} \in U_L^s\}, \text{ for } s \geq 0.$$

So there are injective morphism $G_s/G_{s+1} \to U_L^s/U_L^{s+1} : \sigma \mapsto \sigma(\pi_L)/\pi_L$ for $s \geq 0$.(This is independent of π_L chosen because units are mapped mod U_L^{s+1}). ⌟

Proof: $G_1 = R_w$: one direction is trivial, for the other, we use Teichmüller representatives, then R_w preserves all them, and $\sigma(x) - x \equiv 0 \mod \mathfrak{P}^2$ is true for π, so it is true for all. □

Prop. (14.2.2.21). For local fields L/K, if σ is in the inertia group, then

$$v_L(\frac{\sigma(x)}{x} - 1) \geq v_L(\frac{\sigma(\pi_L)}{\pi_L} - 1) + \delta_{v_L(x),0}$$

for any $x \in \mathcal{O}_L$ and a uniformizer π_L. Equality holds when $v_L(x) = 1$. ⌟

Proof: if L has residue field $\mathbb{F}_q$, then any element of $\mathcal{L}$ can be written as $\sum \xi_n \pi_L^n$, where ξ_n are all $q-1$-th roots of unity. And because σ is inertia group, all $q-1$-th roots of unity are preserved, so $\sigma(\xi_n\pi_L^n) - \xi_n\pi_L^n = \xi_n\pi_L(\frac{\sigma(\pi_L)}{\pi_L} - 1)(\sigma(\pi_L)^{n-1} + \sigma(\pi_L)^{n-2}\pi_L + \ldots + \pi_L^{n-1})$ has valuation$\geq v(\frac{\sigma(\pi_L)}{\pi_L} - 1) + n$. Thus the result. □

In the sequel, we assume that the residue field extension is separable, as to use the proposition(14.2.2.2).

Lemma (14.2.2.22). We define $i_{L/K}(\sigma)=v_L(\sigma x-x)$, where x is the generator of $\mathcal{O}_L/\mathcal{O}_K$.

If $L/L'/K$ are Galois extensions that e is the ramification index of L/L'. Then

$$i_{L'/K}(\sigma')=\frac{1}{e}\sum_{\sigma|_{L'}=\sigma'} i_{L/K}(\sigma).$$

⌟

Proof: Cf.[Neukirch Algebraic Number Theory P178]. □

Def. (14.2.2.23) [Upper Numbering]. We define the **Herbrand function** $\varphi_{L/K}(u)=\int_0^u\frac{\mathrm{dx}}{(G_0:G_x)}$. It maps $\{x\geq 1\}$ to itself and is strictly increasing.

If $m\leq s<m+1$, then it is just $\varphi_{L/K}(s)=\frac{1}{g_0}(g_1+g_2+\ldots+g_m+(s-m)g_{m+1})$, where $g_i=|G_i|$. By a double counting, it is

$$\varphi_{L/K}(s)=\frac{1}{g_0}\sum_{\sigma\in G}\min\{i_{L/K}(\sigma),s+1\}-1.$$

The derivative of $\varphi_{L/K}$ is $\varphi'_{L/K}(s)=\dfrac{|G_s|}{g_0}$.

Let $\psi_{L/K}$ be the inverse function of We define $G^t=G_{\psi_{L/K}(t)}$, this is called the **upper numbering**.
⌟

Lemma (14.2.2.24). For $L/L'/K$ Galois extensions, one has $G_s(L/K)H/H=G_t(L'/K)$, where $t=\varphi_{L/L'}(s)$. Equivalently, $G_s/H_s=(G/H)_{\varphi_{L/L'}(s)}$. ⌟

Proof: For $\sigma'\in G(L'/K)$, we choose a inverse image $\sigma\in G(L/K)$ of maximal $i_{L/K}(\sigma)$, then $i_{L'/K}(\sigma')-1=\varphi_{L/L'}(i_{L/K}(\sigma)-1)$. To prove this, let $i_{L/K}(\sigma)=m$, then we see $i_{L/K}(\sigma\tau)=\min\{i_{L/K}(\tau),m\}$, so by(14.2.2.22), $i_{L'/K}(\sigma')=\frac{1}{e}\sum_{\tau\in H}\min\{i_{L/K}(\tau),m\}$. And $e=|H_0|$ by(14.2.2.14). So the assertion follows from(14.2.2.23).

Now σ' is in the image of G_s is equivalent to $i_{L/K}(\sigma)-1\geq s\iff\varphi_{L/L'}(i_{L/K}(\sigma)-1)\geq\varphi_{L/L'}(s)$, which by what proved is equivalent to $\sigma'\in G_t(L'/K)$. □

Cor. (14.2.2.25). For $L/L'/K$ Galois extensions, $\varphi_{L/K}=\varphi_{L'/K}\circ\varphi_{L/L'}$, hence similar formula holds for ψ. ⌟

Proof: By the proposition and multiplicity of ramification index e, we get

$$\frac{1}{e_{L/K}}|G_s|=\frac{1}{e_{L'/K}}|(G/H)_t|\frac{1}{e_{L/L'}}|H_s|.$$

where $t=\varphi_{L/L'}(s)$, which is equivalent to the derivative $\varphi'_{L/K}(s)=\varphi'_{L'/K}(t)\varphi'_{L/L'}(s)=(\varphi_{L'/K}\circ\varphi_{L/L'})'(s)$, and they are equal at 0, so the conclusion follows. □

Prop. (14.2.2.26) [Herbrand's Theorem]. For $L/L'/K$ Galois extensions, $G^t(L'/K)$ is the image of $G^t(L/K)$ under the quotient. ⌟

Proof: Let $r=\varphi_{L'/K}(t)$, by the above lemme and corollary,

$$G^tH/H=G_{\varphi_{L/K}(t)}H/H=G'_{\varphi_{L/L'}(\psi_{L/K}(t))}=G'_{\varphi_{L/L'}(\psi_{L/L'}(r))}=G_r(L'/K)=G^t(L'/K)$$

□

Prop. (14.2.2.27) [Hasse-Arf]. For an Abelian extension of CDVRs L/K that the residue field extension is separable, the jump in the upper numbering of higher ramification group G^v must happen at integers. (Note: The proof in the case where K is a local field is much easier by Lubin-Tate group, See(14.6.2.30)). ⌟

Proof: The theorem is just saying that if $G_s \neq G_{s+1}$ for s integer, then $\varphi_{L/K}(s)$ is an integer.

This follows follows from the following lemma, because if G is not totally ramified, then we can change it to the Galois field of G_0, this didn't change anything by the definition of(14.2.2.23), and the fact $\varphi(0) = 0$. And when $G^v \neq G^{v+}$, then we consider splitting G/G^{v+} into product of cyclic groups, thus there is one cyclic group H that the projection of G^v into H is not trivial. Now H is a Galois group of some L'/K, and Herbrand's theorem shows that $H^v \neq H^{v+}$, hence v is an integer by the following lemma. □

Lemma (14.2.2.28). For a cyclic totally ramified extension of CDVRs L/K s.t. the residue field extension is separable, if μ is the maximal integer that $G_\mu \neq 1$, then $\varphi_{L/K}(G_\mu)$ is an integer. ⌟

Proof: Cf.[Serre Local Fields P94]. □

Example (14.2.2.29). If $K_n = \mathbb{Q}_p(\mu_{p^n})$, then

$$\mathrm{Gal}_s(K_n/\mathbb{Q}_p) = \mathrm{Gal}(F_n/F_t) \quad \text{for } p^t - 1 \leq s < p^{t+1} - 2.$$

Thus $\mathrm{Gal}^i(K_n/\mathbb{Q}_p) = \mathrm{Gal}(K_n/K_i)$. ⌟

Proof: This is because $\zeta_{p^n} - 1$ is a uniformizer of K_n(14.2.3.23). □

3 Local Fields

Notation (14.2.3.1).

- Let $p \in$ `Prime` and $(K, \mathfrak{m}, \kappa) \in p$-`LField`(14.2.3.5).

⌟

Def. (14.2.3.2) [Local Fields]. A **local field** is a locally compact valued field. A local field is clearly complete. The category of local fields is denoted by `LField`. ⌟

Prop. (14.2.3.3) [Complete Valued Fields]. A complete Archimedean valued field must be $\mathbb{R}$ or $\mathbb{C}$, by(11.2.3.18).

Any complete non-Archimedean valued field is discretely valued, and has finite residue fields of characteristic $p \in \mathbf{P}$. Such a field is called a ***p*-adic local fields**. The category of p-adic local fields is denoted by p-`LField`. ⌟

Proof: Cf.[Sutherland, L9].**?** □

Remark (14.2.3.4). The valuation ring of a p-adic local field is a DVR, thus the theory of Dedekind domains7 applies to this case. ⌟

Prop. (14.2.3.5) [*p*-adic Local Fields]. p-adic local fields are precisely the finite extensions of the field $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$, called ***p*-adic number field** and ***p*-adic function field** respectively.

The category of p-adic number fields are denoted by p-`NField`, and the category of p-adic function fields are denoted by p-`FField`. ⌟

Proof: Cf.[Neukirch Algebraic Number Theory P135]. □

Group Structures

Prop. (14.2.3.6). For $m>0$, there is an isomorphism $(-)^m: U^n\cong U^{n+v(m)}$ when n is sufficiently large. ⌟

Proof: Let $m=u\pi^{v(m)}$. For surjectivity, we need to find x, that $1+a\pi^{n+v(m)}=-(1+x\pi^n)^m$. i.e.

$$-a+ux+\pi^{n-v(m)}f(x)=0.$$

This has a solution x by Hensel's lemma. □

Cor. (14.2.3.7). $(K^*)^m$ is an open subgroup of K^*, and $\bigcap_m(K^*)^m=1$. (Because if $a\in\bigcap_m(K^*)^m=1$, then a is a unit, thus $a\in\bigcap_m(U)^m=1$, thus $a\in U^n$ for every n thus $a=1$). ⌟

Prop. (14.2.3.8). $[K^\times:(K^\times)^m]=m\cdot|m|_{\mathfrak{p}}^{-1}\cdot|\mu_m(K)|$. ⌟

Proof: Use the multiplicative Herbrand quotient(4.8.7.7), $(K^*:(K^*)^m)=q_{0,m}(K^*)|\mu_m(K)|$. $q_{0,m}$ is additive, thus

$$q_{0,m}(K^*)=q_{0,m}(K/U)q_{0,m}(U/U^n)q_{0,m}(U^n).$$

$q_{0,m}(K/U)=m$, $q_{0,m}(U/U^n)=1$ as U/U^n is finite(4.8.7.9). It For $q_{0,m}(U^n)$, when n is large, it equals $(U^n:U^{n+v(m)})$ by(14.2.3.6), which is $|m|_{\mathfrak{p}}^{-1}$. □

Prop. (14.2.3.9)[*p*-adic Logarithm]. For a p-adic umber field K, there is a unique p**-adic logarithm** function $\log:K^*\to K$ that $\log(p)=0$, and for $x\in\mathfrak{p}$, it is defined to be

$$\log(1+x)=x-\frac{x^2}{2}+\frac{x^3}{3}-\ldots.$$

Moreover, for $n>\frac{e_K}{p-1}$, there is a map $\exp:\mathfrak{p}^n\to U^n$: which is an inverse to log on U^n, so $U^n\cong\mathfrak{p}^n$. ⌟

Proof: This follows from(9.5.4.8). □

Remark (14.2.3.10). In fact, this map can be extended to a function from $\mathbb{C}_p^*$ to $\mathbb{C}_p$. ⌟

Cor. (14.2.3.11). For a local field K, $\mathcal{O}_K^*$ thus also $K^\times$ are locally compact. ⌟

Proof: For n large, $U^n\cong\mathfrak{p}^n$ is compact. □

Prop. (14.2.3.12)[Multiplicative Group Structures]. For $K\in p$-`LField`,

- If char $K=0$, then $\mathcal{O}_K^*\cong\mathbb{Z}/(p-1)\oplus\mathbb{Z}/(p^a)\oplus\mathbb{Z}_p^d$, where $d=[K:\mathbb{Q}_p]$ and $a\in\mathbb{N}$.
- If char $K=p$, then $\mathcal{O}_K^*\cong\mathbb{Z}/(p-1)\oplus\mathbb{Z}_p^{\mathbb{N}}$.

⌟

Proof: Cf.[Neukirch P140]. □

Prop. (14.2.3.13)[Multiplicative Group Structures]. For $p\in\mathbf{P}$,

$$\mathbb{Q}_p^\times\cong\begin{cases}\mathbb{Z}\times\mathbb{Z}_p\times\mathbb{Z}/(p-1) & ,p\neq 2\\ \mathbb{Z}\times\mathbb{Z}_2\times\mathbb{Z}/(2) & ,p=2\end{cases}$$

⌟

Cor. (14.2.3.14). For $p \neq \ell \in \mathbf{P}$, $\mathbb{Q}_p \ncong \mathbb{Q}_\ell$. ⌟

Proof: Because $\mathbb{Q}_p^\times \ncong \mathbb{Q}_\ell^\times$: Firstly look at the torsion groups, then also look at $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \ncong \mathbb{Q}_\ell^\times/(\mathbb{Q}_\ell^\times)^2$. □

Prop. (14.2.3.15). Any automorphism of $\mathbb{R}$ or a p-adic number field is identity. ⌟

Proof: It suffices to show that an automorphism is continuous. For $\mathbb{R}$, this is because $a > 0 \iff a = b^2 \iff \sigma(a) = \sigma(b)^2 \iff \sigma(a) > 0$, and $\mathbb{Q}$ is dense in $\mathbb{R}$.

For a local field, we prove that $\sigma(\mathcal{O}_K^*) \subset \mathcal{O}_K^*$. $\mathcal{O}_K^*$ is characterized by the property that $\{n | y^n = x\}$ are infinite. This is because $x^p = a$ has a root for $a \in \mathcal{O}_K^*$ for p large prime, by Henselian lemma. □

Def. (14.2.3.16) [Norm Groups]. For any extension of local fields L/K, $\mathrm{Nm}_{L/K}$ is open, and $\mathcal{N}_{L/K} = \mathrm{Nm}_{L/K} L^\times \subset K^\times$ is called the **norm group** of L/K. ⌟

Extension Fields

Prop. (14.2.3.17). $[\mathbb{Q}_p^{\mathrm{ab,tame}} : \mathbb{Q}_p^{\mathrm{ab,ur}}] < \infty$. ⌟

Proof:

□

Prop. (14.2.3.18). The maximal unramified extension of $\mathbb{F}_p((t))$ is $T = \overline{\mathbb{F}}_p((t))$, and the maximal tamely unramified extension of $\mathbb{F}_p((t))$ is $T(\sqrt[m]{t} | m \geq 1, (m,p) = 1\})$. ⌟

Proof:

□

Prop. (14.2.3.19). Any finite quotient group of Gal_K is solvable. ⌟

Proof: This follows from(14.2.2.16)(14.2.2.15)(14.2.2.17) and(3.1.13.12) and(3.1.6.2). □

Def. (14.2.3.20) [Tame Characters]. There is an isomorphism

$$\widehat{t} : I_K/R_K \cong \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{ur}}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$$

and the projection to $\mathbb{Z}_\ell$ is called the ℓ-adic (additive)**tame character** of I_K.

Equivalently, if $\ell \in \mathbf{P}\backslash\{p\}$, for any compatible system of ℓ^∞-th roots $\{\varpi_{\ell^n}\}$ of ϖ in $\overline{K}$, it is the character t_ℓ of Gal_K that $\sigma(\varpi_{\ell^n}) = \varpi_{\ell^n}^{t_\ell(\sigma)}$. ⌟

Ramifications of Cyclotomic Fields

Prop. (14.2.3.21) [Unramified cases]. Let $\#\kappa = q$ and $n \in \mathbb{Z}_+ \setminus (p)$, consider $L = K(\zeta_n)$. Then L/K is unramified of inertia degree f where f is the minimal number that $q^f \equiv 1 \mod n$. And $\mathcal{O}_L = \mathcal{O}_K[\zeta_n]$. ⌟

Proof: ζ_n is a root of $\Psi_n(X) | X^n - 1$, which is separable over κ, so Ψ_n and $\overline{\Psi_n}$ are both irreducible of the same degree by Hensel's lemma. So it is unramified, and λ is the minimal extension of $\mathbb{F}_q$ that contains the n-th roots and are generated by it, thus the result by the theory of finite fields.

For the last assertion, notice it is unramified so $\mathcal{O}_L = \mathcal{O}_K[\zeta_n] + p\mathcal{O}_L$ hence the result follows from Nakayama's lemma. □

Cor. (14.2.3.22). The maximal unramified extension of K is generated by adjoining all n-th roots where $(n,p)=1$. This is because there is an inclusion relation and their residue field $\overline{\mathbb{F}}_p$ is already generated by roots of unity. ⌟

Prop. (14.2.3.23)[Totally Ramified cases]. Consider $\mathbb{Q}_p$(other local fields behave different), we have the $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ is totally ramified of degree $\varphi(p^n)$ the Galois group is $(\mathbb{Z}/(p^n))^*$. The ring of valuation of $\mathbb{Q}_p(\zeta_{p^n})$ is $\mathbb{Z}_p[\zeta_{p^n}]$ and $1-\zeta_{p^n}$ is a uniformizer. ⌟

Proof: Notice

$$\Psi_{p^n}(X)=\frac{X^{p^n}-1}{X^{p^{n-1}}-1}\equiv(X-1)^{p^{n-1}(p-1)}(\text{mod } p)$$

and $\Phi(1)=p$. So $\mathrm{Nm}(1-\zeta_{p^n})=\prod(1-\sigma(\zeta_{p^n}))=\Phi(1)=p$. Thus $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ is totally ramified of degree $p^{n-1}(p-1)$ and $1-\zeta_{p^n}$ is a uniformizer. The ring of integer is generated by a uniformizer by(11.2.3.20) as the extension is totally ramified. □

Prop. (14.2.3.24)[Infinite Cyclotomic Field]. Let $K_n=K(\zeta_{p^n})$ and $K_\infty=\cup K_n$ and $F=\mathbb{Q}_p$. Let χ be the cyclotomic character, then $\chi(\mathrm{Gal}_K)$ is an open subgroup of $\mathbb{Z}_p^*$, thus contains a U_n for some n. Thus there is an isomorphism of groups: $\chi^{-1}(U_n)\cap\mathrm{Gal}_K/\chi^{-1}(U_n+1)\cap\mathrm{Gal}_K\cong U_n/U_{n+1}$ which has order p, for n large.

So K_{n+1}/K_n is totally ramified of degree p, because $K_n=K\cdot F_n$, and its value group extension is of degree p, too.

And $|\{K_n:F_n\}|$ is decreasing and eventually equals to $[K_\infty:F_\infty]$. This is because its order equals $\chi^{-1}(U_n)/\chi^{-1}(U_n)\cap\mathrm{Gal}_K\cong\chi^{-1}(U_n)\mathrm{Gal}_K/\mathrm{Gal}_K$, which is eventually $\ker(\chi)\mathrm{Gal}_K/\mathrm{Gal}_K$, because $U_n\subset\chi(\mathrm{Gal}_K)$. ⌟

Cor. (14.2.3.25). For n large, if x_i is a set of basis of $\mathcal{O}_{K_n}$ over $\mathcal{O}_{F_n}$, then they form a basis of K_N over F_N for all $N\geq n$. This is because it generate K_N over F_N and $[K_N:F_N]=[K_n:F_n]$. ⌟

Prop. (14.2.3.26). $p^n v_p(\mathfrak{D}_{K_n/F_n})$ is bounded and eventually constant. In particular $v_p(\mathfrak{D}_{K_n/F_n})$ converges to 0. ⌟

Proof: Cf.[Galois representation Berger P20]. □

Cor. (14.2.3.27). If L/K is a finite extension, then $\mathrm{tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty})=\mathfrak{m}_{K_\infty}$. ⌟

Proof: By(14.2.2.3) and the fact $\mathrm{Gal}(L_\infty/K_\infty)\cong\mathrm{Gal}(L_n/K_n)$ for n large by(14.2.3.24), we have $\mathrm{tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_n})=\mathfrak{m}_{K_n}^{c_n}$, where $c_n=\lfloor v_{K_n}(\mathfrak{m}_{L_n}\mathcal{D}_{L_n/K_n})\rfloor$. By the above proposition, c_n is bounded by a c. But if $x\in\mathfrak{m}_{K_\infty}$, $x\in\mathfrak{m}_{K_n}^c$ for n large, so $x\in\mathrm{tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty})$. □

Lemma (14.2.3.28). For any $\delta>0$, when n is large, if $x\in\mathcal{O}_{K_{n+1}}$ and $g\in G(K_{n+1}/K_n)$, $v_p(g(x)-x)\geq\frac{1}{p-1}-\delta$. In particular, $v(N_{K_{n+1}/K_n}(x)-x^p)\geq\frac{1}{p-1}-\delta$. ⌟

Proof: Choose a basis e_i of $\mathcal{O}_{K_n}/\mathcal{O}_{F_n}$, then e_i^* is a basis for $\mathcal{D}_{K_n/F_n}$, and if $x_i=\mathrm{tr}_{K_{n+1}/F_{n+1}}(xe_i)$, then $x_i\in\mathcal{O}_{F_{n+1}}$ and $x=\sum x_ie_i$, by(14.2.3.25), and we have by(14.2.2.29), $v(g(x_i)-x_i)\geq 1/(p-1)$, so when n is large, by(14.2.3.26), $v(x_i)\geq-\delta$, so the require is satisfied. □

Prop. (14.2.3.29). if $\delta>0$ and I is the ideal of elements of valuation$\geq 1/(p-1)-\delta$, then for n large, there is a map $x\mapsto x^p:\mathcal{O}_{K_{n+1}}/I\cap\mathcal{O}_{K_{n+1}}\to\mathcal{O}_{K_n}/I\cap\mathcal{O}_{K_n}$, and it is surjective. ⌟

Proof: For n large, choose a uniformizer π_{n+1} of K_{n+1}, then $\pi_n=N_{K_{n+1}/K_n}(\pi_{n+1})$ is the uniformizer of K_n because it is totally ramified(14.2.3.24), so any element $x\in\mathcal{O}_{K_{n+1}}$ can be written as $\sum\pi_{n+1}^i[x_i]$, where $x_i\in k_{K_{n+1}}=k_{K_\infty}$. Then $x^p\equiv\sum\pi_{n+1}^{pi}[x_i]^p\equiv\sum\pi_n^i[x_i^p]\mod I$ by the above proposition. And the surjection is verbatim. □

Def. (14.2.3.30) [Tate's Normalized Trace]. The function $R_n(x) = p^{-k}\operatorname{tr}_{F_{n+k}/F_n}(x)$ is compatible with k and defines a F_n-linear projection from F_∞ to F_n, and it commutes with G_F action, called the **Tate's normalized trace**.

From(14.2.3.31) it's easily verified that $R_n(\mathcal{O}_{F_{n+k}}) \subset \mathcal{O}_{F_n}$, thus $R_n(\pi_n^j\mathcal{O}_{F_{n+k}}) \subset \pi_n^j\mathcal{O}_{F_n}$. So we have $v(R_n(x)) > v(x) - v(\pi_n)$. So R_n extends by continuity to a map $R_n : \widehat{F}_\infty \to F_n$. If $x \in F_\infty$, then $R_n(x) = x$ for n large, thus $R_n(x) \to x$ for any $x \in \widehat{F}_\infty$.

Now for a finite extension $K/\mathbb{Q}_p$, for n large, if e_i is a set of basis of $\mathcal{O}_{K_n}/\mathcal{O}_{F_n}$, then for any $x \in \mathcal{O}_{K_{n+k}}$, $x = \sum x_i e_i^*$, where $x_i = \operatorname{tr}_{K_{n+k}/F_{n+k}}(xe_i) \in \mathcal{O}_{F_{n+k}}$, as in the proof of(14.2.3.28). So we can define $R_n(x) = \sum R_n(x_i)e_i^*$. Notice this is defined only for n large, and is independent of e_i chosen, and by the following lemma, it is continuous and extends to a K_n-linear projection $R_n : \widehat{K_\infty}$ to K_n. ⌟

Lemma (14.2.3.31). Let $k \geq 0$ and $n \geq 1$, then $R_n(\zeta_{p^{n+k}}^j) = 1$ for $j = 0$ and vanishes otherwise. ⌟

Proof: This is clear from the fact $\operatorname{tr}_{F_{n+k}/F_n}(\zeta_{p^{n+k}}^j) = \zeta_{p^{n+k}}^j \sum_{\eta^{p^k}=1} \eta^j$. □

Lemma (14.2.3.32). for any $\delta > 0$, when n is large, $v(R_n(x)) \geq v(x) - \delta$. ⌟

Proof: We have $v(x_i) > v(x) - v(\pi_{n+k})$ by F_{n+k}-linearity, and $v(R_n(x_i)) > v(x_i) - v(\pi_n)$ as in(14.2.3.30), and $v(e_i^*) \geq -\delta$ when n is large, by(14.2.3.26). Thus the result. □

Prop. (14.2.3.33) [Refinement of Hilbert's Theorem90]. There is a decomposition of $\widehat{K_\infty} = K_n \oplus X_n$, where $X_n = \ker R_n$. If $\delta > 0$, then for n large, $\alpha \in \mathbb{Z}_p^*$ and γ_n that $\chi(\gamma_n)$ is a topological generator of Γ_{F_n}, $1 - \alpha\gamma_n : X_n \to X_n$ (because γ_n commutes with R_n) is invertible and

$$v_p((1-\alpha\gamma_n)^{-1}x) \geq v_p(x) - 1/(p-1) - \delta,$$

unless $\alpha = -1$ and $p = 2$, in which case it is only invertible on X_{n+1}. ⌟

Proof: As usual, x_i is a basis of $\mathcal{O}_{K_n/F_n}$, then $x = \sum x_i e_i^*$, $x_i = \operatorname{tr}_{K_\infty/F_\infty}(xe_i) \in \widehat{F}_\infty$, and $R_n(x) = 0$. Then $(1-\alpha\gamma_n)$ acts on x_i, so it reduce to the case $K = \mathbb{Q}_p$.

Injectivity: If $\alpha = 1$, this is Ax-Sen-Tate theorem. In other situations, $(1-\alpha\gamma_n)(R_{n+k}(x)) = 0$ for all $k \geq 0$, so $R_{n+k}(x) = \alpha^{p^k}\gamma_n^{p^k}(R_{n+k}(x)) = \alpha^{p^k}R_{n+k}(x)$, so $R_{n+k}(x) = 0$, hence $x = 0$ by continuity.

Surjectivity: Let $F_{n+k}^* = \oplus_{j=1,p\nmid j}^{p^k-1} F_n\zeta_{p^{n+k}}^j$, then $F_{n+k} = F_n^* \oplus F_{n+1}^* \oplus \ldots \oplus F_{n+k}^*$, and $F_{n+k} \cap X_n = F_{n+1}^* \oplus \ldots \oplus F_{n+k}^*$. Now if $x = \sum_{j=1,p\nmid j}^{p^k-1} x_j\zeta_{p^{n+k}}^j$ with $x_j \in \mathcal{O}_{F_n}$, then

$$x = (1-\alpha^{p^{k-1}}\gamma_n^{p^{k-1}})\sum_{j=1,p\nmid j}^{p^{k-1}} x_j \frac{\zeta_{p^{n+k}}^j}{1-\alpha^{p^{k-1}}\zeta_p^j}.$$

Now $v_p(1-\alpha^{p^{k-1}}\zeta_p^j) \leq 1/(p-1)$, and

$$(1-\alpha\gamma_n)^{-1} = \frac{1-\alpha^{p^{k-1}}\gamma_n^{p^{k-1}}}{1-\alpha\gamma_n}(1-\alpha^{p^{k-1}}\gamma_n^{p^{k-1}})^{-1},$$

so $\alpha_n : 1-\alpha\gamma_n : F_{n+k}^* \to F_{n+k}^*$ is invertible and

$$v_p((1-\alpha\gamma_n)^{-1}x) \geq v_p(x) - 1/(p-1) - v_p(\zeta_{p^n} - 1)$$

holds. And the assertion holds by uniform continuity. □

Miscellaneous

Def. (14.2.3.34) [Lattices]. If $K \in \texttt{LField}$ and $V \in \mathcal{V}\text{ect}^{\text{fd}}/K$, then a **lattice in** V is

- a compact open $\mathcal{O}_K$-submodule of V if K is non-Archimedean. Equivalently, it is a f.g. $\mathcal{O}_K$-submodule that contains a K-basis of V.
- a discrete subgroup Λ of V s.t. V/Λ is compact if K is Archimedean.

⌟

Prop. (14.2.3.35). Let V be a f.d. vector space over a non-Archimedean local field K and Λ be an $\mathcal{O}_K$-submodule of V, then Λ is a lattice in V iff it is a finite $\mathcal{O}_K$-module and generate V as a K-vector space. ⌟

Proof: If Λ is an $\mathcal{O}_K$-submodule, then it clearly generates V as a K-vector space, and the f.g. $\mathcal{O}_K$-submodules of Λ is a cover of Λ, which has a finite subcover as Λ is compact open, thus Λ is f.g. over $\mathcal{O}_K$.

Conversely, if Λ is a f.g. $\mathcal{O}_K$-submodule that generate V as a K-vector space, then it is a quotient of $\mathcal{O}_K^n$ for some n, thus compact. And let S be a K-basis of V contained in Λ, then $\mathcal{O}_K S$ is an open nbhd of $0 \subset \Lambda$, which means it is open. □

Prop. (14.2.3.36). Let Λ be a subgroup of a f.d. real or complex vector space V, then the following are equivalent:

- Λ is a lattice in V.
- Λ is discrete and contains an $\mathbb{R}$-basis of V.
- Λ has a $\mathbb{Z}$-basis that is also an $\mathbb{R}$-basis of V.

⌟

Remark (14.2.3.37). WARNING: This is not equivalent to Λ is a f.g. $\mathbb{Z}$-module and generated V as an $\mathbb{R}$-vector space: Consider $\mathbb{Z}\{1, \alpha\} \subset \mathbb{R}$. ⌟

Proof: $1 \to 2$: Let W be a complementary subspace of $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \subset V$, then $W \cong \overline{W}$ is closed thus compact in V/Λ, which implies $W = 0$.

$2 \to 3$: We may assume $V = \mathbb{R}^n$ and Λ contains the canonical basis $e_1, \ldots, e_n$, then Λ is generated by $S = \{\lambda \in \Lambda | \max_i |\lambda_i| \leq 1\}$. Because Λ is discrete thus closed in V, S is finite. Thus Λ is a f.g. $\mathbb{Z}$-module, and has no torsion, thus a free Abelian group. But $\Lambda/\mathbb{Z}\{e_i\}$ is finite, thus $\Lambda \cong \mathbb{Z}^n$. Hence a basis of Λ must also be a basis of V.

$3 \to 1$ is clear. □

Def. (14.2.3.38) [Dual Lattice]. If $K \in$ p-$\texttt{Field}$ and V is a f.d. vector space over K, B is a non-degenerate bilinear form on V and ψ is a non-trivial character of K, then for any lattice $L \subset V$, the **dual lattice** $L' = \{u \in V | \psi(2(B(u, v))) = 1, \forall v \in L\}$ is also a lattice in V. ⌟

Proof: It is an open group by no-small-subgroup argument, as ψ, B are continuous. it is compact because take any basis $\{v_1, \ldots, v_n\}$ of V that $v_i \in L$, $\{u \in V | \psi(2(B(u, v_i))) = 1, \forall i\}$ is compact. □

4 Ultranormed Banach Spaces

Notation (14.2.4.1).

- Let $(K, v, \mathcal{O}_K, \mathfrak{p}_v, \varpi, k)$ be a complete non-Archimedean valued field(of rank 1), $K^0 = \mathfrak{p}_v$, and $\varpi \in K^\times, |\varpi| < 1$ a uniformizer. If $\mathcal{O}_K$ is DVR, assume $(\varpi) = \mathfrak{p}_v$.

⌟

Ultranormed K-modules

Prop. (14.2.4.2). Any normed K-module is weakly-Cartesian. ⌟

Proof: Cf.[Non-Archimedean Analysis P92]. □

Cor. (14.2.4.3). Any two valuation on a finite K-vector space are equivalent. ⌟

Proof: Cf.[Non-Archimedean Analysis P93]. □

Prop. (14.2.4.4). If V is a normed $\mathbb{Q}_p$ vector space and $V_0 = \{x \in V||x| \le 1\}$, then $V^\wedge \cong (V_0)_p^\wedge[p^{-1}]$. ⌟

Ultranormed Banach Spaces

Def. (14.2.4.5) [Ultranormed Banach Spaces]. In the non-Archimedean case, an **ultranormed Banach algebra** is defined as in(11.7.4.2), but additionally $|a+b| \le \max\{|a|,|b|\}$. ⌟

Def. (14.2.4.6) [Uniform Banach Space]. For a complete non-Archimedean field K and a Banach algebra R, define R^0 to be the ring of **power bounded elements**. Then it is a subring, and it is open, as it contains the closed ball $\overline{\mathbb{D}(0,1)}$.

Recall R is called uniform if R^0 is itself bounded in R(14.2.1.6). Notice a uniform Banach space must be reduced, because a nilpotent element is clearly power bounded, and any scalar multiple of it is nilpotent. ⌟

Lemma (14.2.4.7). Fix a uniformizer t in a non-Archimedean complete field K, if $|K^*|$ is discrete, then if A is a t-adically complete and t-torsion-free K^0-algebra, let $R = A[t^{-1}]$, then the norm

$$|f| = \inf\{|t|^n | f \in t^n A\},$$

then this makes R into a K-Banach space that the t-adic topology of A is the same as the metric topology of A, so $A \subset R_{\le 1} \subset R^0$.

Notice if $|K^*|$ is not discrete but there is a pseudo-uniformizer t that has a compatible system of p^n-th roots, if A is a t-adically complete and t-torsion-free K^0-algebra, let $R = A[t^{-1}]$, then the norm

$$|f| = \inf\{|t|^{\frac{n}{p^k}} | f \in t^{\frac{n}{p^k}} A\},$$

then this makes R into a K-Banach space that the t-adic topology of A is the same as the metric topology of A, so $A \subset R_{\le 1} \subset R^0$, and in this case $R^0 = A_* = \mathrm{Hom}((t^{\frac{1}{p^\infty}}), A)$(5.7.2.2). ⌟

Prop. (14.2.4.8) [Uniform K-Banach Space and K^0-Algebra]. Fix a pseudo uniformizer t in a non-Archimedean complete field K, the following category are equivalent:

- The category $\mathcal{C}$ of uniform Banach K-algebras R.
- The category $\mathcal{D}_{tic}$ of t-adically complete and t-torsionfree K^0-algebras A with A totally integrally closed(5.2.1.1) in $A[t^{-1}]$.

⌟

Proof: The functor $F : \mathcal{C} \to \mathcal{D}_{tic}$: if R is uniform Banach space, then $F(R) = R^0$: R^0 is open subring by(14.2.4.6), and $R^0 \in B(0,r]$ for some $r > 0$ by uniformity. As R is K-Banach, $\cap t^n B(0,r] = 0$, so R^0 is t-adically separated, and also it is complete. If $f^{\mathbb{N}} \in t^{-k} R^0 \subset t^{-k} B(0,r]$, then clearly f is power bounded thus $f \in R^0$, so R^0 is totally integrally closed in R. $R \to R^0$ is preserved by continuous mappings, so F is truly a functor.

Conversely, lemma above(14.2.4.7) shows $R = A[t^{-1}]$ is a K-Banach algebra, this is a functor $G : \mathcal{D}_{tic} \to \mathcal{C}$, and $A \subset R^0$. We show $A = R^0$, as this is equivalent to $FG \cong \mathrm{id}$: as the t-adic topology and metric topology are the same(14.2.4.7), if $t^c f^{\mathbb{N}} \subset A$ for some c, thus f is totally integral over A, thus $f \in A$ by tic.

Finally, we need to show $GF \cong \mathrm{id}$, which in fact that the given Banach algebra norm on R is equivalent to the norm $|\cdot|'$ given in(14.2.4.7) w.r.t R^0. $R'_{<1} \subset R^0 \subset R_{\leq c}$ by uniformity, and conversely, $R_{\leq 1} \subset R^0 \subset R'_{\leq 1}$, thus this two norms are equivalent. □

Prop. (14.2.4.9). Let $\varphi : A \to B$ be a k-homomorphism between k-Banach algebras that there is a family $\mathfrak{B}$ of ideals of B that for each $b \in \mathfrak{B}$:

- B is closed and $\varphi^{-1}(b)$ is closed in A.
- $\dim_k B/b < \infty$.
- $\cap_{b\in\mathfrak{B}} b = (0)$.

Then φ is continuous. ⌟

Proof: Consider the map $A/\varphi^{-1}(b) \to B/b$ with the residue norms, Cf.[non-Archimedean analysis P167]. □

Cor. (14.2.4.10). Let $\varphi : A \to B$ be a k-homomorphism between Noetherian k-Banach algebras that there is a family $\mathfrak{B}$ of ideals of B that for each $b \in \mathfrak{B}$, $\dim_k B/b < \infty$ and $\cap_{b\in\mathfrak{B}} b = (0)$, then φ is continuous. (Because the closedness condition is automatic by(14.2.4.13)). ⌟

Cor. (14.2.4.11). All complete k-algebra norms on a Noetherian k-algebra B satisfying the condition of(14.2.4.10) are equivalent. ⌟

Modules over K-Banach Spaces

Prop. (14.2.4.12). If M is a normed module over a k-Banach algebra A, if the completion of M is a finite A-module, then M is complete. ⌟

Proof: There are morphism $\pi : A^n \to \widehat{M}$ that are surjective continuous, so by open mapping theorem(11.7.2.5), this map is open, so $\sum \check{A}x_i = \pi(A^n)$ is a nbhd of 0 in $\widehat{M}$, because $\check{A}$ is open(14.2.1.9) and then $\widehat{M} = M + \sum \check{A}x_i$, because M is dense in $\check{M}$, then we are done by(14.2.1.10). □

Cor. (14.2.4.13) [Noetherian and Submodule Closed]. For a complete normed module over a k-Banach algebra A, M is Noetherian iff all submodules of M are closed. In particular, A is Noetherian iff all ideals of A are closed. ⌟

Proof: If M is Noetherian, then the completion of any submodule is finite over A, so it is complete hence closed by(14.2.4.12). Conversely, if any ideal of M is closed, then for a chain of ideals of $M : \cup M_i = M'$, M' is complete hence Baire space by(4.4.9.2), so some M_i must contain a nbhd of M', because it is an ideal, but then $M_i = M'$. □

5 p-adic Analysis

Main References are [p-adic Analysis Robert].

Notation (14.2.5.1).

- Let K be a p-adic field(14.2.5.2).

⌟

p-adic Fields

Def. (14.2.5.2) [p-adic Fields]. For $p \in \mathbf{P}$, a **p-adic field** is a CDVR $(K, v, \mathcal{O}_K, \mathfrak{p}_v, \varpi_K, \kappa)$ s.t. $\operatorname{char} K = 0, \operatorname{char} \kappa = p, \kappa = \kappa^{\text{perf}}$. A p-adic local field is a p-adic field(14.2.5.2). ⌟

Prop. (14.2.5.3). For $b \in \mathbb{Z}_p$, we can define a power series in $\mathbb{Z}_p[[T]]$ as the limit of $(1+a)^{b_n}$ for $b_n \to b$ in $\mathbb{Z}_p$. So for $a \in \mathbb{C}_p$ with $v(a) > 0$, there can be defined an element $(1+a)^b \in \mathbb{C}_p$, and we have $(1+a)^b = \sum C_b^k a^k$. ⌟

Def. (14.2.5.4) [Topological Completion]. If $p \in \mathbf{P}$ and K is a p-adic field, then we can define $\mathbb{C}_K = \widehat{\overline{K}}$, which is an alg.closed complete valued field, by(14.2.1.33)(14.2.1.30) and(14.2.1.24). Also denote $\mathbb{C}_p = \mathbb{C}_{\mathbb{Q}_p}$. ⌟

Lemma (14.2.5.5). If K a p-adic field and $P(X) \in \overline{K}[X]$ is a monic polynomial of degree n, and all of its roots satisfied $v_p(\alpha) \geq c$ for some constant c. Let $q = p^k$ if $n = p^k d, d \neq 1$ or $n = p^{k+1}$.

Then the derivative $P^{(q)}(X)$ has a root β with $v_p(\beta) \geq c$ or in case $n = p^{k+1}$, $v_p(\beta) \geq c - \frac{1}{p^k(p-1)}$. ⌟

Proof: Let $P = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, then $v_p(a_i) \geq (n-i)c$. And

$$1/q! \cdot P^{(q)}(X) = \sum_{i=0}^{n-1} C_{n-i}^q a_{n-i} X^{-i-q}.$$

So at lest one root β satisfies

$$v_p(\beta) \geq \frac{1}{n-q}((n-q)c - v_p(C_n^q)) = c - \frac{1}{p^k(p-1)}.$$

□

Lemma (14.2.5.6). If K is a p-adic field and $\alpha \in \overline{K}$, let $\Delta_K(\alpha) = \inf_{g \in \operatorname{Gal}_K} v_p(g(\alpha) - \alpha)$, then there exists a $\delta \in K$ that $v_p(\alpha - \delta) \geq \Delta_K(\alpha) - p/(p-1)^2$. ⌟

Proof: We strengthen the assertion and use induction on $n = [K(\alpha) : K]$ to prove that there is a δ that $v_p(\alpha - \delta) \geq \Delta_K(\alpha) - \sum_{k=0}^m \frac{1}{p^k(p-1)}$, where p^{m+1} is the largest power of p that $\leq n$.

$n = 1$ is sure, let the minipoly of α over K be $P(X)$. By lemma(14.2.5.5), there is a root β of $P^{(q)}$ that $v_p(\beta - \alpha) \geq v_p(\alpha)$ or minus a factor when $n = p^{k+1}$. Then for any σ, $v_p(\sigma(\beta) - \beta) \geq v_p(\sigma(\alpha) - \alpha)$ or minus a factor. Then $\Delta(\beta) \geq \Delta(\alpha)$ or minus a factor. Now $[K(\beta) : K] < [K(\alpha) : K] = n$, so we can use induction hypothesis to get the result. □

Remark (14.2.5.7). The constant $p/(p-1)^2$ can be replaced by $1/(p-1)$, and it is optimal: this is a theorem of Le Borgne in[Bor10]. ⌟

Prop. (14.2.5.8) [Ax-Sen-Tate]. If F is a p-adic field and if $K \subset \overline{F}$, then $\widehat{\overline{F}}^{\operatorname{Gal}_K} = \widehat{K}$. Thus $\widehat{L}^{\operatorname{Gal}(L/K)} = \widehat{K}$ for any alg.ext L/K. ⌟

Proof: Any $\alpha \in \widehat{\overline{F}}$ can be written as $\sum \alpha_n$ with $\alpha_n \in \overline{F}$. Then $\Delta_K(\alpha_n) \to \infty$, and α_n can be approximated by $\delta_n \in K$ by lemma(14.2.5.6), thus $\alpha \in \widehat{K}$. □

Power Series

Cor. (14.2.5.9) [Convergence of Power Series]. Let $(R, \mathfrak{m})$ be a CDVR of characteristic0 of residue characteristic p, then

- If $f(T) = \sum_{n\geq 1}^{\infty} \frac{a_n}{n} T^n \in (R \otimes \mathbb{Q})[[T]]$ with $a_i \in R$, then $f(x)$ converges in R for $x \in \mathfrak{m}$.
- If $g(T) = \sum_{n\geq 1}^{\infty} \frac{b_n}{n!} T^n \in (R \otimes \mathbb{Q})[[T]]$ with $b_i \in R$, then $f(x)$ converges in R for $v(x) > v(p)/(p-1)$.

⌟

Proof: 1: $v(a_n x^n/n) \geq nv(x) - v(n) \geq nv(x) - \log_p(n)v(p)$ converges to ∞ for $n \to \infty$ when $v(x) > 0$.

2: $v(b_n x^n/n!) \geq nv(x) - v(n!) \geq nv(x) - (n-1)v(p)/(p-1)$(2.6.3.28) converges to ∞ for $n \to \infty$ when $v(x) > v(p)/(p-1)$ □

Prop. (14.2.5.10). Let $f, g \in \mathcal{O}_K[[T]]$ and assume $f = a_0 + a_1 T + \ldots$ where $a_i \in \mathfrak{m}_K$ for $0 \leq i \leq n-1$, and $a_n \in \mathcal{O}_K^*$, then we can uniquely write

$$g = qf + r$$

where $q \in \mathcal{O}_K[[T]]$ and $r \in \mathcal{O}_K[T]$ is a polynomial of degree$\leq n-1$. ⌟

Proof: Cf.[Mazur Control Theorem, P4]. □

Def. (14.2.5.11) [Distinguished Polynomials]. $P(T) \in \mathcal{O}_K[T]$ is called a **distinguished polynomial** if $P(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_0$, where $a_i \in \mathfrak{m}_K$ for $0 \leq i \leq n-1$. ⌟

Prop. (14.2.5.12) [p-adic Weierstrass Preparation]. Every power series $0 \neq f(T) \in \mathcal{O}_K[[T]]$ can be written uniquely as $f(T) = \varpi_K^{\mu} P(T)U(T)$, where $\mu \in \mathbb{N}$, $P(T)$ is a distinguished polynomial, and $U(T)$ is a unit in $\mathcal{O}_K[[T]]$. ⌟

Proof: Cf.[Mazur Control Theorem, P5]. □

Cor. (14.2.5.13). If $0 \neq f(T) \in \mathcal{O}_K[[T]]$, there are only f.m. $x \in \mathcal{O}_{\mathbb{C}_K}$ with $f(x) = 0$. ⌟

Cor. (14.2.5.14). If $P(T) \in \mathcal{O}_K[T]$ is a distinguished polynomial, and $g(T) \in \mathcal{O}_K[T]$. Suppose $g(T)/P(T) \in \mathcal{O}_K[[T]]$, then $g(T)/P(T) \in \mathcal{O}_K[T]$. ⌟

Proof: Let $g(T) = f(T)P(T) \in \mathcal{O}_K[[T]]$. Suppose $x \in \mathcal{C}_K$ is a root of $P(T)$, then $|x| < 1$, thus $f(x)$ converges, and $g(x) = 0$. Then we can divide both $g(T)$ and $P(T)$ by $(T-x)$, and by induction(and change K by a larger field), we can get $P(T)$ divides $g(T)$ as polynomials. □

Prop. (14.2.5.15). $\mathcal{O}_K[[T]]$ is a UFD. ⌟

Proof: it follows from p-adic Weierstrass preparation theorem(14.2.5.12) that each element can be written as products of π_K and irreducible distinguished polynomials. And irreducible distinguished polynomials are all primes: if $P(T)$ is irreducible distinguished and $a, b \in \mathcal{O}_K[[T]]$ s.t. $P(T)|ab$, then we can use(14.2.5.10) to assume a, b are polynomials, and then by(14.2.5.14), $P_n(T)|ab$ as polynomials. Then $P(T)|a$ or $P(T)|b$ because $P(T)$ is irreducible and $\mathcal{O}_K[T]$ is a UFD(3.2.3.8). Then $\mathcal{O}_K[[T]]$ is a UFD, by(3.2.3.6). □

Cor. (14.2.5.16). If $f \in \mathcal{O}_K[[T]]$ is not invertible, then $\mathcal{O}_K[[T]]/(f)$ is infinite. ⌟

Lemma (14.2.5.17). Let $f,g\in\mathcal{O}_K[[T]]$ be relatively prime(3.2.3.4), then the ideal (f,g) is of finite index in $\mathcal{O}_K[[T]]$. ⌟

Proof: Cf.[Mazur Control Theorem, P8]. □

Prop. (14.2.5.18). The prime ideals of $\mathcal{O}_K[[T]]$ are $0,(\varpi_K,T),(\varpi_K)$, and the ideal $(P(T))$ where $P(T)$ is distinguished and irreducible. And the ideal (p,T) is the unique maximal ideal. ⌟

Proof: The above ideals are all primes by(14.2.5.15). And if $\mathfrak{p}$ is a non-zero prime, suppose f is a non-zero polynomial in $\mathfrak{p}$ of minimal degree, which exists by p-adic Weierstrass preparation theorem(14.2.5.12). Then because $\mathfrak{p}$ is a prime ideal, by Weierstrass preparation, we can assume that $f=p$ or f is a distinguished irreducible polynomial. Suppose $(f)\neq\mathfrak{p}$, then there exists $g\in\mathfrak{p}\setminus(f)$. Then f,g are relatively prime, then $\mathcal{O}_K[[T]]/(f,g)$ is finite(14.2.5.17). Thus $\mathfrak{p}$ is also of finite index in $\mathcal{O}_K[[T]]$. Then $p^n\in\mathfrak{p}$ for some n, and by primality, $p\in\mathfrak{p}$. And there are two T^i,T^j that are equal in $\mathcal{O}_K[[T]]/\mathfrak{p}$, so $(1-T^{j-i})T^i\in\mathfrak{p}$. But $(1-T^{j-i})$ is invertible, so $T\in\mathfrak{p}$. Then $(p,T)\subset\mathfrak{p}$, and $\mathfrak{p}=(p,T)$.

For the last assertion, notice if $P(T)$ is distinguished, then $P(T)\in(p,T)$. □

Laurent Series

Notation (14.2.5.19).

- Fix a p-adic field K.
- Denote by $\mathcal{L}_K$ the set of (possibly infinite)Laurent series with coefficients in K.

⌟

Def. (14.2.5.20) [Convergences]. For $f=\sum_{n\in\mathbb{Z}}a_nT^n\in\mathcal{L}_K$ and $r\in\mathbb{R}$, f is called convergent on the radius r if for any $a\in\mathbb{C}_K$ with $v_p(a)=r$, $f(a)$ converge. And f is said to converge on ∞(resp. $-\infty$) if $a_n=0$ for n sufficiently large(resp. sufficiently small). Denote $\mathrm{Conv}(f)\subset[-\infty,\infty]$ to be the set of radius that f is convergent on. Then $\mathrm{Conv}(f)$ is an interval of $[-\infty,+\infty]$.

Let $\mathcal{A}(I)$ denote the set of elements in K of valuation in I. And if f is bounded at r_1 and r_2, then it is convergent on (r_1,r_2). ⌟

Def. (14.2.5.21) [Valuations]. For $f\in\mathcal{L}_K$ and $r\in[-\infty,\infty]$, define $v^{(r)}(f)=\inf_{n\in\mathbb{Z}}\{v(a_n)+nr\}\in[-\infty,\infty]$.

And if $r\in\mathrm{Conv}(f)\cap\mathbb{R}$, denote $n(f,r)$ and $N(f,r)$ to be the smallest and largest integer s.t. $v^{(r)}(f)=v_p(a_i(f))+ir$. ⌟

Def. (14.2.5.22) [Boundedness]. $f\in\mathcal{L}_K$ is called bounded on the radius $r\in\mathbb{R}$ if $v^{(r)}(f)>-\infty$. If f is convergent on radius r, then it is bounded on radius r. ⌟

Def. (14.2.5.23). Denote $\mathcal{L}_K[r_1,r_2]=\{f|f \text{ is convergent on } [r_1,r_2]\}$.

$\mathcal{L}_K(r_1,r_2]=\{f|f \text{ is convergent on } (r_1,r_2]\}$.

$\mathcal{L}_K]r_1,r_2]=\{f|f \text{ is convergent on } (r_1,r_2] \text{ and bounded at } r_1\}$.

$\mathcal{L}_K\{r\}=\mathcal{L}_K[r,r]$.

$\mathcal{B}_L(I)$ is the subset of bounded functions. These are all rings under addition and multiplication.

⌟

Proof: Cf.[Foundations of Theory of (φ,Γ)-modules over the Robba Ring P31].? □

Prop. (14.2.5.24). For $I = [r_1, r_2]$ or $(r_1, r_2]$, $\mathcal{L}_K I$ is an integral domain. Moreover, for $r \in I$ and $f, g \in \mathcal{L}_K I^\times$,

$$v^{(r)}(fg) = v^{(r)}(f) + v^{(r)}(g),$$
$$n(fg, r) = n(f, r) + n(g, r),$$
$$N(fg, r) = N(f, r) + N(g, r).$$

⌟

Proof: Cf.[Foundations of Theory of (φ, Γ)-modules over the Robba Ring]P32.**?** □

Prop. (14.2.5.25). If $f, g \in \mathcal{L}_K$ is bounded at $r \in \mathbb{R}$, then for f, g bounded on radius r,

- $v^{(r)}(f) = \infty \iff f = 0$.
- $v^{(r)}(f + g) \geq \min(v^{(r)}(f), v^{(r)}(g))$.
- For $\lambda \in L$, $v^{(r)}(\lambda f) = v_p(\lambda) + v^{(r)}(f)$.

⌟

Cor. (14.2.5.26). By(14.2.5.24) and(14.2.5.25), if $I = [r_1, r_2]$ or $(r_1, r_2]$ and $r \in I$, then $v^{(r)}$ is an additive valuation on $\mathcal{L}_K I$. ⌟

Def. (14.2.5.27). If we set for $\mathcal{L}_K]r_1, r_2]$ the the valuation $v^{[r_1,r_2]}(f) = \min\{v^{(r_1)}(f), v^{(r_2)}(f)\}$, then this is a valuation on it. ⌟

Prop. (14.2.5.28). $\mathcal{L}_K(\{r\})$ is complete under valuation $v^{(r)}$. Similarly the valuation $v^{[r_1,r_2]}(f)$ makes $\mathcal{L}_K[r_1, r_2]$ a Banach space unless $r_1 = r_2 = \infty$. ⌟

Proof: We let $r = 0$. For a Cauchy sequence of Laurent series, we see that each coefficient is a Cauchy sequence, hence converge to some element in L, so it converge term-wise to a Laurent series f, so it converse to f in $v^{(r)}$. □

Cor. (14.2.5.29)[Fréchet Topology]. We consider $\mathcal{L}_K(0, r]$, then it has a countable sequence of norms $v^{1/n,r}$, which makes it a locally convex space, and the last proposition shows that these valuations are complete, and a Cauchy sequence must converge to the term-wise limit, so $\mathcal{L}_K(0, r]$ is a complete Fréchet space in the Fréchet topology. ⌟

Cor. (14.2.5.30). The same method shows that $\mathcal{L}_K(I)$ is a Fréchet space for any interval I. ⌟

Def. (14.2.5.31) [Newton Polygon]. For a non-Archimedean valued field K and a power series $P(X) = a_0 + a_1 X + \cdots + a_d X^d + \ldots \in K[[X]]$, its **Newton polygon** is defined to be the lower convex hull of the set of points $\{(0, v(a_0)), (1, v(a_1)), \ldots, (d, v(a_d)), \ldots\}$. ⌟

Prop. (14.2.5.32)[Roots and Newton Polygons]. For a non-Archimedean valued field K the number of roots of P in $\overline{K}$ with valuation λ equals the horizontal width of the segment of Newton polynomial of P of slope $-\lambda$. ⌟

Proof: Firstly if P is a polynomial, we may assume P is monic, then its coefficients are elementary polynomials of roots of P. Thus the conclusion follows as K is non-Archimedean.

Next, we can use p-adic Weierstrass preparation(14.2.5.12) to get the desired results.**?** □

Prop. (14.2.5.33). . If $I =]0, +\infty]$ and $f(X) \in \mathcal{H}(I)$, then the number of zeros of $f(X)$ in $\mathcal{A}(I)$ equals the length of the segment of $NP(f)$ whose slope is $-s$, and these roots gives a $P_s(X) \in K[X]$ that $f(X) = P_s(X)G(X)$, $G(X) \in \mathcal{H}(I)$. ⌟

Proof: Cf.[Zeros of Power Series over complete Valued Field Lazard]. □

Cor. (14.2.5.34). If $f(X)\in\mathcal{H}(I)$, then $f(X)\in\mathcal{B}_L(I)$ iff it has f.m. zeros in $\mathcal{A}(I)$. ⌟

Proof: Let $r=\inf I$ and $s=\sup I$. First notice that $f\in\mathcal{L}_K(I)$ is in $\mathcal{B}(I)$ iff $v(a_n)+nr$ is bounded from below as $n\to+\infty$ and $v(a_n)+ns$ is bounded below as $n\to-\infty$. And from the graph of $NP(f)$, this is equivalent to f has f.m. zeros in $\mathcal{A}(I)$. □

Prop. (14.2.5.35). $\mathcal{H}(I)$ is a Bezout domain. ⌟

Proof: [Lazard]. □

Robba Ring

Def. (14.2.5.36) [Robba Ring and Overconvergent Elements]. Define

$$\mathcal{E}_K=\{f=\sum_{n\in\mathbb{Z}}a_nT^n\in\mathcal{L}_K^{]0[}:\lim_{n\to-\infty}v(a_n)=\infty\},$$

and also the **overconvergent elements** $\mathcal{E}^\dagger$ and **Robba ring** $\mathcal{R}$ as

$$\mathcal{E}_K^\dagger=\bigcup_{r>0}\mathcal{L}_K]0,r],\quad \mathcal{R}_K=\bigcup_{r\in(0,1)}\mathcal{L}_K(r,1]$$

and equip them with the final topology w.r.t. the Fréchet topologies on $\mathcal{L}_K(0,r]$(14.2.5.29). Then $\mathcal{E}_K^\dagger=\mathcal{R}_K\cap\mathcal{E}_K$. Also denote

$$\mathcal{E}_K^+=\mathcal{E}_K^\dagger\cap K[[T]],\quad \mathcal{R}_K^+=\mathcal{R}_K\cap K[[T]].$$

⌟

Prop. (14.2.5.37) [Lazard].

- $\mathcal{R}_K$ is a Bezout domain.
- Any finite submodule of $\mathcal{R}_K^n$ admits elementary divisors.

⌟

Proof: Cf.[Ber02]. □

Prop. (14.2.5.38). There is a Frobenius action φ and an action of $\mathbb{Z}_p^*$ on $\mathcal{R}_K$ defined by

$$\varphi(f)(T)=f((T+1)^p-1),\quad \gamma(f)(T)=f((T+1)^\gamma-1).$$

Also denote $t=\log(T+1)=\sum_{n\geq1}(-1)^{n+1}\frac{T^n}{n}\in\mathcal{R}_K$, then $\varphi(t)=pt,\gamma(t)=\gamma t$. ⌟

Proof: □

Prop. (14.2.5.39). The only principle ideals of $\mathcal{R}_K$ stable under the action of φ and $\mathbb{Z}_p^*$ are $t^i\mathcal{R}_K$, $i\in\mathbb{N}$. ⌟

Proof: Cf.[L. Berger, E´quations diff´erentielles p-adiques et (,N)-modules filtr´es]. □

For more properties of Robba ring, See [Foundations of Theory of (φ,Γ)-modules over the Robba Ring Chap4].

14.3 p-adic Lie Groups

References are [Schneider].

14.4 Global Fields

Main references are [Neu99], [Sen80], [R-V99], [Cox13], https://math.mit.edu/classes/18.785/2015fa/lectures.html, http://www.math.columbia.edu/~chaoli/docs/ClassFieldTheory.html#thm:CFTlocalnorm, should also consult notes of Pete. L. Clark.

Notation (14.4.0.1).

- Use notations defined in Commutative Algebra II.
- Use notations defined in Valuations of Rank 1, all valuations are of rank1.
- Use notations defined in More on (Non-Commutative)Algebras.
- Use notations defined in p-adic Analysis.
- Let $(K, \mathcal{O}_K) \in \texttt{LField}$.
- Let $(F, \mathcal{O}_F) \in \texttt{GField}$(14.4.1.1)(14.4.1.2).

⌟

1 Global Fields

Def. (14.4.1.1) [Global Fields]. A **global field** is a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p((t))$, without a valuation. The former is called a **number field** and the latter a **function field**. The set of global fields is denoted by `GField`. The partially ordered set of number fields is denoted by `NField`. The partially ordered set of function fields is denoted by `FField`. ⌟

Def. (14.4.1.2) [Ring of Integers]. $\mathbb{Z} \subset \mathbb{Q}$ and $\mathbb{F}_p[t] \subset F_p((t))$ are PIDs, thus Dedekind domains, thus for a global field F(14.4.1.1), we can define the **ring of integers** $\mathcal{O}_F$ of F to be the integral closure of $\mathbb{Z}$ or $\mathbb{F}_p[t]$ in F, which is an Dedekind domain, by(5.2.7.12) and(3.2.3.17). ⌟

Remark (14.4.1.3). The section Dedekind Domains applies to the ring of integers $\mathcal{O}_F$ for $F \in \texttt{GField}$. ⌟

Def. (14.4.1.4) [Roots of Unity]. Denote $\mu(F)$ be the set of roots of unity in F, which is a finite group. ⌟

Def. (14.4.1.5) [Places].

- Σ_F^{fin} is the equivalent classes of (non-Archimedean)valuations of F, called the **finite places** of F.
- Σ_F^{∞} is the equivalent classes of (Archimedean valuations)$|\cdot|_v = -\log|\tau(\cdot)|$ of F corresponding to embeddings $\tau : K \to \mathbb{C}$(11.2.3.16), called the **infinite places** of F.
- $\Sigma_F^{\mathbb{R}}$ is the set of infinite places v of F corresponding to embeddings $F \to \mathbb{R}$, called the set of **real places** of F. Denote $r_1 = \#\Sigma_F^{\mathbb{R}}$ if it is finite.
- $\Sigma_F^{\mathbb{C}}$ is the set of infinite places v of F that is non-real, called the set of **complex places** of F. Notice two embeddings corresponds to the same place iff they are conjugate. Denote $r_2 = \#\Sigma_F^{\mathbb{C}}$ if it is finite.
- For $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_F)$, $v_{\mathfrak{p}}$ is the valuation of F corresponding to F. Most of the time we will not distinguish between a maximal prime $\mathfrak{p}$ and its corresponding valuation.
- For a finite extension L/F and $v \in \Sigma_F$, Σ_L^v is the set of finite places over L over v.

- For $v\in\Sigma_F$, denote F_v the completion of F w.r.t. v.
- For any non-zero ideal $\mathfrak{a}\neq 0\in\mathrm{Ideal}(\mathcal{O}_F)$, denote $||\mathfrak{a}||=\#\mathcal{O}_F/\mathfrak{a}$, called the **norm of ideal** $\mathfrak{a}$.

⌟

Def. (14.4.1.6) [Constant Fields]. ⌟

Prop. (14.4.1.7) [Valuations]. For $F\in\texttt{GField}, v\in\Sigma_F$, let $\mathrm{p}\in\mathbf{P}\cup\{\infty\}$ s.t. $v|\mathrm{p}$, then define the **inertia degree**

$$f_v=\begin{cases}[\kappa(v):\kappa(\mathrm{p})] & ,v\in\Sigma_F^{\mathrm{fin}}\\ [F_v:F_{\mathrm{p}}] & ,v\in\Sigma_F^{\infty}\end{cases},\quad ||v||=\begin{cases}\mathrm{p}^{f_v} & ,v\in\Sigma_F^{\mathrm{fin}}\\ e^{f_v} & ,v\in\Sigma_F^{\infty}\end{cases},\quad |\cdot|_v=||v||^{-v(a)}$$

This is compatible with the definition in(5.2.7.20) when $v\in\Sigma_F^{\mathrm{fin}}$. ⌟

Prop. (14.4.1.8) [Product Formula]. Let $F\in\texttt{GField}$ and $a\in F^\times$, then $|a|_w=1$ for a.e. $w\in\Sigma_F$, and

$$\prod_{w\in\Sigma_F}|a|_w=1.$$

⌟

Proof: Let $F_0=\mathbb{Q}$ or $\mathbb{F}_p(t)$ be the constant field of F(14.4.1.6), then the assertion is easy to verify for F_0, and

$$\prod_{w\in\Sigma_F}|a|_w=\prod_{v\in F_0}\prod_{w|v}|a|_w=\prod_{v\in F_0}|\mathrm{Nm}_{F/F_0}(a)|_v=1.$$

□

Prop. (14.4.1.9) [Artin-Whaples]. Let $F\in\texttt{Field}$ and Σ_F the set of places of F, then $F\in\texttt{GField}$ iff

- There exists representatives $|\cdot|_v$ for $v\in\Sigma_F$ s.t. the product formula $\prod_{v\in\Sigma_F}|a|_v=1$ for any $a\in F^\times$.
- For any $v\in\Sigma_F$, F_v is a local field(14.2.3.2).

⌟

Proof: □

Prop. (14.4.1.10) [Global and Local]. Let $F\in\texttt{GField}$, $v\in\Sigma_F$, then for any extension L^w/F_v, there exists a global field L/F extension s.t. $L^w=LF_v$, and $[L:F]=[L^w:F_v]$. ⌟

Proof: Cf.[Sutherland, L11]. □

Def. (14.4.1.11) [Algebraic Integers]. An element $\alpha\in\overline{\mathbb{Q}}$ is called an **algebraic number**. It is called an **algebraic integer** iff it satisfies a monic polynomial equation $p(X)\in\mathbb{Z}[T]$. Notice the set of algebraic integers equals

$$\mathcal{O}_{\overline{\mathbb{Q}}}=\bigcup_{F\subset\mathbb{C}}\mathcal{O}_F.$$

where the union is taken over all number fields F. ⌟

Prop. (14.4.1.12). If α is an algebraic integer s.t. any of its conjugate has absolute value 1, then α is a root of unity. ⌟

Proof: For any power α^r of α, its minimal polynomial over $\mathbb{Q}$ has bounded degree and bounded coefficients independent of r, so there are only f.m. such polynomial and f.m. such roots. Thus $\alpha^i = \alpha^j$ for some $i \neq j \in \mathbb{Z}_+$, and $\alpha \in \mu(\overline{\mathbb{Q}})$. ☐

Def. (14.4.1.13) [Weil Numbers]. For $p \in \mathbf{P}, q \in p^{\mathbb{Z}}$, a q-adic **Weil number** of weight w is an algebraic integer $\alpha \in \mathcal{O}_{\overline{\mathbb{Q}}}$ that for any embedding $\iota : \mathbb{Q} \to \mathbb{C}$, $|\iota(\alpha)| = q^{w/2}$. The set of Weil q-numbers of weight w is denoted by $\mathrm{Weil}(q^{w/2})$. ⌟

Prop. (14.4.1.14) [Discriminants]. For $F \in \texttt{NField}$, there is a discriminant $\mathfrak{d}_{F/\mathbb{Q}}$ which is an ideal of $\mathbb{Z}$(5.2.7.36), and if $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis of $\mathcal{O}_F$, then $\mathfrak{d}_{F/\mathbb{Q}} = (d(\alpha_1, \ldots, d_n))$. And this d_F is invariant of the basis chosen. So it is also called the **discriminant of** F.

Then $d_F \equiv 0, 1 (\mathrm{mod}\ 4)$. ⌟

Proof: ☐

Prop. (14.4.1.15) [Sign of Discriminants]. If $F \in \texttt{NField}$. then $d(F) \in (-1)^{r_2}\mathbb{Z}_+$. ⌟

Proof: $d(F) \neq 0$ by(3.2.6.34), and by definition, $d(F) = \det((\sigma\alpha_i)_{\sigma,i})^2$, where σ runs through embeddings $F \hookrightarrow \mathbb{C}$, and $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis of $\mathcal{O}_F$. Then notice

$$\overline{\det((\sigma\alpha_i)_{\sigma,i})} = (-1)^{r_2} \det((\sigma\alpha_i)_{\sigma,i}),$$

so if r_2 is odd, then $\det((\sigma\alpha_i)_{\sigma,i})$ is purely imaginary, and if r_2 is even, $\det((\sigma\alpha_i)_{\sigma,i})$ is real. Thus the assertion follows. ☐

Galois Theory of Extensions

Def. (14.4.1.16) [Ramification Groups]. For a Galois extension of global fields L/K and a valuation extension $w|v$, denote λ/k residue fields extension of $w|v$, and denote $\mathfrak{p}_w, \mathfrak{p}_v$ by $\mathfrak{P}, \mathfrak{p}$.

Then the **decomposition group** is $G_w(L/K) = \{\sigma \in G(L/K) | w \circ \sigma = w\}$. The **decomposition field** Z_w is the fixed field of G_w.

When w is non-Archimedean, we further define:

The **inertia group** is $I_w(L/K) = \{\sigma \in G_w(L/K) | \sigma(x) \equiv x \mod \mathfrak{P}\}$. The **inertia field** T_w is the fixed field of I_w.

The **ramification group** is $R_w(L/K) = \{\sigma \in G_w(L/K) | \sigma(x)/x \equiv 1 \mod \mathfrak{P}\}$. The **ramification field** V_w is the fixed field of R_w.

Similarly we can define for higher ramification groups $G_{w,s}(L/F)$. ⌟

Prop. (14.4.1.17) [Local and Global Ramification Groups]. Let L/F be a Galois extension of global fields, $v \in \Sigma_F, w \in \Sigma_L^v$, then any embedding $L \to \overline{F}_v$ induces isomorphisms

$$G_{w,s}(L/F) \cong G_s(L_w/F_v)$$

by natural restriction. ⌟

Proof: Cf.[ANT, Neukirch]. ☐

Cor. (14.4.1.18) [Local and Global Galois Groups]. There is an embedding $\mathrm{Gal}(L_w/F_v) \hookrightarrow \mathrm{Gal}(L/F)$ that is determined up to conjugation. In particular, there is an embedding

$$\mathrm{Gal}_{F_v} \hookrightarrow \mathrm{Gal}_F$$

determined up to conjugation. ⌟

Proof: It is determined up to conjugation because $\mathrm{Gal}(L/F)$ acts transitively on the places over v: For finite places this follows from(5.2.7.22), and for infinite places this means $\mathrm{Gal}(L/F)$ acts transitively on the extension of embedding to $\mathbb{C}$, which is clearly true. □

Prop. (14.4.1.19) [Z_w].

- The restriction w_Z of w to Z_w extends uniquely to L.
- If v is non-Archimedean, w_Z has the same residue field and value group as v.
- $Z_w = L \cap K_v \subset L_w$.

⌟

Proof: Cf.[Neukirch P171]. □

Prop. (14.4.1.20). T_w/Z_w is the maximal unramified subextension of L/Z_w. ⌟

Proof: Cf.[Neukirch P173]. □

Prop. (14.4.1.21). V_w/Z_w is the maximal tamely ramified subextension of L/Z_w. ⌟

Proof: Cf.[Neukirch P175]. □

Minkowski Theory

Def. (14.4.1.22) [Global Lattices]. If $F \in \mathtt{GField}$ and $V \in \mathcal{V}\mathrm{ect}/F$, then an **$\mathcal{O}_F$-lattice** in V is a f.g. $\mathcal{O}_F$-module Λ s.t. that generates V as a F-vector space.

In general, $\Lambda = \mathcal{O}_F x_1 \oplus \mathcal{O}_F x_2 \oplus \ldots \oplus \mathcal{O}_F x_{n-1} \oplus \mathfrak{a} x_n$ where $\mathfrak{a} \in \mathrm{Ideal}(\mathcal{O}_F)$(Cf. [P-R94]P42, may have to do with(5.2.7.15)**?**), and it is called a **free lattice** if $L \cong \mathcal{O}_F^n$. Notice this is always the case if $\mathrm{cl}(\mathcal{O}_F) = 1$, e.g. when $F = \mathbb{Q}$. ⌟

Prop. (14.4.1.23) [Local to Global Compatibility for Lattices]. Let $F \in \mathtt{NField}$, then

- If Λ is an $\mathcal{O}_F$-lattice in F^n, then for any $v \in \Sigma_F$, its completion in F_v is an $\mathcal{O}_{F_v}$-lattice in F_v^n, and for a.e. place v, $\Lambda_v = \mathcal{O}_{F,v}^n$.
- Conversely, if for any $v \in \Sigma_F^f$, Λ_v is an $\mathcal{O}_{F_v}$-lattice in F_v^n, and $\Lambda_v = \mathcal{O}_{F,v}^n$ for a.e. v, then there is a unique F-lattice $\Lambda \in F^n$ s.t. Λ_v is the closure of Λ in F_v. In fact, $\Lambda = \cap_{v \in \Sigma_F^f}(F^n \cap \Lambda_v)$.
- Λ is determined by Λ_v for each $v \in \Sigma_F^f$.

⌟

Proof: 1 is easy. For 2, notice that $\mathcal{O} = \cap_{v \in \Sigma_F^f}(\mathcal{O}_{F_v})$, so Λ defined as above is commensurable with $\mathcal{O}_F^n$, so it is clearly a lattice, because $\mathcal{O}_F$ is Noetherian. 3 follows from 2. (I think this argument also holds for global function fields?) □

Prop. (14.4.1.24) [Minkowski]. Let $\mathfrak{a} \neq 0 \in \mathrm{Ideal}(\mathcal{O}_F)$ and for each $\tau \in \mathrm{Hom}(F, \mathbb{C})$, let $c_\tau > 0$ s.t. $c_\tau = c_{\overline{\tau}}$ and

$$\prod_\tau c_\tau > (\frac{2}{\pi})^s |d_K|^{1/2} (\mathcal{O}_K : \mathfrak{a}),$$

then there exists $a \in \mathfrak{a}^\times$ s.t. for any $\tau \in \Sigma_F^\infty$,

$$|\tau(a)| < c_\tau$$

⌟

Proof: Cf.[Neu99]P32. □

Cor. (14.4.1.25). For $\mathfrak{a} \neq 0 \in \mathrm{Ideal}(\mathcal{O}_F)$, there exists $a \in \mathfrak{a}^\times$ s.t

$$|\tau(a)| < (\frac{2}{\pi})^{s/n}|d_K|^{1/2n}(\mathcal{O}_K : \mathfrak{a})^{1/n}$$

for any $\tau \in \mathrm{Hom}(F, \mathbb{C})$. ⌟

Prop. (14.4.1.26) [Regulator Map]. There is a **regulator map**

$$\mathrm{Reg}_F : \mathcal{O}_F^* \to [\prod_{\tau\in\Sigma_F^\infty} \mathbb{R}]^+$$

such that the kernel is $\mu(F)$, and the image is a complete lattice in $H = \{(x_i)|\sum x_i = 0\}$. ⌟

Proof: Cf.[Neukirch, P43]. □

Cor. (14.4.1.27)[Regulators]. Let $\{\varepsilon_1, \ldots, \varepsilon_t\}_{t=r_1+r_2-1}$ be a system of fundamental units in F, define $\mathrm{Reg}(F)$ the **regular of** F to be the absolute value of any $t \times t$ minor of the following matrix

$$\begin{bmatrix} \mathrm{Reg}^{(1)}(\varepsilon_1) & \ldots & \mathrm{Reg}^{(1)}(\varepsilon_t) \\ \vdots & & \vdots \\ \mathrm{Reg}^{(t+1)}(\varepsilon_1) & \ldots & \mathrm{Reg}^{(t+1)}(\varepsilon_t) \end{bmatrix},$$

then the volume of $\mathrm{Reg}(\mathcal{O}_F^*) \subset H$ is

$$\mathrm{Vol}(\mathrm{Reg}(\mathcal{O}_F^*)) = \sqrt{r_1 + r_2}\,\mathrm{Reg}(F).$$

⌟

Proof: Cf.[Neukirch, P43]. □

Thm. (14.4.1.28) [Bounded Ramifications are Rare]. Let $\Sigma_F^\infty \subset S \subset \Sigma_F$, $\#S < \infty$, then there are only f.m. field extensions L/F of a given degree n that are unramified outside S. ⌟

Proof: The power of a prime $\mathfrak{P}$ in the discriminant is controlled by n by(5.2.7.35). Together with(5.2.7.37), thus shows the power of $\mathfrak{p}$ in the discriminant of the extension is controlled by n, independent of the field. Also we can assume $\sqrt{-1} \in F$, because it changes the discriminant by a bounded factor, by(5.2.7.38). So it suffices to prove there are only f.m. field extension with fixed degree and discriminant. By(5.2.7.38), we can assume $K = \mathbb{Q}$.

For the rest, we use Minkowski's theorem, Cf.[Neukirch, P203]?. □

Prop. (14.4.1.29) [Lower Bounds for Discriminant]. The discriminant of F satisfies

$$|d_F|^{1/2} \geq \frac{n^n}{n!}(\frac{\pi}{4})^{n/2}.$$

⌟

Proof: Cf.[Neukirch, P204]. □

Cor. (14.4.1.30) [Hermit's Theorem]. There are only f.m. number fields with a given discriminant. ⌟

Proof: (14.4.1.29) shows the degree is controlled by the discriminant, thus the theorem follows from(14.4.1.28). □

Cor. (14.4.1.31) [Minkowski's Theorem]. For $F \neq \mathbb{Q} \in$ `NField`, $d_F \neq \pm 1$. ⌟

Cor. (14.4.1.32). $\mathbb{Q}$ doesn't have any non-trivial unramified extensions, by(5.2.7.39). ⌟

Orders

References are [Neu99]Chap1.12 and [P-R94]P42.

Def. (14.4.1.33) [Orders]. An **order** is a Noetherian integral domain $\mathcal{O}$ of dimension 1 whose conductor(5.2.7.17) is non-zero, or equivalently its integral closure in the fraction field is finite over $\mathcal{O}$ by(5.2.7.18). A Dedekind domain is an order. ⌟

Def. (14.4.1.34)[A-Orders]. If A is Noetherian domain with fraction field K and $B \in \mathcal{R}\mathrm{ing}^{\mathrm{fd}}/K$, then an A**-order** in B is an A-lattice(14.4.1.22) in B that is also a subring. ⌟

Prop. (14.4.1.35)[Orders in Number Fields]. Situation as in(5.2.7.13), if L/K is separable, then a subring $\mathcal{O}$ of L is an $\mathcal{O}_K$-order iff it is an order in L(14.4.1.33) with integral closure $\mathcal{O}_L$. in particular, $\mathcal{O}_L$ is the maximal $\mathcal{O}_K$-order in L.

In particular, for $F \in \mathtt{NField}$, the $\mathbb{Z}$-orders of F are exactly subrings of $\mathcal{O}_F$ that contains a basis of F, and they all have finite indexes in $\mathcal{O}_F$. ⌟

Proof: If $\mathcal{O}$ is an $\mathcal{O}_K$-order, then every element of $\mathcal{O}$ is integral over $\mathcal{O}_K$, by acting on $\mathcal{O}$. $\mathcal{O}_K$ is contained in $\mathcal{O}$, and $\mathcal{O} \otimes_{\mathcal{O}_K} K = L$, so the fraction field of $\mathcal{O}$ is L. Thus the integral closure of $\mathcal{O}$ in L is $\mathcal{O}_L$. Then $\dim \mathcal{O} = 1$ as $\dim \mathcal{O}_L = 1$(5.2.4.14), and it is Noetherian because it is f.g. over A(5.1.1.41). And $\mathcal{O}_L$ is finite over $\mathcal{O}_K$ by(5.2.7.21), thus is also f.g. over $\mathcal{O}$. Thus $\mathcal{O}$ is an order.

If $\mathcal{O}$ is an order with integral closure $\mathcal{O}_L$, then it is f.g. over $\mathcal{O}_K$ as it is contained in the f.g. $\mathcal{O}_K$-module $\mathcal{O}_L$. And it contains a K-basis of L because $L = K\mathcal{O}_L$ and $a\mathcal{O}_L \subset \mathcal{O}$ for some $a \in \mathcal{O}^\times$ because $\mathcal{O}$ is an order. Thus $\mathcal{O}$ is an A-lattice in L that is a ring, so it is an A-order.

For the last assertion, notice that one direction is clear, and if $\mathcal{O}_F$ contains a basis of F and is contained in $\mathcal{O}_F$, then it must be a $\mathbb{Z}$-lattice of F, as $\mathcal{O}_F$ is free because it is finite over $\mathbb{Z}$(5.2.7.21). Then it is clear $\mathcal{O}$ is an order with integral closure $\mathcal{O}_F$. □

Cor. (14.4.1.36). If $F \in \mathtt{NField}$ and $L = F(\alpha_i)$ where $\alpha_i \in \mathcal{O}_L$, then $\mathcal{O} = \mathcal{O}_F[\alpha_i]$ is an $\mathcal{O}_K$-order in L. ⌟

Prop. (14.4.1.37). Let $F \in \mathtt{NField}$ and Λ is a $\mathbb{Z}$-lattice in F, then the ring of multipliers

$$\mathcal{O} = \{\alpha \in \mathcal{O}_F | \alpha\Lambda \subset \Lambda\}$$

is an order in F. ⌟

Proof: $\mathcal{O}$ contains (d) for some $d \in \mathbb{Z}_+$, because for any $\alpha \in \mathcal{O}_F$, $\alpha\Lambda \subset F = \Lambda \otimes \mathbb{Q}$, so for some $d_\alpha \in \mathbb{Z}_+$, $d_\alpha\Lambda \subset \Lambda$.

Thus $\mathcal{O}$ contains a basis of F. And $\mathcal{O}$ is contained in $\mathcal{O}_F$: if $\alpha\Lambda \subset \Lambda$, then α satisfies the equation of its characteristic polynomial, which has coefficients in $\mathbb{Z}$. So $\alpha \in \mathcal{O}_F$. Thus $\mathcal{O}$ is an order, by(14.4.1.35). □

Prop. (14.4.1.38). Let $F \in \mathtt{NField}$ and $B \in \mathcal{R}\mathrm{ing}^{\mathrm{fd}}/F$, then an order $\mathcal{O} \leq B$ is maximal iff for each $v \in \Sigma_F^f$, $\mathcal{O}_v \subset B_{F_v}$ is maximal. ⌟

Proof: This is clear from(14.4.1.23) and the definition(14.4.1.34). □

Def. (14.4.1.39)[Discriminants of Orders]. Compatible with(14.4.1.14), if $F \in \mathtt{NField}$ and $\mathcal{O} \subset \mathcal{O}_F$ is an order, then we define the **discriminant of the order** $\mathcal{O}$ to be the $d(\mathcal{O}) = d(\alpha_1, \ldots, d_n)$ where $\alpha_1, \ldots, \alpha_n$ is a $\mathbb{Z}$-basis of $\mathcal{O}$. Notice this is invariant of the basis chosen. ⌟

Lemma (14.4.1.40). For $K \in p$-`LField`,

- $\mathrm{Mat}(n;\mathcal{O}_K)$ is a maximal order in $\mathrm{Mat}(n;K)$.
- Any two maximal orders in $\mathrm{Mat}(n;K)$ are conjugate.
- Any order $\mathcal{O} \subset \mathrm{Mat}(n;K)$ is contained in some maximal order. And it is contained in f.m. maximal orders.

⌟

Proof: 1: If another order contains $\mathrm{Mat}(n;\mathcal{O}_K)$ and also an element x, then we can clearly see that it contains an element of the form $A = \mathrm{diag}(x_1,\dots,x_n)$ s.t. $x_1 \notin \mathcal{O}_K$. Then $\{A^{\mathbb{Z}}\}$ is not bounded.

3: As $\mathcal{O}$ is compact and $\mathrm{Mat}(n;\mathcal{O}_K)$ is open, there exists f.m. x_i s.t. $B \subset \cup_i(x_i + \mathrm{Mat}(n;\mathcal{O}_K))$. Then it follows that $\Lambda = \oplus\mathcal{O}_K^n x_i$ is a lattice stable under $\mathcal{O}$, thus $\mathcal{O} \subset \mathrm{Stab}(\Lambda)$ is conjugate to $\mathrm{Mat}(n;\mathcal{O}_K)$ thus maximal.

Next we show $\mathcal{O}$ is contained in f.m. maximal orders: Suppose $\mathcal{O} \subset C = \mathrm{Stab}(\Lambda)$ and $\mathcal{O} \subset C' = \mathrm{Stab}(\Lambda')$, then there exists some α that $\varpi^\alpha \mathrm{Stab}(\Lambda) \subset \mathcal{O} \subset \mathrm{Stab}(\Lambda')$. Replacing Λ by a constant doesn't change stabilizer, so we may assume $\Lambda \subset \Lambda'$, and assume $\Lambda = \mathcal{O}_K\{e_1,\dots,e_n\}$ and $\Lambda' = \mathcal{O}_K\{e_1, \varpi^{\alpha_2}e_2,\dots,\varpi^{\alpha_n}e_n\}$. Since $\varpi^\alpha \mathrm{Stab}(\Lambda) \subset \mathrm{Stab}(\Lambda')$, $\mathrm{Stab}(\lambda)(\Lambda') \subset \varpi^{-\alpha}\Lambda'$. Also by using the matrices permuting e_1 and e_i, we see $\alpha_i < \alpha$ for each i, so $\varpi^\alpha\Lambda \subset \Lambda'$, and then $\varpi^n \mathrm{Stab}(\Lambda')(\Lambda) \subset \mathrm{Stab}(\Lambda')(\Lambda') = \Lambda' \subset L$. This implies $\varpi^\alpha \mathrm{Stab}(\Lambda') \subset \mathrm{Stab}(\Lambda)$. From this it is clear that there are only f.m. maximal orders containing $\mathcal{O}$.

2: It follows from the proof of item3 that any order is contained in a stabilizer, then it suffices to show that if $\mathrm{Stab}(\Lambda) = \mathrm{Stab}(\Lambda')$, then $\Lambda = \Lambda'$. But this is already implicit in the proof of item2: In this case, $\alpha = 0$. □

Thm. (14.4.1.41) [Maximal Orders in Semisimple Algebras over Local Fields]. If $K \in p$-`LField` and B is a semisimple algebra over K, then any $\mathcal{O}_K$-order $\mathcal{O} \subset B$ is contained in a maximal order. And there are only f.m. maximal orders containing it. ⌟

Proof: Writing B as a product of simple algebras, it suffices to prove for B simple, and by base change to the center L of B, it suffices to show for B central simple: This is because if two orders are isomorphic after extension by $\mathcal{O}_L$, then their transformation matrix has coefficients in $\mathcal{O}_L \cap K = \mathcal{O}_K$. Then we need to show that there are only f.m. orders containing $\mathcal{O}$. Choose a splitting field L/K for B, it reduces to prove for $B = \mathrm{Mat}(n;K)$: This reason is the same as above. Then the assertion follows from(14.4.1.40). □

Thm. (14.4.1.42)[Maximal Orders in Semisimple Algebras over Global Fields]. If $F \in$ `NField` and B is a semisimple algebra over F, then any order $\mathcal{O} \subset B$ is contained in some maximal order. And there are only f.m. maximal orders containing it. ⌟

Proof: Writing B as a product of simple algebras, it suffices to prove for B simple, and by base change to the center L of B, it suffices to show for B central simple: This is because if two orders are isomorphic after extension by $\mathcal{O}_L$, then their transformation matrix has coefficients in $\mathcal{O}_L \cap F = \mathcal{O}_F$. Then we need to show that there are only f.m. orders containing $\mathcal{O}$. Choose a splitting field L/F for B, it reduces to prove for $B = \mathrm{Mat}(n;F)$: This reason is the same as above.

And for $B = \mathrm{Mat}(n;F)$, by(14.4.1.40) and(14.4.1.23), $\mathcal{O}$ is already maximal at a.e. place, so the assertion follows from(14.4.1.23) and the local case(14.4.1.41). □

Quadratic Fields

Def. (14.4.1.43) [$\mathcal{O}_D$]. For $D \in \mathbb{Z}^\times$ s.t. $D \equiv 0, 1 (\text{mod } 4)$, denote $\mathcal{O}_D = \mathbb{Z}[\frac{D+\sqrt{D}}{2}]$, which is an order in $\mathbb{Q}(\sqrt{D})$. ⌟

Prop. (14.4.1.44) [Ring of Integers in Quadratic Fields]. Let $n \in \mathbb{Z}^\times$ be a square-free, and let $\mathcal{K} = \mathbb{Q}(\sqrt{n})$.

- If $n \equiv 2, 3 \mod 4$, then $\mathcal{O}_\mathcal{K} = \mathbb{Z}[\sqrt{n}]$, and $d_\mathcal{K} = 4n$.
- If $n \equiv 1 \mod 4$, then $\mathcal{O}_\mathcal{K} = \mathbb{Z}[\frac{1+\sqrt{n}}{2}]$, and $d_\mathcal{K} = n$.

In particular, $\mathcal{O}_\mathcal{K} = \mathcal{O}_{d_\mathcal{K}} = \mathbb{Z}[\frac{d_\mathcal{K}+\sqrt{d_\mathcal{K}}}{2}]$. ⌟

Proof: 1: the minimal polynomial of $\sqrt{n}$ is $X^2 - n$, whose discriminant is $4n$, which doesn't have a proper divisor β that $4n/\beta$ is a square and $\beta \equiv 0, 1 \mod 4$, so by(14.4.1.14) $\mathbb{Z}[\sqrt{n}]$ is the ring of integers.

2: the minimal polynomial of $\frac{1+\sqrt{n}}{2}$ is $X^2 - X + \frac{1-n}{4}$, whose discriminant is n, which doesn't have a proper divisor β that $4n/\beta$ is a square, so by(14.4.1.14) $\mathbb{Z}[\frac{1+\sqrt{n}}{2}]$ is the ring of integers.

For the last assertion, given the basis for the ring of integers, we can easily calculate the discriminant as in(3.2.6.33). It equals $4n$ in the first case and n in the second case. Thus the assertion follows. □

Def. (14.4.1.45) [Imaginary Quadratic Orders].

- $\mathbb{Z}[\mathrm{i}]$ is called the ring of **Gaussian integers**.
- $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is called the ring of **Eisenstein integers**.
- $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ is called the ring of **Kleinian Integers**.

These are all PIDs. ⌟

Thm. (14.4.1.46) [Primes in Quadratic Fields]. Let $\mathcal{K}$ be a quadratic field with discriminant $d_\mathcal{K}$. Then for $p \in \mathbf{P}$,

- If $p|d_\mathcal{K}$, then $p\mathcal{O}_K = \mathfrak{p}^2$, where $\mathfrak{p}$ is a prime in $\mathcal{O}_\mathcal{K}$, and $\mathfrak{p} = (p, \sqrt{d_\mathcal{K}})$ if p is odd.
- If $\left(\frac{d_\mathcal{K}}{p}\right) = 1$, then $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, where $p, \mathfrak{p} \neq \mathfrak{p}'$ are primes in $\mathcal{O}_\mathcal{K}$.
- If $\left(\frac{d_\mathcal{K}}{p}\right) = -1$, then $p\mathcal{O}_\mathcal{K}$ is a prime in $\mathcal{O}_\mathcal{K}$.

And every maximal prime in $\mathcal{O}_\mathcal{K}$ are of the form.

In particular, p ramifies in $\mathcal{K}$ iff $p|d_\mathcal{K}$, and p splits completely in $\mathcal{K}$ iff $\left(\frac{d_\mathcal{K}}{p}\right) = 1$. ⌟

Proof: 1 is easy.

2, 3: Cf.[Cox13]P92.

To show that every maximal prime $\mathfrak{p} \subset \mathcal{O}_\mathcal{K}$ is of this form, notice that $\mathfrak{p}|\operatorname{Nm}(\mathfrak{p})$ which is an ideal in $\mathbb{Z}$, so its prime factors are all of the form above. □

Orders in Imaginary Quadratic Fields

Prop. (14.4.1.47) [Orders in Quadratic Fields]. Let $\mathcal{K}$ be a quadratic field with discriminant $d_\mathcal{K}$, then for any $f \in \mathbb{Z}_+$, there exists a unique order in $\mathcal{O}_\mathcal{K}$ of index f, which is

$$\mathcal{O}_{\mathcal{K},f} = \mathbb{Z}[1, f\frac{d_\mathcal{K} + \sqrt{d_\mathcal{K}}}{2}].$$

And $d(\mathcal{O}_{\mathcal{K},f})=f^2 d_{\mathcal{K}}$(14.4.1.39). ⌟

Proof: Let $\mathcal{O}$ be an order of index f in $\mathcal{O}_{\mathcal{K}}$, then it is clear that $f\mathcal{O}_{\mathcal{K}}+\mathbb{Z}=\mathcal{O}_{\mathcal{K},f}\subset\mathcal{O}$. And this one has index f. The last assertion is clear from the definition of discriminant. □

Prop. (14.4.1.48) [Proper Fractional Ideals]. Let $F\in$ `NField` and $\mathcal{O}\subset\mathcal{O}_F$ an order. A fractional ideal $\mathfrak{a}$ of $\mathcal{O}$ is called a **proper fractional ideal** if

$$\mathcal{O}=\{\beta\in\mathcal{K}|\beta\mathfrak{a}\subset\mathfrak{a}\}.$$

Then any invertible fraction ideal is proper.

Moreover, if F is a quadratic field, then a fractional ideal is invertible iff it is proper. ⌟

Proof: Cf.[Cox13]P122. □

Prop. (14.4.1.49) [Class Group of Imaginary Quadratic Orders]. Let $\mathcal{K}$ be an imaginary quadratic field and $f\in\mathbb{Z}_+,\mathcal{O}=\mathcal{O}_{\mathcal{K},f}$. Denote

- $I(\mathcal{O},f)$ the subgroup of $I(\mathcal{O})$ generated by $\mathcal{O}$-ideals $\alpha\subset\mathcal{O}$ that is prime to f.
- $P(\mathcal{O},f)$ the group of $P(\mathcal{O})$ generated by $\alpha\in\mathcal{O}$ s.t. $N(\alpha)$ is prime to f.
- $I_{\mathcal{K}}(f)$ the subgroup of $I(\mathcal{O}_{\mathcal{K}})$ generated by $\mathcal{O}_{\mathcal{K}}$-ideals $\alpha\subset\mathcal{O}$ that is prime to f.
- $P_{\mathcal{K}}(f)$ the subgroup of $P(\mathcal{K})$ generated by $\alpha\in\mathcal{O}_{\mathcal{K}}$ s.t. $\alpha\equiv a(\mathrm{mod}\ f)\mathcal{O}_{\mathcal{K}}$ for some $a\in\mathbb{Z}\setminus(f)$.

Then

$$\mathrm{Cl}(\mathcal{O})\cong I(\mathcal{O},f)/P(\mathcal{O},f)\cong I_{\mathcal{K}}(f)/P_{\mathcal{K}}(f).$$

⌟

Proof: Cf.[Cox13]P131. □

2 Cyclotomic Fields

Def. (14.4.2.1) [Cyclotomic Units]. A **compatible system of roots of unity** is a system $\{\zeta_n,n\in\mathbb{Z}_+\}\subset\overline{\mathbb{Q}}$ s.t.

- $\zeta_m\neq 1$ for $m>1$.
- For $k,n\in\mathbb{Z}_+$, $\zeta_{kn}^k=\zeta_n$.
- $\zeta_4=\mathrm{i}$.

We fix a choice of compatible system of unity throughout this book. ⌟

Prop. (14.4.2.2). $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})\cong(\mathbb{Z}/(n))^*$. ⌟

Proof: We choose a prime p prime to n and show that ζ_n^p is conjugate to ζ_n.

Let $X^n-1=f(X)h(X)$ with f(X) minimal polynomial of ζ_n.If $f(\zeta_n^p)\neq 0$, then $h(\zeta_n^p)=0$,thus $h(X^p)=f(X)g(X)$. So modulo p, X^n-1 has a multi root, which is impossible. □

Lemma (14.4.2.3). For $p\in\mathbf{P},r\in\mathbf{Z}_+$, consider $\mathbb{Q}(\zeta_{p^r})$, then $(p)=(1-\zeta_{p^r})^{p^{r-1}(p-1)}$, and

$$d(1,\zeta_{p^r},\ldots,\zeta_{p^r}^{p^{r-1}(p-1)-1})=\pm p^{p^{r-1}(r(p-1)-1)},$$

where the sign is positive if $p^r=4$ or $p\equiv 3(\mathrm{mod}\ 4)$. ⌟

Proof: As $\Psi_{p^r}(X) = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \ldots + X^{p^{r-1}} + 1$, by taking $X = 1$, we get

$$p = \prod_{g \in (\mathbb{Z}/(n))^*} (1 - \zeta_{p^r}^g).$$

But it is easy to see that for any $g, g \in (\mathbb{Z}/(n))^*$, $1 - \zeta_{p^r}^g$ and $1 - \zeta_{p^r}^{g'}$ differ by a unit, so by(3.2.6.35), if ζ_i are the conjugates of ζ_{p^r}, then

$$d(1, \ldots, \theta^{p^{r-1}(p-1)-1}) = \prod_{i<j} (\zeta_i - \zeta_j)^2 = \pm \prod_i \Psi'_{p^r}(\zeta_i) = \pm \mathrm{Nm}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\Psi'_{p^r}(\zeta_{p^r})).$$

Differentiating the equation

$$(X^{p^{r-1}} - 1)\Psi_{p^r}(X) = X^{p^r} - 1,$$

we get

$$(\zeta_p - 1)\Psi'_{p^r}(\zeta_{p^r}) = p^r \zeta_{p^r}^{-1}.$$

Then notice as p is totally ramified in $\mathbb{Q}(\zeta_p)$(14.2.3.23),

$$\mathrm{Nm}_{\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}}(\zeta_p - 1) = (\mathrm{Nm}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1))^{p^{r-1}} = \pm p^{p^{r-1}},$$

and the assertion follows. The last assertion follows from(14.4.1.15). □

Prop. (14.4.2.4). For $n \in \mathbb{Z}_+$, $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. ┘

Proof: First consider the case $n = p^r$ a prime power. By(14.4.2.3), $d(1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{p^{r-1}(p-1)-1}) = \pm p^s$ for some $s \in \mathbb{Z}_+$, so $p^s\mathcal{O} \subset \mathbb{Z}[\zeta_{p^r}] \subset \mathcal{O}$. Because p totally ramifies by(14.2.3.23), $\mathcal{O} = \mathbb{Z}[\zeta_{p^r}] + (1 - \zeta_{p^r})\mathcal{O}$, thus $\mathcal{O} = \mathbb{Z}[\zeta]$ by Nakayama.

In general, if $n = \prod_i p_i^{r_i}$, for different p_i, and $\mathbb{Q}(\zeta_n) = \prod \mathbb{Q}(\zeta_{p_i^{r_i}})$ by Chinese remainder theorem, and the fields $\mathbb{Q}(\zeta_{p_i^{r_i}})$ are disjoint and the discriminant are pairwisely coprime, thus by(5.2.7.16), the products of the integral basis form an integral basis. □

Cor. (14.4.2.5). $\mathcal{O}_{\mathbb{Q}(\zeta_n + \zeta_n^{-1})} = \mathbb{Z}[\zeta_n + \zeta_n^{-1}]$. ┘

Prop. (14.4.2.6). By(17.3.3.9), for $p \geq 3 \in \mathbf{P}$, $\mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}} p}) \subset \mathbb{Q}(\zeta_p)$. ┘

Prop. (14.4.2.7). For $p \in \mathbf{P}$, if $\varepsilon \in (\mathbb{Z}[\zeta_p])^*$, then there exists $\varepsilon_1 \in \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $r \in \mathbb{Z}$ s.t. $\varepsilon = \zeta_p^r \varepsilon_1$. ┘

Proof: The case $p = 2$ is clear. Assume $p \geq 3$, and $\alpha = \overline{\varepsilon}/\varepsilon$, then any conjugate of α has absolute value 1. Thus α is a root of unity(14.4.1.12), Assume $\alpha = \pm\zeta_p^a$**?**. Let $\varepsilon = b_0 + b_1\zeta_p + \ldots + b_{p-2}\zeta_p^{p-2}$, if $\alpha = -\zeta_p^a$, then

$$\overline{\varepsilon} = b_0 + b_1\zeta_p^{-1} + \ldots \equiv b_0 + b_1 + \ldots \equiv \varepsilon = -\zeta_p^a \overline{\varepsilon} \equiv \overline{\varepsilon} (\mathrm{mod}\ 1 - \zeta_p).$$

Then $2\overline{\varepsilon} \in (1 - \zeta_p)$, which is not possible.

Thus $\alpha = \zeta_p^a$. Assume $a \equiv 2r (\mathrm{mod}\ p)$, and $\varepsilon_1 = \zeta^{-r}\varepsilon$, then $\overline{\varepsilon}_1 = \varepsilon_1$, and $\varepsilon = \varepsilon_1 \zeta_p^r$. □

Prop. (14.4.2.8). $p \in \mathbf{P}$ splits in $\mathbb{Q}(\zeta_n)$ iff $p \equiv 1 \mod n$. ┘

Proof: First, if it splits, then $f_p = 1$. Because the ring of integers is $\mathbb{Z}[\zeta_n]$, so $X^n - 1$ splits in $\mathbb{F}_p$(14.4.2.4), thus $p \equiv 1 \mod n$. And if $p \equiv 1 \mod n$, it is unramified and $X^n - 1$ splits in $\mathbb{F}_p$, so $f_p = 1$. □

Prop. (14.4.2.9). $p \in \mathbf{P}$ is ramified in $\mathbb{Q}(\zeta_n)$ iff $p|n$. ⌟

Proof: This follows from(14.2.3.21) and(14.2.3.23). □

Cor. (14.4.2.10). If $m, n \in \mathbb{Z}_+$ are coprime, then $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. ⌟

Proof: This follows from Minkowski's theorem(14.4.1.31). □

Prop. (14.4.2.11). If $n \in \mathbb{Z}_+$ has at least two prime divisors, then $1 - \zeta_n$ is a unit in $\mathbb{Q}(\zeta_n)$. ⌟

Proof: By(3.3.2.11), $\mathrm{Nm}(1 - \zeta_n) = \Psi_n(1) = 1$. □

Prop. (14.4.2.12).

- If $n \in \mathbb{Z}_+$ is not of the form p^r or $2p^r$ for $p \in \mathbf{P}$, then $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is unramified at finite places.
- If $p \in \mathbf{P}$ and $n \in p^{\mathbb{Z}_+}$ or $n \in 2p^{\mathbb{Z}_+}$, then $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is ramified at any places above p, and unramified at other finite places.

⌟

Proof: For the first case, let p, q are two prime divisors of n(or $q = 2$, in which case take $q = 4$). Then ζ_p, ζ_q are not in $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$, so $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, \zeta_p) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, \zeta_q)$. But then $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ can only ramify at finite places that are both over p and over q, so it is unramified at all finite places.

For the second case, use the fact that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is totally ramified at p and unramified at other places(14.2.3.21) and(14.2.3.23). □

$\mathbb{Z}_p$-Extensions

Def. (14.4.2.13)[$\mathrm{cycl}_p(K)$]**.** For $p \in \mathbf{P}$ and $K \in$ p-`Field` or $K \in$ `GField`, Denote $K_{p^\infty} = K(\zeta_{p^\infty})$. Then by(14.4.2.2) and(14.2.3.12), $\mathrm{Gal}(K_{p^\infty}/K) \subset \mathbb{Z}_p^* \cong \mathbb{Z}_p \oplus G$ is a subgroup of finite index, where G is a finite group. So there is a unique subextension $\mathrm{cycl}_p(K) \subset K(\mu_{p^\infty})$ with $\mathrm{Gal}(\mathrm{cycl}_p(K)/K) \cong \mathbb{Z}_p$, called the **cyclotomic $\mathbb{Z}_p$-extension** of K.

Also denote $\mathrm{cycl}_{p,n}(K) \subset \mathrm{cycl}_p(K)$ the subextension of degree p^n. ⌟

Prop. (14.4.2.14). If ℓ is a p is totally ramified in $\mathrm{cycl}_p(\mathbb{Q})$, and any $\ell \in \mathbf{P} \setminus \{p\}$ is unramified in $\mathrm{cycl}_p(\mathbb{Q})$. ⌟

Proof: Cf.[Washington, P265]. □

Others

Prop. (14.4.2.15). For $n \in \mathbb{Z}_+$, the sum of primitive n-th roots of unity equals $\mu(n)$(2.6.3.21). ⌟

Proof: **?** Prove that the assertion is multiplicative, and then prove for prime powers. □

Prop. (14.4.2.16). Find all $n \in \mathbb{Z}_+$ and primitive n-th roots of unity $\zeta_1, \ldots, \zeta_4$ s.t.

$$\zeta_1 + \zeta_2 + \zeta_3 + \zeta_4 = 1.$$

⌟

Proof: By(14.4.2.15),

$$4\mu(n)=\sum_{k\in(\mathbb{Z}/(n))^*}\sum_{i=1}^{4}\zeta_i^k=\phi(n).$$

Thus $\varphi(n)=4$ and $\mu(n)=1$. Then n can only be 5, 8, 10, 12, and n can only be 10.

Now $\Psi_{10}(X)=X^4-X^3+X^2-X+1$, so the identity $\zeta_1+\zeta_2+\zeta_3+\zeta_4=1$ must be essentially identical to this one. So the only possibility is

$$\{\zeta_1,\zeta_2,\zeta_3,\zeta_4\}=\{e^{2\pi\mathrm{i}\frac{1}{10}},e^{2\pi\mathrm{i}\frac{3}{10}},e^{2\pi\mathrm{i}\frac{7}{10}},e^{2\pi\mathrm{i}\frac{9}{10}}\}.$$

□

3 Class Numbers

Def. (14.4.3.1) [Class Groups]. For $F\in$ `GField`, the **class group of** F is defined to be the class group $\mathrm{Cl}(\mathcal{O}_F)$ of $\mathcal{O}_F$. It is denoted by $\mathrm{Cl}(F)$. The cardinality of $\mathrm{Cl}(F)$ is called the **class number of** F, denoted by $\mathrm{cl}(F)$. ⌟

Lemma (14.4.3.2). For $F\in$ `GField` and $\mathfrak{a}\neq 0\in\mathrm{Ideal}(\mathcal{O}_F)$, there exists $a\in\mathfrak{a}^\times$ s.t.

$$|\operatorname{Nm}_{F/\mathbb{Q}}(a)|\leq(\frac{2}{\pi})^s\sqrt{|d_F|}||\mathfrak{a}||.$$

⌟

Proof: This follows immediately from(15.6.1.4). □

Thm. (14.4.3.3) [Class Numbers are Finite]. For $F\in$ `GField`, $\mathrm{cl}(F)=\#\,\mathrm{Cl}(F)<\infty$. ⌟

Proof: It is clear that there are only f.m. ideals $\mathfrak{a}\in\mathrm{Ideal}(\mathcal{O}_F)$ of bounded norm. Thus it suffices to prove that each ideal class is represented by an integral ideal $\mathfrak{b}\in\mathrm{Ideal}(\mathcal{O}_F)$ with $||\mathfrak{b}||\leq(\frac{2}{\pi})^s$. For this, let the ideal class be represented by $\mathfrak{a}$, and let $\gamma\in\mathcal{O}_F^\times$ s.t. $\mathfrak{b}=\gamma\mathfrak{a}^{-1}\subset\mathcal{O}_F$. Then by(14.4.3.2), there exists $\alpha\in\mathfrak{b}^\times$ s.t. $|\operatorname{Nm}_{F/\mathbb{Q}}(\alpha)|\leq(\frac{2}{\pi})^s\sqrt{|d_F|}||\mathfrak{b}||$. Then $\mathfrak{a}=\alpha\mathfrak{b}^{-1}=\alpha\gamma^{-1}\mathfrak{a}$ is contained in $\mathcal{O}_F$, and

$$||\mathfrak{a}||=|\operatorname{Nm}_{F/\mathbb{Q}}(\alpha)|/||\mathfrak{b}||\leq(\frac{2}{\pi})^s\sqrt{|d_F|}.$$

□

Conj. (14.4.3.4). There are infinitely many real quadratic field with class number 1. ⌟

Proof:

□

Conj.Cor. (14.4.3.5). There are infinitely many number fields with class number 1. ⌟

Proof:

□

Class Numbers of Imaginary Quadratic Orders

References are [Gol85], [Sta67], [Cox13].

Thm. (14.4.3.6) [Dirichlet's Class Number Formula]. Let $\mathcal{K}$ be an imaginary quadratic field with discriminant $d_{\mathcal{K}}$, then

$$\mathrm{cl}(\mathcal{K}) = -\frac{\#\mu(\mathcal{K})}{2|d_{\mathcal{K}}|}\sum_{n=1}^{|d_{\mathcal{K}}|-1}\Big(\frac{d_{\mathcal{K}}}{n}\Big)n.$$

⌟

Proof: Cf.[Cox13]P134. □

Thm. (14.4.3.7). Let $\mathcal{K}$ be an imaginary quadratic field and $f \in \mathbb{Z}_+$, then $\mathrm{cl}(\mathcal{O}_{\mathcal{K}})|\,\mathrm{cl}(\mathcal{O})$, and

$$\mathrm{cl}(\mathcal{O}_{\mathcal{K},f}) = \frac{\mathrm{cl}(\mathcal{O}_{\mathcal{K}})f}{[\mu(\mathcal{O}_{\mathcal{K}}):\mu(\mathcal{O}_{\mathcal{K},f})]}\prod_{p|f}\Big(1-\Big(\frac{d_{\mathcal{K}}}{p}\Big)\frac{1}{p}\Big).$$

⌟

Proof: Cf.[Cox13]P132. □

Prop. (14.4.3.8). Let $p \equiv 3 \pmod 4 \in \mathbf{P}$, then for $D = -p$ or $-4p$, $\mathrm{cl}(\mathcal{O}_D)$(14.4.1.43) is odd. ⌟

Proof: Cf.[Cox, Prop3.11 and Thm7.7(ii)].? □

Thm. (14.4.3.9) [Siegel]. Let $\mathcal{K}$ be an imaginary quadratic field with discriminant $d_{\mathcal{K}}$, then

$$\lim_{d_{\mathcal{K}}\to-\infty}\frac{\mathrm{cl}(\mathcal{K})}{\log|d_{\mathcal{K}}|} = \frac{1}{2}.$$

⌟

Proof: Cf.[Sie35]. □

Thm. (14.4.3.10) [Gauss Class Number Problem1801, Siegel/Goldfeld-Gross-Zagier/Zhang]. There exists an effectively computable constant $C > 0$ s.t. for any imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ with discriminant $D < 0$,

$$\mathrm{cl}(\mathcal{O}_D) > C\frac{|D|^{1/2}}{(\log|D|)^{2022}}.$$

⌟

Proof: This follows from(21.4.3.3) and(21.4.2.11). □

Cor. (14.4.3.11) [Baker-Heegner-Stark].

- Let $\mathcal{K}$ be an imaginary quadratic field with discriminant $d_{\mathcal{K}}$, then

$$\mathrm{cl}(\mathcal{O}_{\mathcal{K}}) = 1 \iff d_{\mathcal{K}} \in \{-3,-4,-7,-8,-11,-19,-43,-67,-163\}.$$

These numbers are called **Heegner numbers**.

- Let $D \in \mathbb{Z}_{<0}$ and $D \equiv 0,1 \pmod 4$, then

$$\mathrm{cl}(\mathcal{O}_D) = 1 \iff D \in \{-3,-4,-7,-8,-11,-12,-16,-19,-27,-28,-43,-67,-163\}.$$

⌟

Proof: 1: Cf.[Cox, P247]?
2: Let $\mathcal{K}=\mathbb{Q}(\sqrt{D})$ and $D=f^2d_{\mathcal{K}}, f\in\mathbb{Z}_+$, then by(14.4.3.7), $\mathrm{cl}(\mathcal{O}_{\mathcal{K}})=0$, thus

$$d_{\mathcal{K}}\in\{-3,-4,-7,-8,-11,-19,-43,-67,-163\}.$$

If $\mu(\mathcal{K})=\{\pm 1\}$, then by(14.4.3.7) again, $f\leq 2$. And it can be checked directly that $f=2$ only happens when $d_{\mathcal{K}}\equiv\pm 1(\mathrm{mod}\ 8)$, so $d_{\mathcal{K}}=-7$.

If $|\mu(\mathcal{K})|>2$, then $d_{\mathcal{K}}=-3$ or -4. For $d_{\mathcal{K}}=-4$, $f\leq 2$, and it can be checked that $f=2$ works, and $D=-16$. If $d_{\mathcal{K}}=-3$, then $f\leq 3$, and it can be checked that $f=2$ or $f=3$ works. □

Class Number of Cyclotomic Fields

Prop. (14.4.3.12). For $p\geq 3\in\mathbf{P}$, $p|\,\mathrm{cl}(\mathbb{Q}(\zeta_p))$ iff there exists some $k\in\mathbb{Z}_+$ s.t. $k\leq\frac{p-3}{2}$ and p divides the denominator of B_{2k}(9.5.1.12). ⌟

Proof: ? □

Prop. (14.4.3.13) [Montgomery/Uchida]. For $p\in\mathbf{P}$, $\mathrm{cl}(\mathbb{Q}(\zeta_p))=1$ iff $p\leq 19$. ⌟

Proof: □

4 Adeles and Ideles

Restricted Direct Products

Def. (14.4.4.1) [Restricted Direct Products]. Let $\{\mathfrak{p}\}$ be a set of indices and given a family of locally compact Abelian groups $G_{\mathfrak{p}}$, and for a.e. $\mathfrak{p}$ an open compact subgroup $H_{\mathfrak{p}}\subset G_{\mathfrak{p}}$. Then the **restricted direct product** is defined to be

$$G=\prod{}'(G_{\mathfrak{p}},H_{\mathfrak{p}})=\varinjlim_{S\in\{\mathfrak{p}\},|S|<\infty}\prod_{\mathfrak{p}\in S}G_{\mathfrak{p}}\times\prod_{\mathfrak{p}\notin S}H_{\mathfrak{p}}$$

given the colimit space topology. And we denote $\prod_{\mathfrak{p}\in S}G_{\mathfrak{p}}\times\prod_{\mathfrak{p}\notin S}H_{\mathfrak{p}}=G_S,\prod_{\mathfrak{p}\notin S}H_{\mathfrak{p}}=G^S$.

This topology is stronger than the product topology of $\prod_{\mathfrak{p}}G_{\mathfrak{p}}$. It has an open basis $N=\prod_{\mathfrak{p}}N_{\mathfrak{p}}$, where $N_{\mathfrak{p}}$ is open in $G_{\mathfrak{p}}$ and $N_{\mathfrak{p}}=H_{\mathfrak{p}}$ for a.e. $\mathfrak{p}$. It is locally compact because every G_S does. ⌟

Prop. (14.4.4.2). Every compact subset N of G is contained in some $\prod_{\mathfrak{p}}N_{\mathfrak{p}}$, where $N_{\mathfrak{p}}$ is compact and $N_{\mathfrak{p}}=H_{\mathfrak{p}}$ for a.e. $\mathfrak{p}$. ⌟

Proof: This is because G_S is an open covering of G, and the union of f.m. G_{S_i} is also of the form G_S. So N is contained in some G_S, thus its projection in the S-coordinates is compact. □

Prop. (14.4.4.3) [Quasi-Characters on G]. Quasi-characters on G are all of the form $\otimes_{\mathfrak{p}}c_{\mathfrak{p}}$ that $c_{\mathfrak{p}}$ is trivial on $H_{\mathfrak{p}}$ for a.e. $\mathfrak{p}$. ⌟

Proof: Let c be a quasi-character, choose a nbhd of $1\in U\subset\mathbb{C}$ that contains no subgroup, then $c^{-1}(U)$ has contains an open basis $\prod_{\mathfrak{p}\in S}N_{\mathfrak{p}}\times G^S$, where $N_{\mathfrak{p}}$ are open nbhds of 1, so $c(G^S)=1$. Thus $c(\mathfrak{a})=\prod_{\mathfrak{p}}c_{\mathfrak{p}}(a_{\mathfrak{p}})$ is true for any $\mathfrak{a}\in G$.

Conversely, clearly $\otimes_{\mathfrak{p}}c_{\mathfrak{p}}$ is a quasi-character on G, it is continuous. □

Prop. (14.4.4.4)[Dual of G]. In each $G_\mathfrak{p}^\vee$, by(11.10.3.7) $H_\mathfrak{p}$ are compact, so $H_\mathfrak{p}^\vee = G_\mathfrak{p}^\vee/H_\mathfrak{p}^\perp$ are discrete, so $H_\mathfrak{p}^\perp$ is open; $H_\mathfrak{p}$ are open, so $H_\mathfrak{p}^\perp = (G_\mathfrak{p}/H_\mathfrak{p})^\vee$ are compact. So we can define the space $\prod'(G_\mathfrak{p}^\vee, H_\mathfrak{p}^\perp)$.

Then the dual group $G^\vee \cong \prod'(G_\mathfrak{p}^\vee, H_\mathfrak{p}^\perp)$ as a topological group. ⌟

Proof: (14.4.4.3) shows that this is an algebraic isomorphism, so it suffices to prove this is a topological homeomorphism(11.10.3.6):

For any compact $B \in G_1 = \prod_{\mathfrak{p}\in S} N_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} H_\mathfrak{p}$, for any $\varepsilon > 0$, if $c \in \prod_{\mathfrak{p}\in S} N'_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} H_\mathfrak{p}^\perp$, where $N'_\mathfrak{p} = \{c_\mathfrak{p} || c_\mathfrak{p}(N_\mathfrak{p} - 1)| < \varepsilon/|S|\}$, then $|c(B) - 1| < \varepsilon$.

Conversely, if ε is small enough, then if $c(\prod_{\mathfrak{p}\in S} N_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} H_\mathfrak{p}) - 1| < \varepsilon$, then $c \in \prod_{\mathfrak{p}\in S} N'_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} H_\mathfrak{p}^\perp$, where $N'_\mathfrak{p} = \{c_\mathfrak{p} || c_\mathfrak{p}(N_\mathfrak{p} - 1)| < \varepsilon\}$ □

Prop. (14.4.4.5)[Restricted Product Measure]. Let measures $d\alpha_\mathfrak{p}$ be given on $G_\mathfrak{p}$ that $\alpha_\mathfrak{p}(H_\mathfrak{p}) = 1$ for a.e. $\mathfrak{p}$, define a Haar measure on G as follows:

On G_S, $d\alpha_S = \prod_{\mathfrak{p}\in S} d\alpha_\mathfrak{p} \cdot d\alpha^S$, where α^S is the product measure on G^S.

Then these can define a functional a positive left-invariant functional I that $|I(f)| \le ||f||$ for any f that depends only on f.m. coordinates $\mathfrak{p} \in S$. Then Stone-Weierstrass theorem shows these functions are dense in $C(G)$, thus I can be uniquely extended to a functional on $C(G)$, and this defines a Haar measure on G by Riesz representation(11.10.1.10), denoted by $d\alpha = \prod'_\mathfrak{p} d\alpha_\mathfrak{p}$, called the **restricted product measure**. ⌟

Prop. (14.4.4.6). For a function f on $G = \prod'(G_\mathfrak{p}, H_\mathfrak{p})$ measurable, if either $f \ge 0$ or $f \in L^1(G)$, then

$$\int_G f(\mathfrak{a}) d\mathfrak{a} = \varinjlim_S \int_{G_S} f(\mathfrak{a}) d\mathfrak{a}$$

as a net limit. ⌟

Proof: The second case follows from the first case, as $\int_G f = \varinjlim_{B \text{ compact}} \int_B f$ by monotone convergence theorem, and any B compact is contained in some G_S(14.4.4.2). □

Cor. (14.4.4.7). If $f(\mathfrak{a}) = \prod_\mathfrak{p} f_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})$, where $f_\mathfrak{p} \in L_1(G_\mathfrak{p})$ and $f_\mathfrak{p} = \chi_{H_\mathfrak{p}}$ a.e. p, then if

$$\prod_\mathfrak{p} \int_{G_\mathfrak{p}} |f_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})| d\mathfrak{a}_\mathfrak{p} < \infty,$$

then $f \in L^1(G)$, and

$$\int_G f(\mathfrak{a}) \mathrm{d}\mathfrak{a} = \prod_\mathfrak{p} (\int f_\mathfrak{p}(\mathfrak{a}_\mathfrak{p}) \mathrm{d}\mathfrak{a}_\mathfrak{p}).$$

⌟

Def. (14.4.4.8)[Dual Measure]. Notice if $f_\mathfrak{p} = \chi_{H_\mathfrak{p}}$, then

$$f_\mathfrak{p}^\vee(c_\mathfrak{p}) = \int_{H_\mathfrak{p}} \overline{c_\mathfrak{p}(\alpha_\mathfrak{p})} d\mathfrak{a}_\mathfrak{p} = d\mathfrak{a}_\mathfrak{p}(H_\mathfrak{p}) \chi_{H_\mathfrak{p}^\perp}(c_\mathfrak{p}).$$

So by Fourier transform(11.10.3.24), if $\mathrm{d}c_\mathfrak{p}$ is the dual measure on $G_\mathfrak{p}^\vee$, then $\chi_{H_\mathfrak{p}^\perp} = \mathrm{d}c_\mathfrak{p}(H_\mathfrak{p}^\perp) d\mathfrak{a}_\mathfrak{p}(H) \chi_{H_\mathfrak{p}^\perp}$, which means $\mathrm{d}c_\mathfrak{p}(H_\mathfrak{p}^\perp) = 1, a.e.\mathfrak{p}$, thus we can define a measure on $G^\vee$ as $dc = \prod' dc_\mathfrak{p}$.

Then $\mathrm{d}c$ is the measure on $\widehat{G}$ dual to $\mathrm{d}\mathfrak{a}$ on G. ⌟

Proof: The duality is by the lemma below(14.4.4.9), applied to both f and $\widehat{f}$. □

Lemma (14.4.4.9) [Fourier Transform on Product]. if $f_\mathfrak{p} \in B_1(G_\mathfrak{p})$ and $f_\mathfrak{p} = \chi_{H_\mathfrak{p}}$ a.e. $\mathfrak{p}$, then $f(\mathfrak{a}) = \prod f_\mathfrak{p}(\mathfrak{a}_\mathfrak{p}) \in B_1(G)$, and $f^\vee(c) = \prod f_\mathfrak{p}^\vee(c_\mathfrak{p})$. ⌟

Proof: For any character c, because
$$f(\mathfrak{a})\overline{c}(\mathfrak{a}) = \prod f_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})\overline{c}_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})$$
and every $f_\mathfrak{p}(\mathfrak{a}_\mathfrak{p})\overline{c}_\mathfrak{p}(\mathfrak{a}_\mathfrak{p}) \in L^1(G_\mathfrak{p})$. So(14.4.4.7) applies and shows the equations. Similarly, because $\widehat{f_\mathfrak{p}} = \chi_{H_\mathfrak{p}^\perp}$ a.e. $\mathfrak{p}$, we have $\widehat{f} \in L_1(\widehat{G})$, so $f(\mathfrak{a}) \in B_1(G)$. □

Adeles

Notation (14.4.4.10) [Adeles]. For $S \in \Sigma_F$, $\#S < \infty$,

- The **adele group**(adele=additive element) of F is defined to be $\mathbf{A}_F = \prod_v'(F_v, \mathcal{O}_v)$(14.4.4.1).
- $\mathbf{A}_{S,F} = \prod_{v\in S} F_v$.
- $\mathbf{A}_F^S = \prod_{v\notin S}'(F_v, \mathcal{O}_v)$, called the group of S**-adeles** of F.
- The **finite adeles** $\mathbf{A}_F^f = \mathbf{A}_F^{S_\infty} = \prod_{v\notin S_\infty}'(F_v, \mathcal{O}_v)$.
- The **infinite adeles** $\mathbf{A}_{F,\infty} = \mathbf{A}_{F,S_\infty} = \prod_{v\in S_\infty} F_v$.
- For $v \in \Sigma_F, x \in F_v$, let $[x]_\mathfrak{p}^\oplus$ be the image of x under the map $F_\mathfrak{p} \to A_F$.

⌟

Prop. (14.4.4.11) [Extension of Adeles]. If $L/F \in$ `GField` is separable, then
$$\mathbf{A}_F \otimes_F L \cong \mathbf{A}_L$$
by diagonal embedding. ⌟

Proof: $\mathbf{A}_K \otimes_F L \cong \prod_v'(F_v, \mathcal{O}_v \otimes_{\mathcal{O}_F} \mathcal{O}_L)$, because for any element $x \in L$, $|\mathrm{Nm}_{L/F}(x)|_v \neq 0$ for only f.m. v. And there are isomorphisms by diagonal maps.
$$F_v \otimes_F L \cong \prod_{w|v} L_w, \quad \mathcal{O}_v \otimes_{\mathcal{O}_F} \mathcal{O}_L \cong \prod_{w|v} \mathcal{O}_w (5.2.7.26).$$
□

Prop. (14.4.4.12) [K Cocompact in Adele]. F is discrete in $\mathbf{A}_F$ and $\mathbf{A}_F/F$ is compact. ⌟

Proof: Let ∞ be any prime, consider $U = \{\mathfrak{a} \in A_F | |a|_\infty < 1, |a|_v \leq 1\}$, then $U \cap K = 0$ by(14.4.4.16).

Now we show A_F/F is compact. By(14.4.4.11), it suffices to prove for $F = \mathbb{Q}$ or $\mathbb{F}_p(t)$. Let $U_\infty = \{x \in F_\infty | |x|_\infty \leq 1\}$, and Cf.[MIT notes, 22.12].**?** □

Lemma (14.4.4.13) [Strong Approximation for $\mathbb{G}_a$]. For any $S \neq \varnothing \in \Sigma_F$, strong approximation holds for S. In other words, the image of F is dense in $\mathbf{A}_F^S$, or equivalently, $FF_vU = \mathbf{A}_F$ for any non-empty open subset $U \subset \mathbf{A}_F^S$. ⌟

Remark (14.4.4.14). See(15.4.3.9) for more general strong approximation theorems. ⌟

Proof: Cf.[MIT notes, 22.14].**?** □

Ideles

Notation (14.4.4.15) [Ideles]. For $S \in \Sigma_F$, $\#S < \infty$,

- The **idele group**(idele=ideal element) of F is defined to be $\mathbf{I}_F = \prod'_v (F_v^\times, \mathcal{O}_{F_v}^*)$(14.4.4.1), which is set-theoretically just $\mathbf{A}_F^\times$. Notice the topology on $\mathbf{I}_K$ is stronger than the subspace topology induced from $\mathbf{A}_K$.
- The **ideal class group** $C_F = \mathbf{I}_F / F^\times$.
- $\mathbf{I}_F$ is naturally a valuation ring with valuation $|\cdot|$, called the **idelic norm**.
- $\mathbf{I}_F^1 \subset I_F$ is the subgroup consisting of elements of idelic norm 1, called the set of **unit ideles**.
- $\mathbf{I}_F^S = \prod_{\mathfrak{p}\in S} F_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\notin S} \mathcal{O}_{F,\mathfrak{p}}^*$, called the group of S-**ideles** of F.
- $\mathbf{I}_{F,S} = \prod_{v\in S} F_v^\times$.
- $F^S = \mathcal{O}_{F,S}^* = F^\times \cap \mathbf{I}_F^S$ is the set of S-units of F(5.2.7.10).
- The **finite ideles** $\mathbf{I}_F^f = \mathbf{I}_F^{\Sigma_F^\infty} = \prod'_{v\notin\Sigma^\infty} (F_v^\times, \mathcal{O}_v^*)$.
- The **infinite ideles** $\mathbf{I}_{F,\infty} = \mathbf{I}_{F,S_\infty} = \prod_{v\in S_\infty} F_v^\times$.
- For $v \in \Sigma_F, x \in F_v^\times$, let $[x]_v$ be the image of x under the map $F_v^\times \to \mathbf{I}_F$ or the map $F_\mathfrak{p}^\times \to \mathbf{A}_F$.

⌟

Prop. (14.4.4.16) [Product Formula]. If $\mathfrak{a} \in F^\times \subset \mathbf{I}_F$, then $|\mathfrak{a}|_F = 1$. In other words, $F^\times \subset \mathbf{I}_F^1$. ⌟

Proof: Consider the restricted product measure $d\mu$ on A_F, then clearly $d\mu(\mathfrak{a}x) = |\mathfrak{a}|d\mu(x)$, and multiplying by $\mathfrak{a}$ induces an isomorphism of $\mathbf{A}_F$, but preserves the counting measure on F. But A_F is compact(14.4.4.12) thus has finite volume, so $|\mathfrak{a}| = 1$. □

Prop. (14.4.4.17). If $F \in$ `FField`, the norm group $|\mathbf{I}_F|$ of the Adelic norm is $|\mathbf{I}_F| = q^\mathbb{Z}$, where $q = \#F_0$ and F_0 is the maximal finite field contained in F. ⌟

Proof: This is because in this case, F corresponds to smooth curve over F_0**?**. Then by Weil conjecture(21.2.3.4), there exists a point of F_0 with residue order q^n for any n large. Then their quotient gives q. □

Prop. (14.4.4.18) [Splitting of $\mathbf{I}_F$].

- If $F \in$ `NField`, take $v \in \Sigma_F^\infty$, then the exact sequence $1 \to I_F^1 \to I_F \xrightarrow{v} \mathbb{R}_+ \to 1$ splits, so there are a non-canonical isomorphisms
$$I_F \cong I_F^1 \times \mathbb{R}_+, \quad I_F/F^\times \cong I_F^1/F^\times \times \mathbb{R}_+.$$
- If $F \in$ `FField`, take $v \in \Sigma_F$, then for some $q = (\mathrm{char}\, k)^r$, the exact sequence $1 \to \mathbf{I}_F^1 \to \mathbf{I}_F \xrightarrow{v} q^\mathbb{Z} \to 1$ splits, so there are a non-canonical isomorphisms
$$I_F \cong \mathbf{I}_F^1 \times q^\mathbb{Z}, \quad \mathbf{I}_F/F^\times \cong I_F^1/F^\times \times q^\mathbb{Z}.$$

⌟

Lemma (14.4.4.19). $\mathbf{I}_F^1$ is closed in $\mathbf{A}_F$, and the subspace topologies from $\mathbf{A}_F$ and $\mathbf{I}_F$ are the same on $\mathbf{I}_F^1$. ⌟

Proof: **?** □

Lemma (14.4.4.20) [Blichfeldt-Minkowski]. For $F \in$ `GField`, there exists $C > 0$ s.t. for any $x \in \mathbf{I}_F$ s.t. $|x|_F \geq C$, let

$$W(x) = \{y \in \mathbf{I}_F : |y_v|_v \leq |x_v|_v, \forall v \in \Sigma_F\}.$$

Then $W(x) \cap F^\times \neq \varnothing$. ⌟

Proof: **?** □

Prop. (14.4.4.21) [$F^\times$ Cocompact in $\mathbf{I}_F^1$]. $F^\times$ is discrete in $\mathbf{I}_F$, and $\mathbf{I}_F^1/F^\times$ is compact. Thus $C_F = \mathbf{I}_F/F^\times$ is Hausdorff and locally compact. ⌟

Proof: $F^\times$ is discrete in $\mathbf{I}_F$ because it is already discrete in $\mathbf{A}_F$(14.4.4.12). By(14.4.4.19), use Minkowski(14.4.4.20), it suffices to show that for $||x||_F \geq C$, $W(x) \cap I_F^1 \to I_F^1/F^\times$ is surjective: If $y \in I_F^1$, then $||x/y|| = ||x|| \geq C$, thus there exists $z \in K^\times \cap W(x/y)$, thus $zy \in W(x)$, and y is in the image of $W(x) \cap I_F^1$. □

Prop. (14.4.4.22). For $L/F \in$ `GField`, $\mathbf{I}_F \subset \mathbf{I}_L$, and $\mathbf{I}_L^G = \mathbf{I}_K$, this is be the diagonal inclusion to all the primes above a given prime, and the action is by $(\sigma\mathfrak{a})_\mathfrak{P} = \sigma\mathfrak{a}_{\sigma^{-1}\mathfrak{P}}$. This induces an inclusion $C_K \subset C_L$ and $C_L^G = C_K$. The last assertion uses long exact sequence and $H^1(G, L^*) = 0$. ⌟

Lemma (14.4.4.23). The map $\mathbf{I}_F \to \mathbf{A}_F \times \mathbf{A}_F : x \mapsto (x, x^{-1})$ is a homeomorphism of $\mathbf{I}_F$ onto a closed subspace of $\mathbf{A}_F \times \mathbf{A}_F$. ⌟

Proof: Compare their topological basis. □

Prop. (14.4.4.24) [Idele Groups and Extensions]. For an extension of global fields L/F,

- the diagonal embedding $\mathbf{A}_F \to \mathbf{A}_L$ induces a closed embedding, and also a closed embedding $\mathbf{I}_F \to \mathbf{I}_L$ by(14.4.4.23), thus also a closed embedding $I_F/F^\times \to I_L/L^\times$.
- A_L is a finite A_K-module, thus there is a norm map $\mathrm{Nm}_{L/K} : A_L \to A_F$, which restricts to $\mathrm{Nm}_{L/K} : \mathbf{I}_L \to \mathbf{I}_F$, which is compatible with $\mathrm{Nm}_{L/K} : L^\times \to K^\times$, thus inducing a map $\mathrm{Nm}_{L/K} : C_L \to C_F$. Then this map is continuous, open and proper.
- $[n] : C_F \to C_F$ is continuous and proper.

⌟

Proof: 2: It is continuous because it is compatible with the local norms $\mathrm{Nm}_{L_\mathfrak{P}/F_\mathfrak{p}}$, and $\mathrm{Nm}_{L_\mathfrak{P}/F_\mathfrak{p}}^{-1}(\mathcal{O}_{F,\mathfrak{p}}^\times) = \mathcal{O}_{L,\mathfrak{P}}^\times$. To show it is open, use the fact the local norms are open and for unramified places $\mathrm{Nm}_{L_\mathfrak{P}/F_\mathfrak{p}} \mathcal{O}_{L,\mathfrak{P}} = \mathcal{O}_{F,\mathfrak{p}}$(14.2.3.16)(14.6.2.5). To show it is proper, use the splitting $C_F \cong \mathbf{I}_F^1/F^\times \times q^\mathbb{Z}$(14.4.4.18) and the fact $I_F^1/F^\times$ is proper(14.4.4.21).

3: Use the splitting(14.4.4.18). □

<u>C_F</u>

Def. (14.4.4.25) [Hecke Character]. A **Hecke character** over F is a character of C_F. ⌟

Def. (14.4.4.26) [Unramified Places]. Let χ be a Hecke character of C_F, then for a.e. $v \in \Sigma_F^{\mathrm{fin}}$, the conductor of χ_v is $\mathcal{O}_v^*$. For these v, χ is said to be **unramified** at v. ⌟

Prop. (14.4.4.27). Let $p \in \mathfrak{P}, F \in p$-`FField`, and $\ell \in \mathbf{P}\backslash p, E \in \ell$-`NField`, then any continuous homomorphism $\chi : C_F \to \mathcal{O}_E^*$ that is unramified outside a finite set of places is of the form $\chi = \chi_1 \cdot c^{\deg(\cdot)}$, where $\chi_1 : C_F \to \mathcal{O}_E^*$ is of finite order and $c \in \mathcal{O}_E^*$. ⌟

Proof: Let $\sigma \in C_F^{\mathrm{ab}}$ s.t. $\deg(\sigma) = 1$, let $c = \chi(\sigma)$, and $\chi_1 = \chi \cdot c^{-\deg(\cdot)}$, then $\chi_1(C_F) = \chi_1(I_F)$. But as $\#\operatorname{Cl}(F) < \infty$, by(14.6.4.7), it suffices to show that $\chi_1(F^\times U^{\mathbb{1}}/F^\times)$ is finite. Then it suffices to show that $\#\chi(U^{\mathbb{1}}) < \infty$. But if χ is unramified outside a finite set S of places, then it suffices to show that $\#\chi(\prod_{v\in S}\mathcal{O}_v^*) < \infty$. But this is because $\prod_{v\in S}\mathcal{O}_v^*$ has a pro-p-group of finite index and $\mathcal{O}_E^*$ has a pro-ℓ-group of finite index. □

Def. (14.4.4.28)[Norm Groups]. For an extension of global fields L/F, let $\mathcal{N}_{L/F} = \mathrm{Nm}_{L/F} C_L$, called the **norm group** of L/F. ⌟

Prop. (14.4.4.29) [Connected Component of identity of C_F]. If F is a number field, let $I^0_{F,\infty} \cong \mathbb{R}_+^{r_1} \times (\mathbb{C}^\times)^{r_2}$ be the connected component of identity of $I_{F,\infty}$, $D_F \subset C_F$ the closure of $I^0_{F,\infty} \subset C_F$, then

- D_F is the connected component of identity of C_F.
- $D_F = \cap_{n\in\mathbb{Z}_+} C_F^n$ is the group of divisible elements of C_F.
- C_F/D_F is a profinite group.(which will be isomorphic to Gal_F^{ab}, as we will see in(14.6.3.27)).

⌟

Proof: $I^0_{F,\infty}$ is divisible, thus so does its image in C_F. Then D_F is also divisible as $[n] : C_F \to C_F$ is continuous and proper(14.4.4.24).

Consider the map $\prod_{v\in\Sigma_F^{\mathrm{fin}}}\mathcal{O}^*_{F,v} \to C_F/D_F$, its cokernel is finite because $C_F/\prod_{v\in\Sigma_F^{\mathrm{fin}}} I_{F,\infty} \cong \operatorname{Cl}(\mathcal{O}_F)$ is finite and $I_{F,\infty}/I^0_{F,\infty}$ is finite. But $\prod_{v\in\Sigma_F^{\mathrm{fin}}}\mathcal{O}^*_{F,v}$ is a profinite group, thus C_F/D_F is also a profinite group.

To show $D_F = C_F^0$, firstly $C_F^0 \subset D_F$ by the fact C_F/D_F is connected thus totally disconnected, and the reverse is true because D_F is connected.

To show $D_F = \cap_{n\in\mathbb{Z}_+} C_F^n$, notice any divisible element is in D_F as a profinite group C_F/D_F doesn't contain non-trivial divisible elements. □

Thm. (14.4.4.30) [Class Numbers and Unit Theorems]. If $\Sigma_F^\infty \subset S \subset \Sigma_F$,

1. The S-class group $\operatorname{Cl}(\mathcal{O}_{F,S}) \cong \mathbf{I}_F/F^\times\mathbf{I}_F^S$ is finite. In particular, $\mathbf{I}_\mathbb{Q} = \mathbb{Q}^\times \times \mathbb{R}_+^\times \times \prod_{p\in\mathbf{P}}\mathbb{Z}_p^\times$.
2. If $x \in F^\times$ and $|x|_v = 1$ for any $v \in \Sigma_F$, then $x \in \mu(F)$.
3. The S-unit group(5.2.7.10) $\mathcal{O}^*_{F,S} \cong \mu(F) \times \mathbb{Z}^{\#S-1}$.

⌟

Proof: 1: Let $(\mathbf{I}_F^S)^1 = \mathbf{I}_F^1 \cap I_F^S$. As $\mathcal{O}^*_{F,S} = F^\times \cap \mathbf{I}_F^S$, there is an exact sequence

$$1 \to (I_F^S)^1/F^S \cong F^\times(I_F^S)^1/F^\times \to I_F^1/F^\times \to (I_F^S)^1/F^\times(I_F^S)^1 \to 1.$$

The first term is an open subset, and $\mathbf{I}_F^1/F^\times$ is compact by(14.4.4.21), thus $(I_F^S)^1/F^\times(I_F^S)^1$ is finite and $(I_F^S)^1/F^S$ is compact. There is also an exact sequence

$$1 \to (I_F^S)^1/F^\times(I_F^S)^1 \to I_F^S/F^\times I_F^S \cong \operatorname{Cl}(\mathcal{O}_{F,S}) \to ||I_F||_F/||I_F^S||_F \to 1$$

and $||I_F||_F/||I_F^S||_F$ is always finite, so $\#\operatorname{Cl}(\mathcal{O}_{F,S}) < \infty$.

2, 3: Consider the regulator map

$$\mathrm{Reg}^S : \prod_{v\in S} F_v^\times \to \mathbb{R}^{\#S} : (x_v) \mapsto (-\log|x_v|_v).$$

Then this map restricted to F^S has image a discrete subset of the hyperplane $H=\{\sum x_i=0\}$. In fact the image is a full lattice in H: let n_1 be the number of infinite places in S and n_2 the number of finite places in S, then $\mathrm{Reg}^S((\prod_{v\in S}F_v^\times)^1)\cong\mathbb{R}^{n_1-1}\times\mathbb{Z}^{n_2}$ if $n_1>0$ and $\mathbb{Z}^{\#S-1}$ if $n_1=0$. Then notice $(\prod_{v\in S}F_v)^1/F^S$ is finite, which is true as $(\mathbf{I}_F^S)^1/F^S$ is compact, so The image of F^S is a full lattice of H.

Also notice if x is in the kernel of Reg^S, then $|x|_v=1$ for any $v\in\Sigma_F$, so $\{x^n|n\in\mathbb{Z}\}$ is a bounded subset in the lattice $\prod_{v\in S}F_v^\times$, but it is also contained in the discrete subset F^S, thus it a finite subset, so x is a root of unity. □

Cor. (14.4.4.31). If $S\subset\Sigma_F$ is sufficiently large, then $\mathbf{I}_F=\mathbf{I}_F^S\cdot F^\times$ hence $C_F=\mathbf{I}_F^S.F^\times/F^\times$. ⌟

Proof: The ideal class group is finite, hence we can find a finite set of representative for it. Only finite set of primes are involved in it, thus we let S contain all these primes and infinite primes, then for any $\mathfrak{a}$, $\prod_{\mathfrak{p}\nmid\infty}a_{\mathfrak{p}}=A_i\cdot(x)$, and $A_i\in I_K^S$, hence $\mathfrak{a}\in I_K^S\cdot K^*$. □

Cor. (14.4.4.32) [Dirichlet Characters and Hecke Characters for $\mathbb{Q}$]. Hecke characters of $\mathbb{Q}$ are exactly of the form $\chi(x)=\chi_1(x)|x|^\lambda$ for some $\lambda\in i\mathbb{R}$, where χ_1 a Hecke character of finite order corresponding to a primitive Dirichlet character χ_0 via(14.4.4.30).

To transit between these two, we need to use $\mathbb{Q}^\times$ to "clear the denominators". For example, for p prime to the conductor of χ_0, $\chi_1(p_v)=\chi_0(p)$. ⌟

5 Fourier Analysis on Adeles

Main references are [Poo15], [R-V99] and [Tat65].

Local Notations

Def. (14.4.5.1) [Normalized Valuations]. Let $\mathrm{d}\mu$ a Haar measure on K, let the valuation on K be given by $d\mu(\alpha\xi)=|\alpha|d\mu(\xi)$. Then for $k\in K$,

$$|k|=\begin{cases}|k| & K=\mathbb{R}\\ |k|^2 & K=\mathbb{C}\\ \frac{1}{||\mathfrak{p}||^{v(k)}} & K\in p\text{-}\mathtt{LField}\end{cases}.$$

⌟

Proof: If $K=\mathbb{R},\mathbb{C}$, this is routine calculation. If K is non-Archimedean , then by the translation invariance of μ, $\mu(\alpha\mathcal{O})=\frac{\mu(\mathcal{O})}{N(\alpha)}=|\alpha|\mu(\mathcal{O})$. □

Def. (14.4.5.2) [Unramified Quasi-Character]. The multiplicative group $K^\times$ is also a locally compact group. For a quasi-character χ of $K^\times$, it is called **unramified** iff $\chi(\mathcal{O}_K^*)=1$.

An unramified quasi-character on $K^\times$ is all of the form $|\cdot|^s$ for $s\in\mathbb{C}$. ⌟

Proof: An unramified quasi-character is equivalent to a continuous group homomorphism from $\mathrm{val}(K^\times)\to\mathbb{Z}$. But $\mathrm{val}(K^\times)$ must be isomorphic to $\mathbb{Z}$ or $\mathbb{R}$, so the assertion follows from(11.10.3.3). □

Lemma (14.4.5.3) [Canonical Character of Local Fields]. Consider k the closure of the base field of K, which is $\mathbb{R}, \mathbb{Q}_p$ or $\mathbb{F}_p((t))$ by Ostrowski(11.2.3.18). Now let

$$\lambda(x) = \begin{cases} x (\mathrm{mod}\ 1) & k = \mathbb{R} \\ \text{a rational number } \lambda(x) \text{ that } \lambda(x) - x \in \mathbb{Z}_p \text{ in } \mathbb{Q}/\mathbb{Z} & k = \mathbb{Q}_p \\ a_{-1}/p = \mathrm{res}(x)/p & k = \mathbb{F}_p((t)) \end{cases}$$

Then λ is a continuous additive function on k. Now let

$$\Lambda(x) = \begin{cases} \lambda(\mathrm{tr}_{K/k}(x)) & \text{number field case} \\ \lambda(\mathrm{tr}_{K_v/k_v}(x\omega_v)) & \text{function field case, where } \omega \text{ is a chosen global meromorphic form on } X. \end{cases}$$

And $X(x) = e^{2\pi i \Lambda(x)}$. Notice that this is just a rigorous definition of the character $e^{2\pi \mathrm{i}\, \mathrm{tr}_{K/k}(x)}$. ⌟

Cor. (14.4.5.4). $F(\eta) = e^{2\pi \mathrm{i}\, \Lambda(\eta\xi)}$ is trivial on $\mathcal{O}_K$ is equivalent to $\xi \in \mathfrak{d}^{-1}$, where $\mathfrak{d} = \mathfrak{d}_{K/k}$. In other words, adopting the isomorphism of(11.10.3.35), $\mathcal{O}^\perp = \mathfrak{d}^{-1}, (\mathfrak{d}^{-1})^\perp = \mathcal{O}$. ⌟

Proof: Because $\Lambda(\eta\mathcal{O}) = 0$ iff $\mathrm{tr}_{K/k}(\eta\mathcal{O}) \subset \mathcal{O}_k$, which is equivalent to $\eta \in \delta^{-1}$. □

Prop. (14.4.5.5) [Canonical Self-Adjoint Haar Measures]. We can calculate the self-adjoint Haar measure w.r.t. the canonical character on K^+(14.4.5.3) as follows:

$$d\mu = \begin{cases} \mathrm{dm} & K = \mathbb{R} \\ 2\,\mathrm{dm} & K = \mathbb{C} \\ \text{the measure that } \mu(\mathcal{O}) = \frac{1}{||\mathfrak{d}||^{1/2}} & \text{others} \end{cases}$$

⌟

Proof: We only calculate for the p-adic fields**?**.

Let $f = \mathbb{1}_{\mathcal{O}}$, then

$$\widehat{f}(\eta) = \int_{\mathcal{O}} e^{-2\pi i \Lambda(\xi\eta)} d\mu(\xi) = \begin{cases} \mu(\mathcal{O}) & \eta \in \mathfrak{d}^{-1} \\ 0 & \text{otherwise} \end{cases} = \mu(\mathcal{O}) \mathbb{1}_{\mathfrak{d}^{-1}}(\eta)$$

By(14.4.5.4) and(11.10.1.14). So

$$I_{\mathcal{O}}(\xi) = \int_G \widehat{f}(F(\eta))(\xi, F(\eta)) d\mu(\eta) = \int_{\delta^{-1}} \mu(\mathcal{O}) e^{2\pi i \Lambda(\eta\xi)} d\mu(\eta) = \mu(\mathcal{O})\mu(\delta^{-1}) I_{\mathcal{O}}(\eta).$$

So $\mu(\mathcal{O})\mu(\delta^{-1}) = N(\delta)\mu(\mathcal{O})^2 = 1$, which shows the desired result. □

Remark (14.4.5.6). In fact, if we use other characters ψ, then $\mu(\mathcal{O}_K) = ||\mathfrak{c}_\psi||^{1/2}$. ⌟

Cor. (14.4.5.7) [Quasi-Character of $K^\times$]. There is a continuous morphism from $K^\times \to \mathcal{O}_K^*$: $\widetilde{\alpha} = \alpha/\pi^{v(\alpha)}$ when α is non-Archimedean or $\widetilde{\alpha} = \alpha/|\alpha|$ if K is Archimedean. So any quasi-character c is of the form $c(\alpha) = c(\widetilde{\alpha})$ times an unramified quasi-character, which is of the form $|\cdot|^s$, where $\mathrm{Re}(s)$ is called the **exponent** of c. Now $\mathcal{O}_K^*$ is a compact group, so continuous quasi-characters $\widetilde{c}$ on it must be a character. ⌟

Def. (14.4.5.8) [Haar Measure on $K^\times$]. Notice that if $g(\alpha)\in C_c(K^\times)$, then $\frac{g(\alpha)}{|\alpha|}\in C_c(K^+\backslash 0)$, so if we define $\Phi(g)=\int_{K^+\backslash\{0\}} g(\xi)|\xi|^{-1}d\xi$, then

$$\Phi(ag)=\int_{K^+\backslash 0} g(a\xi)|a\xi|^{-1}|a|d\xi=\int_{K^+\backslash 0} g(a\xi)|a\xi|^{-1}da\xi=\Phi(g).$$

By(14.4.5.1). So By Riesz representation, there is a Haar measure $d_1^\times\alpha$ on $K^\times$ that $\int_{K^\times} g(\alpha)d_1^\times\alpha=\int_{K^+\backslash 0} g(\xi)|\xi|^{-1}d\xi$, for any $g\in C_c(K^\times)$.

But when K is non-Archimedean, renormalize $d^\times\alpha=(1-\frac{1}{N\mathfrak{p}})^{-1}d_1^\times\alpha$. ⌟

Remark (14.4.5.9). The reason behind this normalization is when $d\mu$ is the canonical measure(14.4.5.5), we want to make $\mathrm{d}^\times\alpha(\mathcal{O}^*)=||\mathfrak{d}||^{-1/2}$:

$$\int_{\mathcal{O}\backslash 0} d\xi=\sum_{k=0}^\infty\int_{\pi^k\mathcal{O}^*} d\xi=(1+\frac{1}{N\mathfrak{p}}+\frac{1}{N\mathfrak{p}^2}+\ldots)\int_{\mathcal{O}^*} d\xi=\frac{1}{1-\frac{1}{N\mathfrak{p}}}\int_{\mathcal{O}^*} d\xi$$

so

$$\int_{\mathcal{O}^*} d_1^\times\alpha=\int_{\mathcal{O}^*}|\xi|^{-1}d\xi=\frac{||\mathfrak{p}||-1}{||\mathfrak{p}||}\int_{\mathcal{O}\backslash 0} d\xi=\frac{||\mathfrak{p}||-1}{||\mathfrak{p}||}||\mathfrak{d}||^{-1/2}\text{(14.4.5.5)}$$

⌟

Def. (14.4.5.10) [Schwartz-Bruhat Function]. Define the set $\mathcal{S}(K)$ of **Schwartz-Bruhat function** on K as Schwartz functions on K if $F=\mathbb{R},\mathbb{C}$(11.8.2.1) and locally constant functions with compact support if $K\in p$-`LField`. ⌟

Prop. (14.4.5.11) [Local Schwarz Functions]. The space $\mathcal{S}(K)$ of Schwartz functions satisfy the following properties: If $f\in\mathcal{S}(K)$,

- $f,f^\vee\in L^1(K^+)$.
- $f(\alpha)|\alpha|^\sigma, f^\vee(\alpha)|\alpha|^\sigma\in L^1(K^\times)$ for $\sigma>0$.
- $f^\vee\in\mathcal{S}(K)$ too.

⌟

Proof: 3: p-adic case: Let $\mathfrak{p}^n$ be the conductor of ψ, then the Fourier transform of $\chi_{\mathfrak{p}^{-k}}$ is $V(\mathfrak{p}^{-k})\chi_{\mathfrak{p}^{n+k}}$. Then for k large, $\chi_{\mathfrak{p}^{-k}}v=V(\mathfrak{p}^{-k})V(\mathfrak{p}^{n+k})v$, thus $v\in C_c^\infty(F)$.

Archimedean case:(11.11.2.5). □

Global notations

Notation (14.4.5.12).

- There are natural Haar measures $\mathrm{d}\mu_K,\mathrm{d}^\times\mu_K$ on $\mathbf{A}_F$ and $\mathbf{I}_F$ defined by(14.4.4.5) and(14.4.5.5)(14.4.5.8). They satisfy $\mathrm{d}^\times\mu_K=\frac{1}{|-|_K}\mathrm{d}\mu_K$.
- Let $\mathfrak{d}=\mathfrak{d}_{F/\mathbb{Q}}$ when $F\in$ `NField`, or $\mathfrak{d}=\{x|\operatorname{tr}(\operatorname{res}(x\mathcal{O}))=0\}^{-1}$ when $F\in$ `FField`.
- Fix $\psi=\prod_v\psi_v$ an additive character of $\mathbf{A}_F/F$, then

⌟

Def. (14.4.5.13) [Global Fourier Transform]. (11.10.3.35) shows ψ induces a canonical isomorphism

$$\mathbf{A}_F\cong\mathbf{A}_F^\vee:\eta\mapsto(\xi\to\psi(\eta\xi)),$$

and we choose the corresponding self-dual Haar measure $d\mu$, then the Fourier transform and inversion formula on $\mathbf{A}_F$ is then written as:

$$f^\vee(y)=\int_{\mathbf{A}_F} f(x)\overline{\psi(xy)}dx,\quad f(x)=\int_{\mathbf{A}_F} f^\vee(y)\psi(xy)dy.$$

In fact $dx=\prod x_\mathfrak{p}$ is the restricted product measure on $\mathbf{A}_F$(14.4.4.5), where $dx_\mathfrak{p}$ is the self-dual measure w.r.t ψ_p in(14.4.5.5), then dx is the self-dual Haar measure w.r.t the global canonical character ψ by(14.4.4.8), called the **Tamagawa measure** on $\mathbf{A}_F$. ⌟

Def. (14.4.5.14) [Global Schwartz-Bruhat Functions]. For a global field F, the set $\mathcal{S}(F)$ of global **Schwartz-Bruhat functions** is defined to be

$$\mathcal{S}(F)=\bigotimes_{v\in\Sigma_F}{}' \mathcal{S}(F_v)(3.6.4.13).$$

⌟

Prop. (14.4.5.15) [Schwartz-Bruhat Functions]. A Schwartz-Bruhat function $f\in\mathcal{S}(\mathbf{A}_F)$(14.4.5.14) satisfies:

- $f(x)\in L^1(A), f^\vee(x)\in L^1(\mathbf{A}_F)$ and $f,f^\vee$ is continuous.
- $\sum_{\xi\in K} f(\mathfrak{a}(x+\xi))$ and $\sum_{\xi\in K}\widehat{f}(\mathfrak{a}(x+\xi))$ converges uniformly absolutely on compact sets of A.
- $f(\mathfrak{a})|\mathfrak{a}|^\sigma,\widehat{f}(\mathfrak{a})|\mathfrak{a}|^\sigma\in L^1(I_F)$ for $\sigma>1$.

⌟

Proof: $1,2$ is the same as in(14.4.5.23), for 3: $\int_{\mathbf{I}_F}|f||\mathfrak{a}|^\sigma d\mathfrak{a}=\prod_\mathfrak{p}\int_{F_\mathfrak{p}^\times}|f_\mathfrak{p}||\mathfrak{a}|^\sigma d\mathfrak{a}_\mathfrak{p}$, and for a.e. $\mathfrak{p}$,

$$\int_{F_\mathfrak{p}^\times}|f_\mathfrak{p}||\mathfrak{a}|^\sigma d\mathfrak{a}_\mathfrak{p}=\int_{\mathcal{O}_\mathfrak{p}^\times}|\mathfrak{a}_\mathfrak{p}|_\mathfrak{p}^\sigma d\mathfrak{a}_\mathfrak{p}=\frac{1}{1-\frac{1}{||\mathfrak{p}||^\sigma}}\int_{\mathcal{O}_\mathfrak{p}^*}d\mathfrak{a}_\mathfrak{p}=\frac{1}{1-\frac{1}{||\mathfrak{p}||^\sigma}}.$$

Thus the global integral converges by comparison with the Dedekind Zeta function(21.3.2.1). □

Def. (14.4.5.16) [Global Canonical Character]. Define the **global canonical character**

$$X:\mathbf{A}_F\to\mathbb{C}^\times:x\mapsto e^{2\pi\,\mathrm{i}\,\Lambda(x)},\quad \Lambda(x)=\sum_{\mathfrak{p}\in\Sigma_F}\Lambda_\mathfrak{p}(x_\mathfrak{p})(14.4.5.3).$$

Notice this is definable because $x_\mathfrak{p}\in\mathcal{O}_\mathfrak{p}$ a.e. $\mathfrak{p}$, thus $\Lambda_\mathfrak{p}(x_\mathfrak{p})=1$ a.e..

Then $X(F)=1$. ⌟

Proof: In the number field case,

$$\Lambda(\xi)=\sum_p\sum_{\mathfrak{p}|p}\lambda_p(\mathrm{tr}_{\mathfrak{p}/p}(\xi))=\sum_p\lambda_p(\mathrm{tr}_{K/\mathbb{Q}}(\xi))$$

so to show λ is an integer, it suffices to show $\Lambda(a)$ is a q-adic integer for any q and any $a\in\mathbb{Q}$, but for this, notice

$$\sum\lambda_\mathfrak{p}(x)=\sum_{p\neq q,\infty}\lambda_p(x)+\lambda_q(x)-x$$

is a q-adic integer, by definition(14.4.5.3).

In the function field case, this follows from the fact that the sum of residues of a meromorphic 1-form is 0**?**. □

Prop. (14.4.5.17). $F^\perp = F$, i.e. $X(xy) = 0, \forall y \in F \iff x \in K$. ⌟

Proof: Because $K^\perp \cong \widehat{A/K}$ and A/K is compact(14.4.4.12), $K^\perp$ is discrete(11.10.3.7) and contains K. So $K^\perp/K$ is discrete hence finite in A/K. But $K^\perp$ is clearly a vector space over K, thus $K^\perp = K$ must be true, because $|K| = \infty$. □

Cor. (14.4.5.18). By(11.10.3.35) and(14.4.5.17), any non-trivial character on A_F/F is of the form $\mathfrak{a} \mapsto X(k\mathfrak{a})$ for some $k \in K$.

In particular, for any such character ψ, ψ_v is non-trivial. ⌟

Def. (14.4.5.19) [Unramified Places]. Let χ be a Hecke character of F, then $v \in \Sigma_F$ is called **unramified** if $v \in \Sigma_F^{\text{fin}}$, $\mathfrak{d}_v = 1$, $\mathfrak{c}(\psi_v) = \mathcal{O}_v$, χ_v is unramified(14.4.5.2). Notice a.e. place v is unramified. ⌟

Proof: To show that for any unramified character ψ, the conductor of φ_v is $\mathcal{O}_v$, consider the canonical character X defined(14.4.5.16), it can be verified the conductor of X_v is $\mathcal{O}_v$ for a.e. v, and ψ must be of the form $\psi(x) = X(ax)$ for some $a \in K$ by(14.4.5.13) and(14.4.5.17), thus this is also true for ψ. □

Prop. (14.4.5.20).

$$V(\mathbf{I}_F^1/F^\times) = \frac{2^{r_1}(2\pi)^{r_2}}{w_F\sqrt{|d_F|}} h_F \operatorname{Reg}(F)$$

where $w_F = \#F_{\text{tor}}^\times$, h_F is the class number, and $\operatorname{Reg}(F)$ is the regulator(14.4.1.27). ⌟

Proof: Cf.[Tate Thesis, P337] or[GTM186, P281].**?** □

Lemma (14.4.5.21) [Poisson Formula]. If $F \in L^1(\mathbf{A}_F)$ and $\sum_{\xi\in F} |f^\vee(\xi)| < \infty$, then in the self-dual Haar measure

$$\sum_{\xi\in F} f^\vee(\xi) = \sum_{\xi\in F} f(\xi).$$

and $V(\mathbf{A}_F/F) = 1$. ⌟

Proof: By(14.4.5.17), this is a special case of(11.10.3.31). In fact, we know it is true for a constant $V(\mathbf{A}_F/F)$, but it is symmetric, so $V(\mathbf{A}_F/F)^2 = 1$. □

Prop. (14.4.5.22) [Riemann-Roch]. If $f(\mathfrak{a}x) \in L^1(\mathbf{A}_F)$ and $\sum_{\xi\in F} |\widehat{f}(\mathfrak{a}\xi)| < \infty$ for any idele $\mathfrak{a} \in I_F$, then for any $\mathfrak{a} \in \mathbf{I}_F$,

$$\frac{1}{|\mathfrak{a}|}\sum_{\xi\in F} \widehat{f}(\frac{\xi}{\mathfrak{a}}) = \sum_{\xi\in F} f(\mathfrak{a}\xi).$$

⌟

Proof: Consider $g(x) = f(\mathfrak{a}x)$, then

$$g^\vee(x) = \int_{\mathbf{A}_F} f(\mathfrak{a}\eta)e^{-2\pi i\lambda(x\eta)}d\eta = \frac{1}{|\mathfrak{a}|}\int_{\mathbf{A}_F} f(\eta)e^{-2\pi i\Lambda(x\eta/\mathfrak{a})}d\eta = \frac{1}{|\mathfrak{a}|} f^\vee(x/\mathfrak{a}).$$

Then apply Poisson formula(14.4.5.21) to g. □

Prop. (14.4.5.23). Schwartz-Bruhat functions(14.4.5.14) satisfy the condition in(14.4.5.22). ⌟

Proof: $\int_A |f| = \prod_v \int_{F_v} \int |f_v| dx_v < \infty$, noticing(14.4.5.5) and $N(\mathfrak{d}_v) = 1$ for a.e. v. And for any Schwartz function f and any x, the set of k that $f_v(x_v + k_v) \neq 0$ is v-bounded for v non-Archimedean and $|k|_v \leq 1$ a.e., so in the function case, these k are finite because F is discrete in $\mathbf{A}_F$.

And in the number field case, these k is contained in some fractional ideal I, but I is then a lattice in F_∞ by Minkowski theory, so

$$\sum_{\xi \in K} |f(x+\xi)| \leq C \sum_{x \in K} | \prod_{\mathfrak{p} \in S_\infty} |f_{\mathfrak{p}}(x+\xi)|$$

but $f_{\mathfrak{p}}$ is an Archimedean Schwartz function, thus this is absolutely convergent.

Now we showed that $\int_{\xi \in F} f^\vee(\xi) < \infty$, because $f^\vee \in \mathcal{S}(\mathbf{A}_F)$, by(14.4.5.11). □

Prop. (14.4.5.24) [True Riemann-Roch For Function Fields]. Cf.[Fourier Analysis on Number Fields, P267].**?** ⌟

14.5 Quadratic Forms over Fields

Basic references are [Lam05], [Quadratic Forms Clark] and [Algebraic and Geometric Theory of Quadratic Forms].

All fields K in this section has char$\neq 2$.

1 Quadratic Forms

This subsection should be regarded as a continuation of Bilinear & Hermitian Forms. In fact, must materials in this subsection are trivial facts.

Def. (14.5.1.1). Given a field K of char$\neq 2$, a **quadratic form** over K is a bilinear form on K^n for some K. It is represented by a symmetric matrix.

The reason that char$K \neq 2$ is because only in this case, a quadratic form q is equivalent to a symmetric bilinear form B, and I will use this equivalence freely.

The determinant det is a function from the set of quadratic forms to $K^\times/(K^\times)^2$ that is invariant under congruence. ⌟

Def. (14.5.1.2) [Quadratically Closed]. A field is called **quadratically closed** iff $(K^\times)^2 = K^\times$, or equivalently K has no quadratic field extensions. ⌟

Def. (14.5.1.3). The category of **quadratic spaces** is a category with objects as finite dimensional spaces with a quadratic form, and its morphisms are isometric embeddings. ⌟

Def. (14.5.1.4) [Universal Quadratic Form]. For a quadratic form A, let $D_F(A)$ be the set of elements representable by A. A **universal quadratic form** is a quadratic form that represents every element of K^*. ⌟

Prop. (14.5.1.5). If every binary quadratic form over K is universal, then any two non-degenerate quadratic forms over K are isomorphic iff they have the same rank and determinant. ⌟

Proof: This is because $\langle a, b\rangle \cong \langle 1, ab\rangle$ and then use induction. □

<u>**Non-Degeneracy**</u>

Def. (14.5.1.6) [Non-degeneracy]. A quadratic space is called **non-degenerate** if $v \mapsto B(v,\cdot)$ is an isomorphism from V to V^*. Notice if $\dim V = \infty$, this cannot happen, because $\dim V^* > \dim V$(3.5.3.9). And in case $\dim V < \infty$, $\dim V = \dim V^*$, so it suffices to show $v \mapsto B(v,\cdot)$ is injective, i.e. if $v \neq 0$, then there is a w that $B(v, w) \neq 0$. ⌟

Prop. (14.5.1.7)[Radical Splitting]. The **radical** of a quadratic space is defined to be $\mathrm{rad}(V) = V^\perp$. Then for any quadratic form V, there is an orthogonal decomposition $V = \mathrm{rad}(Y) \oplus W$, where W is a non-degenerate form. ⌟

Proof: In fact, by the definition, any complement space of $\mathrm{rad}(V)$ in V can be chosen as the orthogonal complement W. □

Prop. (14.5.1.8). If W is a non-degenerate sub-quadratic space of V, then $W \oplus W^\perp = V$. ⌟

Proof: Since W is non-degenerate, $W \cap W^\perp = 0$. and for any $v \in V$, $B(v,\cdot) \in W^*$, so by degeneracy, there is a $w \in W$ that $B(v,\cdot) = B(w,\cdot)$, then $z = v - w \in W^\perp$ and $v = w + z$. □

Prop. (14.5.1.9) [Orthogonal Complement and Non-Degeneracy]. If V is a non-degenerate quadratic space, then for any non-degenerate subspace W, $\dim W + \dim W^{\perp} = \dim V$, and $(W^{\perp})^{\perp} = W$. ⌟

Proof: The first is immediate from the fact $\dim\ker + \dim\mathrm{Coker} = \dim V$. The second is by dimensional reason. □

Cor. (14.5.1.10). A subspace W of a non-degenerate quadratic space V is a non-degenerate quadratic space iff $W \cap W^{\perp} = 0$. ⌟

Remark (14.5.1.11). We basically only care about non-degenerate forms, so from now on, we only care about non-degenerate forms. ⌟

Diagonalizability

Prop. (14.5.1.12) [Quadratic Form Representable]. Any quadratic forms over K of char$\neq 2$ is diagonalizable, and if $\alpha \in K^*$ is represented by K, then it is diagonalizable to a matrix with first entry α.

We will use the notation $\langle \alpha_1, \ldots, \alpha_n \rangle$ for the diagonal quadratic form $\sum \alpha_i x_i^2$. ⌟

Proof: Use(3.5.10.20), since in this case, a quadratic form is equivalent to a symmetric form. And if $\alpha = B(v, v)$, then we can choose v in the first place in the proof of(3.5.10.20). □

Cor. (14.5.1.13). Over a quadratically closed field K of char$\neq 2$, any non-degenerate quadratic form is congruent to $x_1^2 + \ldots + x_n^2$. ⌟

Proof: Because in this case, we can make $\sum a_i x_i^2$ into $\sum(\sqrt{a_i} x_i)^2$. □

Isotropic and Hyperbolic Spaces

Def. (14.5.1.14) [Isotropic]. Given a non-degenerate quadratic space V, a vector v is called **isotropic** if $B(v, v) = 0$. V is itself called **isotropic** if it is non-degenerate and there exists an isotropic vector, otherwise it is called **anisotropic**. ⌟

Def. (14.5.1.15) [Hyperbolic]. The **hyperbolic plane** $\mathbb{H}$ is the 2-dimensional space with quadratic form $H(x, y) = xy$, which is congruent to $\frac{1}{2}(x^2 - y^2)$.

A quadratic space is called **hyperbolic** if it is isomorphic to a direct sum of hyperbolic planes. ⌟

Lemma (14.5.1.16). If V is a non-degenerate isotropic space, then there is an isometric imbedding of the hyperbolic plane into V. ⌟

Proof: There is a $u \in V$ that $B(u, w) = 0$. By non-degeneracy, there is a w that $B(u, w) \neq 0$. We may assume $B(u, w) = 1$. Now I claim there is an α that $q(\alpha u + w) = 0$: in fact, $q(\alpha u + w) = 2\alpha B(u, w) + q(w)$, so take $\alpha = -q(w)/2$. Let $v = \alpha u + w$, then $q(u) = q(v) = 0$, and $B(u, v) = 1$, so it is isomorphic to $\mathbb{H}$. □

Prop. (14.5.1.17) [Isotropic Complement]. If V is a non-degenerate quadratic space, and $W \subset V$ is an isotropic space with basis $u_1, \ldots, u_m$, then there is another isotropic space W' with basis $v_1, \ldots, v_m$ that $B(u_i, v_j) = \delta_{ij}$. ⌟

Proof: Use induction on m. The $m=1$ case is lemma(14.5.1.16) above. If this is true for $n<m$, let $W=\{u_2,\dots,u_m\}$, then if $W^\perp\subset\{u_1\}^\perp$, then $u_1\in W$ by(14.5.1.9), contradiction, so there is a $v\in W^\perp$ that $B(u_1,v)\neq 0$, so by the same proof as(14.5.1.16), there is a αu_1+v that is isotropic, and a $\mathbb{H}\subset W^\perp$, so by(14.5.1.9), $W\subset\mathbb{H}^\perp$, so by induction, we can find in $\mathbb{H}^\perp$ elements $v_2,\dots,v_m$ that satisfies the requirement. □

Cor. (14.5.1.18). $\langle a,-a\rangle\cong\mathbb{H}$, because it is isotropic, and it has dimension 2. ⌟

Cor. (14.5.1.19) [Isotropic Form is Universal]. A non-degenerate isotropic space is universal, because hyperbolic plane does. ⌟

Cor. (14.5.1.20). A maximal totally isotropic space in a non-degenerate quadratic space V has dimension at most $\frac{1}{2}\dim V$, and equality holds if V is hyperbolic. ⌟

Prop. (14.5.1.21) [First Representation Theorem]. If q is a non-degenerate quadratic form, then q represents $\alpha\in K^*$ iff $q\oplus\langle-\alpha\rangle$ is isotropic. ⌟

Proof: If q represent α, then by(14.5.1.12) shows that q is equivalent to $\langle\alpha,\alpha_1,\dots,\alpha_n\rangle$, so $q\oplus\langle-\alpha\rangle$ contains a $\langle\alpha,-\alpha\rangle$ which is isomorphic to $\mathbb{H}$ by(14.5.1.16).

Conversely, if $q\oplus\langle-\alpha\rangle$ is isotropic, then there is a $-\alpha x_0^2+\sum\alpha_i x_i^2=0$. If $x_0\neq 0$, then q represent α, and if $x_0=0$, then q is isotropic, thus represent any element(14.5.1.19). □

Cor. (14.5.1.22). The following are equivalent:

- Any n-quadratic form over K is universal.
- Any $(n+1)$-quadratic form over K is isotropic.

⌟

Cor. (14.5.1.23) [Transform of Binary Forms]. For any $a,b\in F^*$ that $a+b\in F^*$, $\langle a,b\rangle\cong\langle a+b,(a+b)ab\rangle$. ⌟

Prop. (14.5.1.24) [Isotropy Criterion]. For two non-degenerate forms f,g over K, $h=\langle f,-g\rangle$ is isotropic iff there is an $\alpha\in K^*$ that is represented by both f and g. ⌟

Proof: Easy, notice to use isotropic form is universal(14.5.1.19). □

2 Witt Theory

Prop. (14.5.2.1) [Witt Cancellation Theorem]. If U_1,U_2,V_1,V_2 are quadratic spaces and $V_1\cong V_2$, $V_1\oplus U_1\cong V_2\cong U_2$, then $U_1\cong U_2$. ⌟

Proof: We may identify $V_1=V_2=V$, and $W=U_1\oplus V=U_2\oplus V$.

First if V is totally isotropic and U_1 is non-degenerate, then there is a matrix $M=\begin{bmatrix}A & B\\ C & D\end{bmatrix}$ that

$$M^t\begin{bmatrix}0 & 0\\ 0 & B_2\end{bmatrix}M=\begin{bmatrix}0 & 0\\ 0 & B_1\end{bmatrix}$$

So $B_1=D^tB_2D$. As B_1 is non-singular, so is D, thus $U_1\cong U_2$.

Now if V is isotropic but U_1,U_2 are not non-degenerate, then we may assume in their diagonalization, U_1 has less 0s, it has r 0s, then we can extract from both U_i a zero part, thus reducing to the above case.

Now if $\dim V = 1$, $V = \langle a \rangle$, if $a = 0$, then we are done by the above argument, and if $a = 0$, then find $q(x) = a$, then by(14.5.2.13), we can find a $\tau \in O(W)$ that $\tau(V_1) = V_2$, so now U_1, U_2 as the orthogonal complement of V_1, V_2, they are isometric under the map τ.

So now in general, we can cancel V out by moving its diagonal part once a time. □

Cor. (14.5.2.2). If X is a quadratic space and V_1, V_2 are non-degenerate subspaces of X, then any isometry $V_1 \cong V_2$ extends to an isometry of X. ⌟

Proof: $V_i \oplus V_i^{\perp} = X$ by(14.5.1.8). □

Cor. (14.5.2.3) [Witt's Extension Theorem]. If X is a non-degenerate quadratic space and $f : W_1 \to W_2$ is an isometry of two subspaces of X, then f extends to an isometry of X.

Notice this also holds for symplectic spaces X, by the same method of proof. ⌟

Proof: If W_1 is non-degenerate, then so does W_2, and we can use(14.5.2.2). By(14.5.1.7), we can write $W_i = U_i \oplus V_i$ where U_i is totally isotropic and V_i is non-degenerate. Now X, V_i are non-degenerate, $V_i^{\perp}$ is non-degenerate also, so there is an isotropic complement $U_i' \subset V_i^{\perp}$(14.5.1.17). Let $T_i = \langle U_i, U_i' \rangle V_i$, then T_i is non-degenerate and $W \subset T$. As U_i is the radical of W_i, $U_1 \cong U_2$, and then $\langle U_1, U_1' \rangle \cong \langle U_2, U_2' \rangle$. By Witt cancellation, $W_1 \cong W_2$. So we reduced to the non-degenerate case. □

Cor. (14.5.2.4). If V is a non-degenerate quadratic space, then the group of isometries of X acts transitively on the set of all totally isotropic subspaces of a fixed dimension d. ⌟

Prop. (14.5.2.5) [Witt's Decomposition Theorem]. For any quadratic space V, there is an orthogonal decomposition

$$V \cong \mathrm{rad}(V) \oplus \bigoplus_{1}^{k} \mathbb{H} \oplus V'$$

where V' is anisotropic(14.5.1.14). Moreover the number $k = I(V)$ which is called the **Witt index** of V and the isometry class of $V' = w(V)$ which is called the **non-isotropic kernel** is independent of the decomposition. ⌟

Proof: The existence of the decomposition follows from(14.5.1.7) and an easy induction using(14.5.1.16). The uniqueness is an easy corollary of(14.5.1.16) and Witt's cancellation theorem. □

Cor. (14.5.2.6). The Witt index equals the maximal dimension of a maximal totally isotropic subspace of W, by(14.5.1.17). ⌟

Remark (14.5.2.7). This is a good reason that <u>we will only consider non-degenerate quadratic forms from now on.</u> ⌟

Cor. (14.5.2.8) [Sylvester's Law of Nullity]. Let $q_{r,s} = [r]\langle 1 \rangle \oplus [s]\langle 1 \rangle$, then any non-degenerate quadratic form q over $\mathbb{R}$ is congruent to exactly one of $q_{r,s}$, and $r - s$ is called the **signature** of q. ⌟

Def. (14.5.2.9). Two quadratic forms $q_1 = \langle a_1, \ldots, a_n \rangle$ and $q_2 = \langle b_1, \ldots, b_n \rangle$ are called **simply equivalent** iff there are two indices that $\langle a_i, a_j \rangle \cong \langle b_i, b_j \rangle$. Two quadratic forms are called **chain equivalent** iff there is a chain of simply equivalence between them. ⌟

Prop. (14.5.2.10) [Witt's Chain Equivalence Theorem]. Two diagonal quadratic forms over K are equivalent iff they are chain equivalent. ⌟

Proof: Chain equivalent is clearly equivalent, Conversely, by Witt's decomposition theorem, it is easy to reduce to the non-degenerate case.

Now if $q = \langle \alpha_1, \ldots, \alpha_n \rangle \cong q' = \langle \beta_1, \ldots, \beta_n \rangle$, any form $q = \langle \gamma_1, \ldots, \gamma_n \rangle$ that is chain equivalent to q is equivalent to q', so β_1 is represented by it, choose a form that there is a minimal l that β_1 is represented by $\langle \gamma_1, \ldots, \gamma_l \rangle$, we prove that $l = 1$:

if the minimal l is not 1, then $d = \gamma_1 a_1^2 + \gamma_2 a_2^2 \neq 0$(otherwise l can be smaller), so $\langle \gamma_1, \gamma_2 \rangle \cong \langle d, \gamma_1\gamma_2 d \rangle$ by(14.5.1.12) and invariance of det. so $q \cong \langle d, \gamma_3, \ldots, \gamma_n, d\gamma_1\gamma_2 \rangle$(notice permutation is chain equivalence), and this is smaller, contradiction.

Now $l = 1$, so we may assume $\alpha_1 = \beta_1$, and then Witt's cancellation(14.5.2.1) shows that $\langle \alpha_2, \ldots, \alpha_n \rangle \cong \langle \beta_2, \ldots, \beta_n \rangle$, so we win by induction. □

Orthogonal Group

Prop. (14.5.2.11). The **orthogonal group** of a quadratic form q is the set of matrixes M that $g(Mx) = q(x)$. And it is clear $\det M = \pm 1$, so we can also define $O^+(V)$ and $O^-(V)$. ⌟

Def. (14.5.2.12). A **hyperplane reflection** for a non-isotropic vector v is defines by $x \mapsto x - \frac{2B(x,v)}{q(v)} v$, it is an element in $O(V)$. ⌟

Prop. (14.5.2.13). If x, y are two non-isotropic vectors that $q(x) = q(y)$, then there is a $\tau \in O(V)$ that $\tau(x) = y$. ⌟

Proof: First notice $q(x+y) + q(x-y) = 2q(x) + 2q(y) = 4q(x) \neq 0$, so one of $x+y, x-y$ is non-isotropic. And it can be easily calculated that $\tau_{x-y}(x) = y$ or $-\tau_{x+y}(x) = y$. □

Prop. (14.5.2.14) [Cartan-Dieudonné]. Let V be a non-degenerate quadratic form of dimension n, then every element of the orthogonal group $O(V)$ can be represented as a product of n reflections. ⌟

Proof: Cf.[Quadratic Forms Clark P22]. □

3 Witt Ring

References are [Quadratic Forms 2, Clark].

Def. (14.5.3.1)[Witt Ring]. The **Witt ring** $W(K)$ of K is a free commutative ring over $\mathbb{Z}$ generated by equivalent classes of anisotropic(14.5.1.14) quadratic forms over K, modulo the the relations $[q_1] + [q_2] - [q_1 \oplus q_2]$ and $[q_1] \cdot [q_2] - [q_1 \otimes q_2]$.

There is another ring, the **Grothendieck-Witt ring** $\widehat{W}(K)$ which is defined as the ring generated by all non-degenerate quadratic forms over K. ⌟

Cor. (14.5.3.2)[Rank Functor]. There are rank functors from $\widehat{W}(K) \to \mathbb{Z}$, which is a ring homomorphism. In particular, two elements of the same rank are equal in $\widehat{W}(K)$ iff they are equal in $W(F)$, by Witt's cancelation theorem(14.5.2.1). ⌟

Prop. (14.5.3.3). The rank functor is an isomorphism $\widehat{W}(K) \to \mathbb{Z}$ iff K is quadratically closed. In this case, $W(K) \cong \mathbb{Z}/2\mathbb{Z}$. ⌟

Proof: This is equivalent to $\langle a \rangle \cong \langle 1 \rangle$ for any $a \in K^*$, which means K is quadratically closed. □

Prop. (14.5.3.4). The subgroup $[\mathbb{H}]$ generated by the hyperbolic plane is an ideal of $\widehat{W}(K)$. And $\widehat{W}(K)/\mathbb{Z}[\mathbb{H}] \cong W(K)$. ⌟

Proof: $\mathbb{Z}[\mathbb{H}]$ is an ideal because $[\mathbb{H}]\cdot[\langle a_1,\ldots,a_n\rangle]\cong\sum\langle a_i,-a_i\rangle$ which is a multiple of $[\mathbb{H}]$, by(14.5.1.18). The last assertion follows from Witt's decomposition(14.5.2.5). □

Cor. (14.5.3.5). $[\langle a_1,\ldots,a_n\rangle]+[\langle -a_1,\ldots,-a_n\rangle]=0\in W(F)$, by(14.5.1.18). ⌟

Prop. (14.5.3.6) [Presentation of the Witt Ring]. $\widehat{W}(F)$ is isomorphic to the quotient of the free commutative ring generated by $\{[a]|a\in F^*\}$ module the following relations:

- $[1]-1$.
- $[ab]-[a]-[b]$.
- $[a]+[b]-[a+b](1+[ab])$, $a,b,a+b\in F^*$.

⌟

Proof: Cf.[Lam, P39]. □

4 Quaternion Algebras

References are [Quaternion Algebras].

Notation (14.5.4.1).

- In this subsection, let $k,F\in \texttt{Field}$.

⌟

Def. (14.5.4.2) [Quaternion Algebras]. Let $a,b\in F^\times$, define a **Quaternion algebra** $Q(a,b)$ as

$$Q_F(a,b)=Q\langle X,Y\rangle/(X^2-a,Y^2-b,XY+YX).$$

Denote $\overline{X}=\mathrm{i},\overline{Y}=\mathrm{j},\overline{XY}=\mathrm{k}$. ⌟

Prop. (14.5.4.3). Let $a,b\in F^\times$, then

- $\dim_F Q_F(a,b)=4$, thus any element of $Q_F(a,b)$ is of the form $x+y\,\mathrm{i}+z\,\mathrm{j}+w\,\mathrm{k}$.
- $Q_F(ax^2,by^2)\cong Q_F(a,b)$ for $x,y\in F^\times$.
- $Q_F(-1,1)\cong \mathrm{Mat}(2;F)$.
- $Q_F(a,b)$ is a simple algebra with center F.

⌟

Proof: 1: $Q_F(a,b)\otimes_F\overline{F}=Q_{\overline{F}}(a,b)\cong Q_{\overline{F}}(-1,1)\cong M_2(\overline{F})$ has dimension 4 over $\overline{F}$, by item2 and3.

2: trivial.

3: The map is given by $\varphi:Q_F(-1,1)\to\mathrm{Mat}(2;F):i\mapsto\begin{bmatrix} & 1\\ -1 & \end{bmatrix}, j\mapsto\begin{bmatrix} & 1\\ 1 & \end{bmatrix}$. The verification is straightforward.

4: Consider $Q_F(a,b)\otimes_F\overline{F}\cong\mathrm{Mat}(2,\overline{F})$ is simple with center $\overline{F}$, the center of $Q_F(a,b)$ has to be F, and also simple. □

Def. (14.5.4.4) [Pure Tensors]. A quaternion element of the form $yi+zj+wk$ is called a **pure tensor**. The space of pure tensor is denoted by A_0.

Let $v\neq 0\in Q_F(a,b)$, then $v\in A_0$ iff $v\notin F$ but $v^2\in F$. ⌟

Proof: By direct calculation,

$$(x+y\,\mathrm{i}+z\,\mathrm{j}+w\,\mathrm{k})^2=(x^2+ay^2+bz^2-abw)+2x(y\,\mathrm{i}+z\,\mathrm{j}+w\,\mathrm{k}).$$

□

Def. (14.5.4.5) [Bar Involution]. There is an anti-involution of $Q_F(a,b) = Q\langle X,Y\rangle/(X^2-a, Y^2-b, XY+YX)$ given by $X \mapsto -X, Y \mapsto -Y$(thus $XY \mapsto (-Y)(-X) = YX$), called the **bar involution**.

Thus if we define the **norm** and **trace** $N : x \mapsto x\overline{x}, \mathrm{tr} : x \mapsto x + \overline{x}$, then they have images in F. If $\alpha = x + y\,\mathrm{i} + z\,\mathrm{j} + w\,\mathrm{k}$, then $\mathrm{tr}(\alpha) = 2x, \mathrm{Nm}(\alpha) = x^2 - ay^2 - bz^2 + abw^2$. ⌟

Cor. (14.5.4.6) [Invariance of Bar Involutions]. Notice the bar involution can be defined intrinsically, by defining pure vectors, which are vectors x s.t. $x^2 \in F$ but $x \notin F$. In particular, the bar involution, trace and determinants are invariant under isomorphisms of quaternion algebras. ⌟

Cor. (14.5.4.7). For $x \in Q_F(a,b)$, if we let $T(x)$ be the left(or right) multiplication by x on $Q_F(a,b)$, then the determinant of $T(x)$ equals $\mathrm{Nm}(x)^2$. ⌟

Proof: After base change, all the values won't change, thus it suffices to prove for $M(2,F)$, in which case, it can be verified by(14.5.4.3) that $\det(A) = N(A)$, and the $T(A)$ has determinant $\det(A)^2$. □

Prop. (14.5.4.8) [Norm Form]. Define a symmetric bilinear form on $Q_F(a,b)$: $B(x,y) = \mathrm{tr}(x\overline{y})/2$. Its norm form is just $N(x)$.

Thus this symmetric space has $\{1,\mathrm{i},\mathrm{j},\mathrm{k}\}$ as an orthonormal basis. It is non-degenerate and isomorphic to
$$\langle 1,-a,-b,ab\rangle \cong \langle 1,-a\rangle \otimes \langle 1,-b\rangle.$$
⌟

Prop. (14.5.4.9). Let A, A' be two quaternion algebras over F, then the following are equivalent:

- A, A' are isomorphic as quaternion algebras.
- A, A' are isomorphic as quadratic spaces.
- A_0, A_0'(14.5.4.4) are isomorphic as quadratic spaces.

⌟

Proof: Cf.[Lam, P57]. □

Cor. (14.5.4.10). $Q_F(a,-1) \cong Q_F(a,a)$. ⌟

Proof: These algebras have norm forms $\langle 1,-a,-1,-a\rangle$ and $\langle 1,-a,-a,a^2\rangle$, which are clearly isometric quadratic spaces. □

Prop. (14.5.4.11) [Split or Division Ring]. Let $A = Q_F(a,b)$, then the following are equivalent:

1. $A \cong \mathrm{Mat}(2,F)$.
2. A is not a division algebra.
3. A is isotropic as a quadratic space.
4. A is hyperbolic as a quadratic space.
5. A_0 is isotropic as a quadratic space.
6. $(\langle a\rangle - 1)(\langle b\rangle - 1) = 0$ in $W(F)$(or $\widehat{W}(F)$, by(14.5.3.2)).
7. (Hilbert's Criterion)The binary form $\langle a,b\rangle$ represents 1.
8. $a \in \mathrm{Nm}_{E/F}(E^*)$, where $E = F(\sqrt{b})$.

⌟

Proof: $4\to 5\to 3$ is clear. As $Q_F(-1,1)\cong M(2,F)$, $1,4,6,7$ are equivalent by(14.5.1.12) and(14.5.4.9). Also $3\iff 4$ as the the norm form of A has determinant in $(F^*)^2$. Also $1\to 2\to 3$ is clear, as $x\in A$ is invertible iff $N(x)\neq 0$. Thus 1 to 7 are all equivalent.

Now we show $7\iff 8$: Firstly assume $b\notin (F^\times)^2$, otherwise both are true. Let $E=F(\sqrt{b})$, then $N_{E/F}(x+y\sqrt{b})=x^2-by^2$, thus 8 says $a\in D_F(\langle 1,-b\rangle)$, which is equivalent to $\langle 1,-b,-a\rangle$ isotropic, which is equivalent to $\langle a,b\rangle$ represents 1, by representation theorem(14.5.1.21). □

Cor. (14.5.4.12). Let $a\in F^\times$,

- $Q_F(1,-a)\cong Q_F(a,-a)\cong \mathrm{Mat}(2;F)$.
- If $a\neq 1$, then $Q_F(a,1-a)$ splits.
- $Q_F(-1,a)$ splits iff a is a sum of two squares in F.

⌟

Proof: These follows from Hilbert's criterion and representation theorem(14.5.1.21). □

Prop. (14.5.4.13) [Characterizing Quaternion Algebras].

- If $A\neq F$ is a central simple algebra over F of dimension≤ 4, then A is isomorphic to a quaternion algebra over F.
- If $B\neq F$ is a f.d. central simple F-algebra equipped with an F-algebra involution $x\mapsto\overline{x}$ s.t. $x+\overline{x}\in F, x\overline{x}\in F$ for any $x\in B$, then B is isomorphic to a quaternion algebra over F.

⌟

Proof: 1: Use Wedderburn's theorem, then $A\cong M(n,D)$ where D is a division ring over F with center F. Then $A=M(2,F)\cong Q_F(1,-1)$ or D. If $A=D$, choose $i\notin F$, and $K=F(i)$ a subfield of D. Then $F\subset K\subset D$, thus $\dim K=2$, thus we may modify i that $i^2=a\in F$. The conjugation of i on D satisfies $(\mathrm{ad}(i))^2=\mathrm{id}$, thus $A=A^+\oplus A^-$ where $\mathrm{ad}(i)$ acts by 1 and -1 resp.. Let $j\neq 0\in A^-$, then $ij=-ji$, $j^2i=ij^2$, thus $j^2\in A^+$. Now $K(j)$ is also a quadratic field over F, thus $j^2+cj-b=0$ for $c,b\in F$. Then $cj=b-j^2\in A^+\cap A^-=0$ shows $c=0$. Then $A=F\oplus Fi\oplus Fj\oplus Fij$ is the quaternion algebra $Q_F(a,b)$.

2: Use Wedderburn's theorem, then $A\cong \mathrm{Mat}(n,D)$ where D is a central division ring over F. The hypothesis shows every element of B satisfies a degree 2 equation $x^2-(x+\overline{x})x+x\overline{x}=0$, thus $n\leq 2$. If $n=2$, then consider the diagonal elements, then we get $D=F$. If $B=D$, then the same argument as above shows we can find i,j that $ij=-ji$ and $\mathrm{i}^2=a,\mathrm{j}^2=b,a,b\in F^*$. Then j induces an isomorphism $A^+\cong A^-$. If there are some $l\in A^+\backslash F(i)$, then $\overline{il}=\overline{l}\overline{i}=il$, thus $il+\overline{il}=2il\in F$, contradiction. Thus $A^+=F(\mathrm{i})$, and $D=Q_F(a,b)$. □

Prop. (14.5.4.14) [Classifying Binary Forms]. Let $q=\langle a,b\rangle, q'=\langle a',b'\rangle$ be non-singular binary forms, then they are isomorphic iff $\det(q)=\det(q')$ and $Q_F(a,b)\cong Q_F(a',b')$. ⌟

Proof: If $q\cong q'$, then $ab=a'b'\in F^\times/(F^\times)^2$, thus $\langle 1,-a,-b,ab\rangle\cong\langle 1,-a',-b',a'b'\rangle$, thus $Q_F(a,b)\cong Q_F(a',b')$ by(14.5.4.11). The converse follows the same way by cancellation theorem(14.5.2.1). □

Def. (14.5.4.15) [Hilbert Symbol]. For $a,b\in k^\times$, define the **Hilbert symbol**

$$\{a,b\}_k=\begin{cases}1 & Q_k(a,b)\cong \mathrm{Mat}(2;k)\\ -1 & \text{otherwise}\end{cases}.$$

⌟

Splitting Fields

Def. (14.5.4.16)[Splitting Fields]. A quaternion algebra A over F is said to **split** in a field extension K/F if $A\otimes_F K\cong \mathrm{Mat}(2,K)$. K is said to be a **splitting field** for A. ⌟

Prop. (14.5.4.17). Let $A=Q_F(a,b)$ and $K=F(\sqrt{c}), c\in F^\times$, then the following are equivalent:

- A splits over K.
- $A\cong Q_F(c,d)$ for some $d\in F^\times$.
- K is a subalgebra of A over F.

⌟

Proof: 1 → 2: Consider the pure tensor space $A_0\cong\langle -a,-b,ab\rangle$. If it is isotropic, then $A_0\cong\langle -c,-d,cd\rangle$ for some $d\in F^\times$. If it is anisotropic, then because $A_K\cong\mathrm{Mat}(2;K)$, by(14.5.4.11), there exists x_i,y_i not all zero s.t.

$$-a(x_1+\sqrt{a}y_1)^2-b(x_2+\sqrt{a}y_2)^2+ab(x_3+\sqrt{a}y_3)^2=0$$

Thus $\mathtt{x}$ is orthogonal to $\mathtt{y}$ and $N(\mathtt{x})+cN(\mathtt{y})=0$. $\mathtt{y}\neq 0$, because otherwise $N(\mathtt{x})=0$ and $\mathtt{x}=0$. Thus there is an orthogonal basis $\{x,y,z\}$, and

$$A_0\cong\langle N(z),N(y),-cN(y)\rangle,$$

and because $\det(A_0)=1$, $N(z)\in c(K^\times)^2$, thus item2 holds.

2 → 3: In fact, if $\mathrm{i}^2=c\in A$, then $F(\mathrm{i})\cong K$.

3 → 1: This follows from(3.6.3.17). □

Prop. (14.5.4.18). ⌟

5 over Local or Finite Fields

References are [Quadratic Forms 3, Clark]

In this subsection, Let F be a local field or a finite field, of char$\neq 2$ with a non-trivial character ψ.

Prop. (14.5.5.1) [$W(\mathbb{F}_q)$]**.**

- If $q\equiv 1 \mod 4$, then $W(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}[F^*/(F^*)^2]\cong\mathbb{Z}/2\mathbb{Z}[\mathbb{F}_2]$ as rings.
- If $q\equiv 3 \mod 4$, then $W(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ as rings.

⌟

Proof: 1: In this case, -1 is a square, let s be a non-square, then there are only three anisotropic forms: $\langle 1\rangle,\langle s\rangle,\langle 1,s\rangle$. Thus the assertion is clear.

2: In this case, we can take $s=-1$, thus any anisotropic form must be of the form $\langle 1,\ldots,1\rangle$ or $\langle -1,\ldots,-1\rangle$. As $\langle 1,1\rangle$ is universal by(25.6.1.5), $\langle 1,1,1\rangle\cong\langle -1\rangle$ by representation theorem(14.5.1.21), thus $4[\langle 1\rangle]=0$. □

Prop. (14.5.5.2). Every binary quadratic form over a finite field $\mathbb{F}_q$ is universal. ⌟

Proof: By(14.5.5.1), if s is a non-square, there are essentially three quadratic forms, $\langle 1,1\rangle,\langle s,s\rangle,\langle 1,s\rangle$. By(25.6.1.5), these are all universal. □

Cor. (14.5.5.3). Any quaternion algebra over a finite field splits, by Hilbert's criterion(14.5.4.11). ⌟

Prop. (14.5.5.4) [$W(\mathbb{R})$].

- There exists two anisotripic forms at each rank n: $\langle 1,\ldots,1\rangle$ and $\langle -1,\ldots,-1\rangle$.
- $W(\mathbb{R})\cong\mathbb{Z}$.
- (Sylvester's Law of Inertia)Two non-degenerate forms over $\mathbb{R}$ are equivalent iff they have the same rank and signature.
- $\widehat{W}(\mathbb{R})\cong\mathbb{Z}[\mathbb{F}_2]$ as a ring.

⌟

Proof: Only 4 need a proof: It suffices to show $[\langle 1\rangle]$ and $[\langle -1\rangle]$ are linearly independent in $\widehat{W}(\mathbb{R})$, because they generate all other rings. But if $a[\langle 1\rangle]+b[\langle -1\rangle]=0$, then $a+b=0$ by rank reason, but when pass to $W(F)$, $a-b=0$, thus $a=b=0$. □

Prop. (14.5.5.5). Let $\langle a_1,\ldots,a_n\rangle_F$ be a quadratic space over a non-Archimedean local field F, we may assume $a_i\in\mathcal{O}_F$. If $\langle a_1,\ldots,a_n\rangle_{\mathcal{O}_F/\mathfrak{p}^n}$ is isotropic for all n, then $\langle a_1,\ldots,a_n\rangle_F$ is isotropic. ⌟

Proof: This is because we can find non-zero elements $v_n\in(\mathcal{O}_F/\mathfrak{p}^n)^d$ that $q(v_n)=0\in\mathcal{O}_F/\mathfrak{p}^n$, thus we can find elements $v\in\mathcal{O}_F^d$ that $q(v)=0$. □

Prop. (14.5.5.6) [Unique Quaternion Algebra]. If $F\not\cong\mathbb{C}$ is a local field, then there is a unique non-split quadratic algebra over F. ⌟

Proof: Cf.[Lam, P156]. □

Cor. (14.5.5.7). For this unique quaternion algebra A, the valuation $|N(x)|$ is a valuation of A, i.e. defines the topology. ⌟

Proof: This is because $|N(\cdot)|$ is bounded on the compact subset $\{x||x|=1\}$. □

Prop. (14.5.5.8)[Hilbert Symbol]. Let F be a local or finite field, then the Hilbert symbol(14.5.4.15) $(\cdot,\cdot)_F:F^*/(F^*)^2\times F^*/(F^*)^2\to\{\pm 1\}$ satisfies

- It is symmetric and bi-multiplicative for both terms.
- It is non-degenerate: if $F\not\cong\mathbb{C}$ is a local field, for any $y\in F^*\backslash(F^*)^2$, then there exists a $z\in F^*$ that $(y,z)_F=-1$.
- $(a,-a)=1$.
- If $a(a-1)\neq 0$, $(a,1-a)=1$.

⌟

Proof: 1: To show it is multiplicative, by(14.5.4.11), $(a,b)_F=1$ iff $a\in N_{E/F}(E^*)$, where $E=F(\sqrt{b})$. Notice $N_{E/F}(E^*)$ has index 1 or 2 in F^* by class field theory(14.6.2.10), thus $a\mapsto(a,b)_F$ is a character of a in any case.

2: Cf.[Lam, P160].?

3: By(14.5.4.12). □

Prop. (14.5.5.9) [Weil]. Let (V,B) be a quadratic space over a local or finite field F of dimension d, ψ a non-trivial character of F. Let V be identified with V^* via $(v,v^*)\mapsto\psi(-2B(v,v^*))$, denote the Fourier transform $\mathcal{F}$ to be compatible with this identification.

Let $F_B(v)=\psi(B(v,v))$, then for any $a\in F^*$, then $\varphi*F_{aB}\in\mathcal{S}(V)$ for any $\varphi\in\mathcal{S}(V)$, and there is a complex number $\gamma(aB)$ with norm 1 that for any $\varphi\in\mathcal{S}(V)$,

$$\mathcal{F}(\varphi*F_{aB})=|a|^{-d/2}\gamma(aB)\mathcal{F}(\varphi)F_{-a^{-1}B}.$$

which means $|a|^{-d/2}\gamma(aB)F_{-a^{-1}B}$ is formally the Fourier transform of F_{aB}. ⌟

Proof: We only prove for $a=1$:

$$(\Phi*F_B)(v)=\int_V\Phi(u)\psi(B(v-u,v-u))du=F_B(v)\mathcal{F}(\Phi\cdot F_B)(-v)$$

is an element of $\mathcal{S}(V)$, as $\mathcal{F}(\mathcal{S}(V))=\mathcal{S}(V)$(14.4.5.11). Now use the last equation of(3.1.5.8) for $z=1$ and the projective unitary representation ω_1 of $SL(2,F)$ on $L^2(V)$(20.7.3.2),

$$\omega_1(w_1)\omega_1(n(1))\omega_1(w_1)\omega_1(n(1))\omega_1(-1)\Phi=\gamma(B)\omega_1(n(-1))\omega_1(w_1)\Phi$$

for some $|\gamma(B)|=1$. Then it can be computed that the LHS equals $\widehat{\Phi*F_B}$, and the RHS equals $F_B\cdot\widehat{\Phi}$, thus we are done. □

Cor. (14.5.5.10) [Analytic Interpretation of Isotropy].

- If (V_1,B_1), (V_2,B_2) are quadratic spaces, then $\gamma(B_1\oplus B_2)=\gamma(B_1)\gamma(B_2)$.
- If (V,B) is a quadratic space, then $\gamma(-B)=\gamma(B)^{-1}$.
- If (V,B) is a hyperbolic quadratic space(14.5.1.15), then $\gamma(B)=1$.
- γ is a group homomorphism $W(F)\to\mathbb{C}^*$(14.5.3.1).

⌟

Proof: 1, 2 follow from taking test functions φ to be $\varphi_1\otimes\varphi_2$ or $\overline{\varphi}$. 3 follows from the fact $\gamma(\langle -1,1\rangle)=\gamma(\langle 1\rangle)\gamma(\langle -1\rangle)=1$. 4 follows from 1 and 3. □

Prop. (14.5.5.11). Situation as in(14.5.5.9),

- For any $\Phi\in\mathcal{S}(V)$, $\int_V(\Phi*F_B)(v)dv=\gamma(B)\int_V\Phi(v)dv$.
- If F is non-Archimedean , then for any lattice in V(14.2.3.34) sufficiently large, $\gamma(B)=\int_L F_B(v)dv$.
- If F is finite, then $\gamma(B)=\int_V F_B(v)dv$.

⌟

Proof: 1 follows from(14.5.5.9) evaluated at $a=1$ and $v=0$.

2: Consider the dual lattice L'(14.2.3.38), if L is sufficiently large, then L' is sufficiently small, s.t. $F_B(u)=1$ for all $u\in L'$. Then

$$(\chi_{L'}*F_B)(v)=\int_{L'}F_B(v-u)du=\psi(B(v,v))\int_{L'}\psi(-2B(u,v))du,$$

which equals $V(L')\chi_L F_B$. Then let $\Phi=\chi_{L'}$ in item1, we get the desired assertion.

3: This is the same as 2, take $\Phi=1$. □

Prop. (14.5.5.12) [Weil's Characterization of Hilbert Symbol]. Let $Q_F(a,b)$ be a quadratic algebra over a local field F of characteristic$\neq 2$, let $q:Q_F(a,b)\to F$ be the norm form, then $\gamma(q)=(a,b)_F$(14.5.4.15).

In particular, $(a,b)_F=\gamma(\langle 1,-a,-b,ab\rangle)$. ⌟

Proof: By(14.5.5.10) and(14.5.5.8), it suffices to show for a non-split $Q_F(a,b)$, $\gamma(\langle 1,-a,-b,ab\rangle)=-1$.

If F is Archimedean or finite, then the existence of a non-split $Q_F(a,b)$ over A shows $F=\mathbb{R}$, and $a=b=-1$, and $\gamma(\langle 1,1,1,1\rangle)=(\gamma(\langle 1\rangle))^4$. Let $\psi:\mathbb{R}\to\mathbb{C}:x\mapsto e^{2\pi ix}$ as in(14.4.5.3), and $\Phi(x)=e^{-\pi x^2}$, then it can be calculated using(14.5.5.9) that $\gamma(B)$ is an 8-th roots of unity, thus we are done.

If F is non-Archimedean, denote the Haar measure on $A=Q_F(a,b)$ by dz, and then by(14.5.4.7) and(11.10.1.19), the Haar measure on A^* is of the form $d^\times z=|N(z)|^{-2}dz$. By(14.5.5.7), for large n, $L=N^{-1}(\mathfrak{p}^{-n})$ is a sufficiently large lattice in V, thus we can use(14.5.5.11) to evaluate the sign of

$$\gamma(N)=\int_{L\backslash\{0\}}\psi(N(z))|N(z)|^2d^\times z.$$

But this integrand factors through $N:L\backslash 0\to\mathfrak{p}^{-n}$, thus it suffices to evaluate the sign of

$$\int_{\mathfrak{p}^{-n}\backslash 0}\psi(x)|x|^2d^\times x=\int_{\mathfrak{p}^{-n}}\psi(x)|x|dx,$$

which is $-q^{1-2r}(1-q^{-1})^{-1}$, where the conductor of ψ is $\mathfrak{p}^r$. So $\gamma(N)=-1$. □

Cor. (14.5.5.13). Let $r_i\in F^*$, then $\gamma(\langle ar_1,\ldots,ar_{2n}\rangle)=((-1)^nr_1\ldots r_{2n},a)_F\gamma(\langle r_1,\ldots,r_{2n}\rangle)$. ⌟

Proof: By(14.5.5.12), it suffices to show for $n=1$. $\gamma(\langle r_1,r_2\rangle)=(r_1,r_2)_F\gamma(\langle 1,r_1r_2\rangle)$, thus also $\gamma(\langle ar_1,ar_2\rangle)=(ar_1,ar_2)_F\gamma(\langle 1,a^2r_1r_2\rangle)$, so

$$\gamma(\langle ar_1,ar_2\rangle)/\gamma(\langle r_1,r_2\rangle)=(ar_1,ar_2)_F/(r_1,r_2)_F=(a,-r_1r_2)$$

by(14.5.5.8). □

Cor. (14.5.5.14). Let (V,B) has dimension $2n$, then $\gamma(B)^2=((-1)^n\det(B),-1)_F$. ⌟

Proof: It reduces to $n=1$, in which case, it suffices to show that $\gamma(\langle r_1,r_2\rangle)^2=(-1,-r_1r_2)_F$. But $(-1,-r_1r_2)_F=\gamma(\langle 1,1,r_1r_2,r_1r_2\rangle)=\gamma(\langle 1,r_1r_2\rangle)^2$. By(14.5.5.12), $\gamma(\langle 1,-r_1,-r_2,r_1r_2\rangle)^2=1$, thus $\gamma(\langle 1,r_1r_2\rangle)^2=\gamma(\langle r_1,r_2\rangle)^2$. □

6 over Global Fields

References are [Quadratic Forms over Global Fields, Clark].

Prop. (14.5.6.1). Let $k\in\texttt{Field},k=\overline{k}$ and $F=k(t)$, then any binary quadratic form Q over F is universal. ⌟

Proof: We may assume $Q=\langle 1,f\rangle$, where $f\in F^*$. We can assume $f\notin-(F^*)^2$, otherwise this is clearly universal. It is easy to see that the $\mathbb{F}_2$ vector space $F^*/(F^*)^2$ has a basis $\{t-a|a\in k\}$. Notice $D_F(Q)$ is a subgroup of F^* as it is the norm group of $F(\sqrt{-f})$, it suffices to show that $t-a\in D_F(Q)$. After a change of variable, it suffices to show that $t\in D_F(Q)$, or $\langle 1,f,-t\rangle$ is isotropic, or equivalently $-f\in\langle 1,-t\rangle$ for any f. The same argument show that it suffices to show that $\langle 1,-t,t-a\rangle$ is isotropic. But $t-a+(-t)+(\sqrt{a})^2=0$. □

Cor. (14.5.6.2). Any quaternion algebra over $\overline{k}(t)$ splits, by Hilbert's criterion(14.5.4.11). ⌟

Prop. (14.5.6.3) [Examples].

- $Q_{\mathbb{Q}}(-1,-1) \cong Q_{\mathbb{Q}}(-2,-3)$.
- $Q_{\mathbb{Q}}(-1,-1) \ncong Q_{\mathbb{Q}}(-2,-5)$.
- Let p be a prime number, $Q_{\mathbb{Q}}(-1,p)$ splits iff $p=2$ or $p \equiv 1 \mod 4$.
- Let p be a prime number, $Q_{\mathbb{Q}}(-2,p)$ splits iff $p=2$ or $p \equiv 1,3 \mod 8$.
- $Q_{\mathbb{Q}}(-3,5)$ is a division ring, but splits over $K=\mathbb{Q}(\sqrt{17})$.

⌟

Proof: 1: By(14.5.1.23), $Q_{\mathbb{Q}}(1,1,1,1) \cong (1,1,2,2) \cong (1,3,6,2)$, thus $Q_{\mathbb{Q}}(-1,-1) \cong Q_{\mathbb{Q}}(-2,-3)$ by(14.5.4.11).

2: if they are isomorphic, then $\langle 2,5,10\rangle \cong \langle 1,1,1\rangle \cong \langle 2,2,1\rangle$, thus $\langle 5,10\rangle \cong 1,2$, which is impossible as 1 is not representable by $\langle 5,10\rangle$.

3: By Hilbert's criterion(14.5.1.23), if $Q_{\mathbb{Q}}(-1,p)$ splits, then $-x^2+py^2=z^2$ for some $x,y,z \in \mathbb{Z}$ that $(x,y,z)=1$, thus -1 is a square in $\mathbb{F}_p$, which means $p \equiv 1 \mod 4$ or $p=2$. Conversely, if $p \equiv 1 \mod 4$, then by(21.4.1.7), $p=x^2+y^2$ for some $x,y \in \mathbb{Z}$, thus $\langle -1,p\rangle$ represents 1, so $Q_{\mathbb{Q}}(-1,p)$ splits. if $p=2$, then $\langle -1,2\rangle$ represents 1, thus it splits.

4: By Hilbert's criterion(14.5.1.23), if $Q_{\mathbb{Q}}(-1,p)$ splits, then $-2x^2+py^2=z^2$ for some $x,y,z \in \mathbb{Z}$ that $(x,y,z)=1$, thus -2 is a square in $\mathbb{F}_p$, which means $p \equiv 1,3 \mod 8$ or $p=2$. Conversely, if $p \equiv 1 \mod 4$, then by(21.4.1.7), $p=x^2+y^2$ for some $x,y \in \mathbb{Z}$, thus $\langle -1,p\rangle$ represents 1, so $Q_{\mathbb{Q}}(-1,p)$ splits. If $p=2$, then it splits as above.

5: If it splits, then $-3x^2+5y^2=z^2$ for some $x,y,z \in \mathbb{Z}$ that $(x,y,z)=1$. This is a contradiction modulo3. In $K=\mathbb{Q}(\sqrt{17})$, however, $5\cdot 2^2-3=17$, thus $Q_{\mathbb{Q}(\sqrt{13}}(-3,5)$ splits. □

Prop. (14.5.6.4)[Hasse-Minkowski Principle]. If $F \in$ `GField` and char $F \neq 2$, and Q is a quadratic form over F, then q is isotropic over F iff Q is isotropic over $F_{\mathfrak{p}}$ for all place $\mathfrak{p}$. ⌟

Proof: Cf.[Lam, P170].**?** □

7 Algebraic Extensions

14.6 Cohomology of Arithmetic Fields

Main references are [Neu15], [Cohomology of Number Fields, Neukirch], http://www.math.columbia.edu/~chaoli/docs/ClassFieldTheory.html#sec28 and [Mil20] and [Arithmetic Duality Theory, Milne].

Notation (14.6.0.1).

- Use notations from Global Fields

┘

1 Abstract Class Field Theory

Def. (14.6.1.1) [Class Formations]. A **profinite formation** consists of a profinite group G regarded as a Galois group of a field Gal_K and $A \in T_G$. It is called a **field formation** iff for any normal extension L/K, $H^1(L/K, A^L) = 0$.

For a field extension, by(8.7.1.13), inf is an injection on H^2. We denote $H^2(K)$ as the profinite cohomology group $H^2(G, A) = \mathrm{Br}(K)$. Inflation should be thought of as inclusions.

It is called a **class formation** if moreover for every normal extension L/K, there is an canonical isomorphism

$$\mathrm{inv}_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

that is compatible with inflation and restriction in the sense that:

- If $N/L/K$ with N/K and L/K normal, then $\mathrm{inv}_{L/K} = \mathrm{inv}_{N/K}|_{H^2(L/K)}$ via inflation.
- If $N/L/K$ with N/L and N/K normal, then $\mathrm{inv}_{N/L} \circ \mathrm{res}_L = [L : K] \cdot \mathrm{inv}_{N/K}$.

$\mathrm{inv}^{-1}_{L/K}(\frac{1}{[L:K]} + \mathbb{Z}) \in H^2(L/K)$ is called the **fundamental class** $u_{L/K}$. ┘

Prop. (14.6.1.2). inv also commutes with cor and conjugation:

$$\mathrm{inv}_{N/K}(\mathrm{cor}_K c) = \mathrm{inv}_{N/L} c, \quad \mathrm{inv}_{\sigma N/\sigma K}(\sigma^* c) = \mathrm{inv}(c).$$

The first is because inv commutes with res thus res is surjective, thus there is a c' that $c = \mathrm{res}\, c'$. Because of cor res=$[L : k]$, we have $\mathrm{cor}_K(c) = c'^{[L:K]}$. Thus $\mathrm{inv}_{N/K}(\mathrm{cor}_K c) = [L : K]\mathrm{inv}_{N/K}(c') = \mathrm{inv}_{N/L}(\mathrm{res}_L c') = \mathrm{inv}_{N/L}(c)$.

For the conjugation, Cf.[Neu15]P69**?**. ┘

Cor. (14.6.1.3). From this we easily get that

$$u_{L/K} = (u_{N/K})^{[N:L]}, \quad \mathrm{res}_L(u_{N/K}) = u_{L/K}$$

$$\mathrm{cor}_K(u_{N/L}) = (u_{N/K})^{[L:K]}, \quad \sigma^*(u_{N/K}) = u_{\sigma N/\sigma K}.$$

┘

Prop. (14.6.1.4) [Class Formation Main Theorem]. Tate's theorem(8.7.1.24) tells us for a class formation, for L/K normal extension, there is a **Nakayama isomorphism**

$$\theta_{L/K} = u_{L/K} \cup - : H^q(\mathrm{Gal}(L/K), \mathbb{Z}) \cong H^{q+2}(L/K).$$

Especially, for $q=-2$, there is a canonical isomorphism $\mathrm{Gal}^{\mathrm{ab}}(L/K)\cong A_K/\operatorname{Nm}_{L/K}A_L$. Its inverse is called the **Artin reciprocity isomorphism** and induces a **norm residue symbol** map $(-,L/K)$

$$1\to\operatorname{Nm}_{L/K}A_L\to A_K\xrightarrow{(-,L/K)}\mathrm{Gal}^{\mathrm{ab}}(L/K)\to 1.$$

This norm residue symbols induce an **Artin map**

$$\mathrm{Art}_K=(-,K):A_K\to\mathrm{Gal}_K^{\mathrm{ab}}=\varprojlim_{L/K}\mathrm{Gal}^{\mathrm{ab}}(L/K)$$

that has dense image. ⌟

Lemma (14.6.1.5). Let L/K be a normal extension, $a\in A_K$ and $\chi\in\mathrm{Gal}^{\mathrm{ab}}(L/K)^\vee=H^1(G(L/K),\mathbb{Q}/\mathbb{Z})$ is a character, then

$$\chi((a,L/K))=\mathrm{inv}_{L/K}(a\smile\delta\chi)\in\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}.$$

⌟

Proof: Cf.[Neukirch CFT P71]. □

Prop. (14.6.1.6)[Properties of Norm Residue Symbols]. For formal field extensions $N/L/K$ with N/K normal, there are commutative diagrams:

$$\begin{array}{ccc} A_K & \xrightarrow{(-,N/K)} & \mathrm{Gal}(N/K)^{\mathrm{ab}} \\ \downarrow{\scriptstyle\mathrm{id}} & & \downarrow{\scriptstyle\mathrm{pr}} \\ A_K & \xrightarrow{(-,L/K)} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array}\qquad \begin{array}{ccc} A_K & \xrightarrow{(-,N/K)} & \mathrm{Gal}(N/K)^{\mathrm{ab}} \\ {\scriptstyle\mathrm{Nm}_{L/K}}\uparrow\downarrow{\scriptstyle i} & & {\scriptstyle i}\uparrow\downarrow{\scriptstyle\mathrm{Ver}} \\ A_L & \xrightarrow{(-,N/L)} & \mathrm{Gal}(N/L)^{\mathrm{ab}} \end{array}\qquad \begin{array}{ccc} A_L & \xrightarrow{(-,N/L)} & \mathrm{Gal}(N/L)^{\mathrm{ab}} \\ \downarrow{\scriptstyle\sigma} & & \downarrow{\scriptstyle\sigma^*} \\ A_{\sigma L} & \xrightarrow{(-,\sigma N/\sigma L)} & \mathrm{Gal}(\sigma N/\sigma L)^{\mathrm{ab}} \end{array}$$

Where Ver is the transfer map defined in**??**. ⌟

Proof: Cf.[Neukirch CFT P72].? □

Remark (14.6.1.7) [Non-Abelian Problems]. For a finite normal extension L/K, $\operatorname{Nm}_{L/K}A_L=\operatorname{Nm}_{L^{\mathrm{ab}}/K}A_{L^{\mathrm{ab}}}$. This is because the quotient both correspond to $G(L/K)^{\mathrm{ab}}$. So class field theory doesn't tell about non-Abelian extension. ⌟

Prop. (14.6.1.8) [Norm Groups and Abelian Extension]. The map $L\mapsto\mathcal{N}_{L/K}=\operatorname{Nm}_{L/K}A_L$ defines a inclusion reversing isomorphism between the lattice of Abelian extension L of K and the lattice of norm groups of A_K, i.e.:

$$\mathcal{N}_{L_1L_2/K}=\mathcal{N}_{L_1/K}\cap\mathcal{N}_{L_2/K},\quad \mathcal{N}_{L_1\cap L_2/K}=\mathcal{N}_{L_1/K}\cdot\mathcal{N}_{L_2/K}.$$

And any group that contains a norm group is a norm group. ⌟

Proof: By the first commutative diagram of inv, if $(a,L_i/K)=0$, then $(a,L_1L_2/K)$ is trivial on $G_{L_i/K}$, thus trivial on $G_{L_1L_2/K}$, thus $a\in I_{L_1L_2}$. so $I_{L_1}\cap I_{L_2}\subset I_{L_1L_2}$, the other side is easy. the second is because $|I_{L_1\cap L_2}/I_{L_1}|=|G_{L_1/L_1\cap L_2}|=|G_{L_1L_2/L_2}|=|I_{L_1}I_{L_2}/I_{L_1}|$. Also we deduce $I_{L_1}\subset I_{L_2}\iff L_2\subset L_1$, thus by canonical isomorphism, groups containing $\operatorname{Nm}_{L/K}A_L$ are one-to-one correspondence with middle fields of L/K by counting numbers. □

Remark (14.6.1.9). This shows the philosophy of CFT, i.e. the property of Abelian extensions of a field is can be read from its multiplicative group structure. Of course, determining and characterizing these norm groups requires some work. ⌟

Weil Groups

Main references are[A-T67].

2 Local Class Field Theory

Notation (14.6.2.1).

- Let $K \in p$-`LField`.
- Let L/K be a finite extension field.

⌟

Unramified Extensions

Lemma (14.6.2.2). If L/K is unramified, then $H^q(G_{L/K}, \mathcal{O}_L^*) = 0$ for all q. ⌟

Proof: Cf.[Neukirch P83]. □

Prop. (14.6.2.3) [Witt Residues]. The unramified extensions of K form a class formation. ⌟

Proof: We first define the inv map: use the exact sequence $1 \to \mathcal{O}_L^* \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 0$, using the lemma(14.6.2.2), we have an isomorphism

$$H^2(\mathrm{Gal}(L/K), L^\times) \xrightarrow{v_L} H^2(\mathrm{Gal}(L/K), \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) = \mathrm{Gal}(L/K)^\vee.$$

And there is an isomorphism

$$\varphi : \mathrm{Gal}(L/K)^\vee \cong \frac{1}{[L;K]}\mathbb{Z}/\mathbb{Z}, \quad \varphi(\chi) = \chi(\varphi_{L/K})$$

where $\varphi_{L/K}$ is the Frobenius which generates $\mathrm{Gal}(L/K)$. Then define

$$\mathrm{inv}_{L/K} = \varphi \circ \delta^{-1} \circ v_L : H^2(\mathrm{Gal}(L/K), L^\times) \cong \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

To verify this is a class formation, we should verify(14.6.1.1), Cf.[Neukirch P85]**?**. □

Prop. (14.6.2.4) [Local Norm Symbol is given by Frobenius]. If L/K is unramified, then $(a, L/K) = \varphi_{L/K}^{v_K(a)}$. The same holds for L replaces by K^{ur}, in which case

$$1 \to \mathcal{O}_K^* \to K^\times \to \mathrm{Gal}(K^{\mathrm{ur}}/K) \to 0$$

is exact. Cf[Neukirch P88]. ⌟

Proof: We use(14.6.1.5), then $\chi(a, L/K) = \mathrm{inv}_{L/K}(\overline{a} \cup \delta\chi) = \varphi \circ \delta^{-1} \circ v_K(\overline{A} \smile \delta\chi) = \varphi(\delta^{-1}(v_K(a)\delta\chi)) = \varphi(v_K(a)\chi) = v_K(a)\chi(\varphi_{L/K}) = \chi(\varphi_{L/K}^{v_K(a)})$, for any χ. The second assertion follows from the last prop(14.6.2.5). □

Cor. (14.6.2.5) [Norm Group of Unramified Extensions]. The norm group of an unramified extension of degree f is

$$\mathcal{O}_K^* \times (\varpi_K^f)^{\mathbb{Z}}.$$

In particular, L/K is unramified iff $\mathcal{O}_K^* \subset \mathcal{N}_{L/K}$. ⌟

Ramified Extensions

Lemma (14.6.2.6). If L/K is normal, then $\#H^2(L/K)\Big|[L:K]$. ⌟

Proof: Cf.[Neukirch CFT P89]. Should use the fact that $G_{L/K}$ is solvable and Herbrand quotient. □

Lemma (14.6.2.7) [Invariant Maps]. If L/K is normal and L'/K is another unramified extension of the same degree, then $H^2(L/K)=H^2(L'/K)\subset \mathrm{Br}(K)$. In particular, we can define an invariant map $\mathrm{inv}:\mathrm{Br}(K)\to\mathbb{Q}/\mathbb{Z}$. ⌟

Proof: In view of(14.6.2.6) and(14.6.2.3), we only need to prove $H^2(L'/K)\subset H^2(L/K)$. For this, we let $N=LL'$, then there is an exact sequence(8.7.1.13)

$$1\to H^2(L/K)\to H^2(N/K)\xrightarrow{\mathrm{res}_L} H^2(N/L)$$

then we only need to prove $\mathrm{res}_L(c)=0$, and this follows from $\mathrm{inv}_{N/L}(\mathrm{res}_L\, c)=0$. This will follow, if we have

$$\mathrm{inv}_{N/L}(\mathrm{res}_L\, c)=[L:K]\cdot\mathrm{inv}_{L'/K}\, c.$$

This follows from(14.6.2.8). □

Lemma (14.6.2.8). For two subextensions L/K, L'/K in M/L normal with L'/K unramified extension, $N=LL'$, for $c\in H^2(L'/K)$,

$$\mathrm{inv}_{N/L}(\mathrm{res}_L c)=[L:K]\cdot\mathrm{inv}_{L'/K}c.$$

⌟

Proof: Cf[Neukirch CFT P90]. □

Lemma (14.6.2.9). $(\mathrm{Gal}_K,(K^{\mathrm{sep}})^\times,\mathrm{inv}_K)$ forms a class formation. ⌟

Proof: This almost follows from that of unramified extensions(14.6.2.3). We verify axioms(14.6.1.1) that inf is natural and commutes with res. It is natural because it is natural on unramified extensions, it commutes with res because we can assume $c\in H^2(L'/K)$ unramified and use(14.6.2.8). □

Cor. (14.6.2.10) [Local Artin's Reciprocity Law]. Let L/K be a normal extension, then the homomorphism

$$u_{L/K}\cup - : H^q(\mathrm{Gal}(L/K),\mathbb{Z})\cong H^{q+2}(L/K)$$

is an isomorphism. ⌟

Cor. (14.6.2.11). $H^3(L/K)=1, H^4(L/K)=\mathrm{Gal}^{\mathrm{ab}}(L/K)^\vee$, by(8.7.1.6). ⌟

Thm. (14.6.2.12) [Artin's Reciprocity Law]. By(14.6.1.4), cup product with the fundamental class in $H^2(L/F)$ define an isomorphism

$$\theta_{L/K}:\mathrm{Gal}^{\mathrm{ab}}(L/K)\cong H^{-2}(\mathrm{Gal}(L/K),\mathbb{Z})\to H^0(L/K)=K^\times/\mathrm{Nm}_{L/K}L^\times,$$

called the **Nakayama map**. And the reverse map is called the **norm residue symbol**$(-,L/K)$

$$1\to\mathrm{Nm}_{L/K}L^\times\to K^\times\xrightarrow{(-,L/K)}\mathrm{Gal}^{\mathrm{ab}}(L/K)\to 1.$$

This norm residue symbols induce an **Artin map**

$$\mathrm{Art}_K=(-,K):K^\times\to\mathrm{Gal}_K^{\mathrm{ab}}$$

with dense image. ⌟

Cor. (14.6.2.13). By(14.6.1.6), there are commutative diagrams

$$\begin{array}{ccc} K^\times & \xrightarrow{(-,N/K)} & \mathrm{Gal}(N/K)^{\mathrm{ab}} \\ \downarrow \mathrm{id} & & \downarrow \mathrm{pr} \\ K^\times & \xrightarrow{(-,L/K)} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} K^\times & \xrightarrow{(-,N/K)} & \mathrm{Gal}(N/K)^{\mathrm{ab}} \\ \mathrm{Nm}_{L/K} \uparrow \downarrow i & & i \uparrow \downarrow \mathrm{Ver} \\ L^\times & \xrightarrow{(-,N/L)} & \mathrm{Gal}(N/L)^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} L^\times & \xrightarrow{(-,N/L)} & \mathrm{Gal}(N/L)^{\mathrm{ab}} \\ \downarrow \sigma & & \downarrow \sigma^* \\ \sigma L^\times & \xrightarrow{(-,\sigma N/\sigma L)} & \mathrm{Gal}(\sigma N/\sigma L)^{\mathrm{ab}} \end{array}$$

Where Ver is the transfer map defined in**??**. ⌟

Cor. (14.6.2.14) [Quadratic Character]. If L/K is a quadratic extension, then $\mathcal{N}_{L/K}$ is a subgroup of $K^\times$ of order 2. Let χ be the non-trivial character of $K^\times$ that is trivial on $\mathcal{N}_{L/K}$, called the **quadratic character** of $K^\times$ attached to L/K. ⌟

Prop. (14.6.2.15) [Higher Ramification Groups]. For an Abelian extension L/K, the higher principal units U_K^n are mapped under the higher ramification groups of $G_{L/K}$ under the upper numbering. **?** ⌟

Proof: □

Def. (14.6.2.16) [Conductors]. If L/K is Abelian, define the **conductor** $\mathfrak{f}_{L/K}$ to be the smallest positive integer n s.t. $U_K^n \subset \mathcal{N}_{L/K}$. ⌟

Cor. (14.6.2.17). For an Abelian extension L/K, $\mathfrak{f}_{L/K} = 1$ iff L/K is unramified, by(14.6.2.5). ⌟

Characterize the Norm Groups of $K^\times$

Prop. (14.6.2.18) [Norm Group and Abelian Extension]. The map $L \mapsto \mathcal{N}_{L/K}$ defines a inclusion reversing isomorphism between the lattice of Abelian extension L of K and the lattice of norm groups of $K^\times$, i.e.:

$$\mathcal{N}_{L_1L_2/F} = \mathcal{N}_{L_1/K} \cap \mathcal{N}_{L_2/K}, \quad \mathcal{N}_{L_1\cap L_2/K} = \mathcal{N}_{L_1/K} \cdot \mathcal{N}_{L_2/K}.$$

And any group that contains a norm group is a norm group. This follows from(14.6.1.8) and (14.6.2.9). ⌟

Prop. (14.6.2.19). The norm groups are precisely the open(closed) subgroups of finite index in K^*. In fact finite index are itself open because it contains $(K^\times)^n$ which is open. ⌟

Proof: One part follows from(14.6.2.18) and the fact that $(K^*)^m$ is open(14.2.3.7). For the converse, we only need to prove $(K^*)^m$ is a norm group. This uses Kummer theory and Cf.[Neukirch CFT P96]. □

Prop. (14.6.2.20) [Norm Groups of Local Fields]. The norm groups of K^* are exactly the groups containing $U_K^n \times (\pi^f)$ for some n, f. ⌟

Proof: $U_K^n \times (\pi^f)$ is a norm group because it is closed of finite index. Conversely, any norm group contains some U_K^n because it is open and contains some (π^f) because it is of finite index. □

Local Weil Groups

Prop. (14.6.2.21)[Weil Groups]. The Artin map $\mathrm{Art}_K : K^\times \to \mathrm{Gal}_K^{\mathrm{ab}}$ is injective because $(K^\times)^n$ are all norm groups by(14.6.2.19), so the kernel is their intersection with is 1 by(14.2.3.7). It image is just W_K^{ab}. ⌟

Prop. (14.6.2.22)[Norm on Weil Groups]. The Artin map(14.6.2.21) gives a norm $|x| = |\,\mathrm{Art}^{-1}(x)|$ on W_K^{ab}, which maps a lift of the geometric Frobenius in Gal_κ to q^{-1}. ⌟

Totally Ramified Extensions

References are [L-T65].

Notation (14.6.2.23).

- Use notations defined in Lubin-Tate Formal Group Law.

⌟

Prop. (14.6.2.24) [Tate Modules]. There is an isomorphism of $\mathcal{O}$-modules $\Lambda_{f,n} \cong \mathcal{O}/\pi^n\mathcal{O}$, Cf.[Neukirch CFT P101]. Thus the automorphism of $\Lambda_{f,n}$ is all of the form u_f for units, isomorphic to U_K/U_K^n.

So we can define a **Tate module** $TG = \varprojlim \ker[\pi_K^n]$, it is a free $\mathcal{O}_K$-module of rank 1. ⌟

Def. (14.6.2.25)[Lubin-Tate Character]. As TG is a free $\mathcal{O}_G$-module of dimension 1, and Gal_K acts on TG, there can be attached a **Lubin-Tate character** $\chi_K : \mathrm{Gal}_K \to \mathcal{O}_K^*$ by $g(\alpha) = [\chi_K(g)](\alpha)$, this depends on π_K, but its restriction on I_K doesn't depend on π_K, and is just the local CFT isomorphism composed with $x \to x^{-1}$. ⌟

Proof: $[\chi_K(g)]$ is, by definition, the morphism that is id on K^{ur} and g on L_π. So it equals g on all K^{ab} iff g is id on K^{ur}, that is, $g \in I_K$. So if $g \in I_K$, by local CFT, $(\chi(g))^{-1}$ corresponds to g, uniquely. □

Prop. (14.6.2.26). $G_{\pi,n} \cong \mathcal{O}_K^*/U_K^n$, thus we have $G_\pi \cong \mathcal{O}_K^*$. $L_{\pi,n}/K$(9.5.3.26) is Abelian totally ramified of degree $p^{n-1}(p-1)$ generated by a Eisenstein polynomial with constant coefficient ϖ. In particular, ϖ is in the norm group.

⌟

Proof: For this, first note Galois action induce an isomorphism on $\Lambda_{f,n}$, thus correspond to an element of U_K/U_K^n by(14.6.2.24), this is an injection because $\Lambda_{f,n}$ generate $L_{\pi,n}$. Then we use the canonical polynomial $f(Z) = \pi Z + Z^q$, $f^n = f^{n-1}\varphi(n)$, where $\varphi(n)$ is a Eisenstein polynomial, thus $L_{\pi,n}/K$ is totally ramifies with $|G_{\pi,n}| = q^{n-1}(q-1) = |U_K/U_K^n|$, thus the result. □

Prop. (14.6.2.27)[Explicit Local Norm Residue Symbol]. Now we can write the universal residue symbol little bit more explicitly. For $a = u\varpi^m$, (a, K) acts as φ^m on K^{ur}, and on $L_{\pi,n}$, its action is generated by the action $(u^{-1})_f$ on the generating set $\Lambda_{f,n}$.

Thus the norm group of $L_{\pi,n}$ is just U_K^n by(14.6.2.26). ⌟

Proof: Cf.[Neukirch CFT P106].**?** □

Cor. (14.6.2.28)[Norm Groups of Totally Ramified Extensions]. The norm groups of the totally ramified Abelian extension are precisely the groups that contains some $U_K^n \times \varpi^{\mathbb{Z}}$ for some uniformizer π. And every totally ramified Abelian extension L/K is contained in some $L_{\varpi,n}$. ⌟

Proof: For any totally ramified extension, choose a uniformizer, then its norm is a uniformizer ϖ of K. And $\mathrm{Nm}_{L/K}$ is open, thus it contains some U^n. The rest follows from local CFT(14.6.2.18). □

Cor. (14.6.2.29)[Maximal Abelian Extension of p-adic Local Fields]. Let $L_\pi = \cup L_{\pi,n} = K(\Lambda_f)$, where $\Lambda_f = \cup \Lambda_{f,n}$, then $T \cdot L_\pi$ is the maximal Abelian extension of K. Hence $G_K^{\mathrm{ab}} = G_{T,K} \times G_\pi$. ⌟

Proof: This follows immediately from(14.6.2.20). □

Cor. (14.6.2.30) [Hasse-Arf]. We can prove Hasse-Arf(14.2.2.27) in the case where K is a local field. This is because we already know the maximal Abelian extension, and $G(K^{\mathrm{ab}}/T) \cong G(L_\pi/K) \cong \mathbb{Z}_p$ for which we know the Galois action well(14.6.2.24)(14.6.2.26), so $i(\sigma) = v(\sigma(\alpha_n) - \alpha_n) = v([\sigma - 1](\alpha))$, which jumps at U_K^n(the same pattern as $K = \mathbb{Q}_p$(14.2.2.29)), thus the result. ⌟

Example (14.6.2.31) [Cyclotomic Fields]. When $K = \mathbb{Q}_p$, we can choose $f(T) = (1+T)^p - 1$, thus $L_{\varpi,n}$ is just $\mathbb{Q}_p(\zeta_{p^n})$. And we have $r_f = (1+T)^r - 1$, thus we have

$$(a, \mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)(\zeta_{p^n}) = \zeta_{p^n}^r$$

where $a = up^m$, and $r \equiv u^{-1} (\mathrm{mod}\ p^n)$. ⌟

3 Global Class Field Theory

Notation (14.6.3.1).
- Let $F \in \mathtt{GField}$.

⌟

Prop. (14.6.3.2). Let $\mathfrak{P}$ be a prime of L lying over $\mathfrak{p}$, then $H^q(G, I_L^{\mathfrak{p}}) \cong H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$. If $\mathfrak{p}$ is a finite unramified prime of L, then $H^q(G, U_L^{\mathfrak{p}}) = 1$ for all q. ⌟

Proof: Notice $I_L^{\mathfrak{p}} = \prod_{\sigma \in G/G_{\mathfrak{P}}} L_{\sigma\mathfrak{P}}^* = \prod_{\sigma \in G/G_{\mathfrak{P}}} \sigma L_{\mathfrak{P}}^*$ is an induced module, so by(8.7.2.7), we have $H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$, and similarly for $U_{\mathfrak{p}}$, which vanish by(14.6.2.2). □

Cor. (14.6.3.3).

$$H^q(G, I_L^S) = \bigoplus_{p \in S} H^q(G_{\mathfrak{P}/\mathfrak{p}}, L_{\mathfrak{P}}^*), \quad H^q(G, I_L) = \bigoplus_{p} H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*).$$

And the isomorphism is natural, by restriction to components. ⌟

Proof: For this, just notice $I_L = \cup_S I_L^S$, then use the last proposition, notice group cohomology commutes with colimits(8.7.2.2). □

Cor. (14.6.3.4). $H^1(G, \mathbf{I}_L) = H^3(G, \mathbf{I}_L) = 0$, by(14.6.2.11). ⌟

Cor. (14.6.3.5). An idele $\mathfrak{a} \in \mathbf{I}_F$ is the norm of an idele $\mathfrak{b}$ in $\mathbf{I}_L$ if each component $\mathfrak{a}_{\mathfrak{p}}$ is the norm of an element $b_{\mathfrak{P}} \in L_{\mathfrak{P}}^*$. ⌟

Prop. (14.6.3.6). The decomposition commutes with inf, res and cor. Cf.[Neukirch CFT P125]. ⌟

Cyclic Class Formations

Lemma (14.6.3.7). For a cyclic extension L/F of order p, C_L is a Herbrand module with Herbrand quotient $h(C_L) = p$. ⌟

Proof: □

Prop. (14.6.3.8) [First Fundamental Inequality]. $[C_F : \mathrm{Nm}_{L/F} C_L] \geq p$ ⌟

Proof: □

Prop. (14.6.3.9). If $\mathbb{Q}(\zeta_p) \subset F$ and L/F is a cyclic extension of order p, then $[C_F : \mathrm{Nm}_{L/F} C_L] \leq p$. ⌟

Proof: □

Cor. (14.6.3.10) [Second Fundamental Inequality]. If L/F is a cyclic extension of order p, then $[C_F : \mathrm{Nm}_{L/F} C_L] = p$. ⌟

Proof: □

Cor. (14.6.3.11) [Hasse Norm Principle]. For a cyclic extension L/F and $a \in F^\times$, $a \in \mathrm{Nm}_{L/F} L^\times$ iff $a \in \mathrm{Nm}_{L/F}(\mathbf{I}_L)$. ⌟

Proof: Use the long exact sequence for $1 \to L^\times \to \mathbf{I}_L \to C_L \to 1$, we see that $H^0(G, L^\times) \to H^0(G, \mathbf{I}_L)$ is an injection, which is

$$F^\times / \mathrm{Nm}_{L/F} L^\times \hookrightarrow \bigoplus_p F_\mathfrak{p}^\times / \mathrm{Nm}_{L_\mathfrak{P}/F_\mathfrak{p}} L_\mathfrak{P}^\times.$$

In fact, by(14.6.3.4), we say that this is equivalent to $H^1(\mathrm{Gal}(L/K), C_L) = 1$, which is equivalent to second fundamental inequality. □

Remark (14.6.3.12). WARNING: the Hasse norm principle is not true for non-cyclic Galois extensions, for examples $\mathbb{Q}(\sqrt{13}, \sqrt{17})/\mathbb{Q}$. ⌟

General Class Formations

Prop. (14.6.3.13). For L/F normal, $\#H^2(G, C_L) | [L : F]$. ⌟

Proof: Cf.[Neukirch P137]. □

Prop. (14.6.3.14).

$$\mathrm{Br}(F) = \bigcup_{L/F \text{ cyclic}} H^2(\mathrm{Gal}(L/F), L^\times), \quad H^2(\mathrm{Gal}_K, \mathbf{I}_{\overline{K}}) = \bigcup_{L/K \text{ cyclic}} H^2(\mathrm{Gal}(L/K), \mathbf{I}_L).$$

⌟

Proof: Cf,[Neukirch P127]. □

Def. (14.6.3.15) [Invariant Maps]. For $c = (c_\mathfrak{p}) \in H^2(G_{L/K}, I_L)$, define the **invariant map**

$$\mathrm{inv}_{L/K} c = \sum_\mathfrak{p} \mathrm{inv}_{L_\mathfrak{P}/K_\mathfrak{p}} c_\mathfrak{p} \text{(14.6.2.9)}.$$

⌟

Prop. (14.6.3.16). If $c \in H^2(G_{L/K}, L^\times)$, then $\mathrm{inv}_{L/K} c = 0$. ⌟

Proof: Cf.[Neukirch P141]. □

Cor. (14.6.3.17). Now we can define the inv map for C_K. By the exact sequence $1 \to L^* \to I_L \to C_K \to 1$, we have

$$1 \to H^2(\mathrm{Gal}(L/K), L^*) \to H^2(\mathrm{Gal}(L/K), I_L) \to H^2(\mathrm{Gal}(L/K), C_L) \to H^3(G_{L/K}, L^*)$$

The last one is 1 if L/K is cyclic, thus tby this proposition, inv is defined for $H^2(G_{L/K}, C_L)$. ⌟

Prop. (14.6.3.18) [Reduce to Cyclic Case]. If L/K is normal and L'/K is cyclic with the same degree, then $H^2(L'/K) = H^2(L/K) \subset H^2(\overline{K}/K)$. ⌟

Proof: □

Cor. (14.6.3.19). $H^2(\overline{K}/K) = \cup_{L/K \text{ cyclic}} H^2(L/K)$, thus the homomorphism $H^2(\mathrm{Gal}_K, I_{\overline{K}}) \to H^2(\overline{K}/K)$ is surjective by(14.6.3.17). ⌟

Proof: Why can always find such a cyclic extension**?**. □

Cor. (14.6.3.20). The inv map is defined for $H^2(\overline{K}/K)$, and $\mathrm{inv}_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ is an isomorphism for every normal extension L/K. ⌟

Lemma (14.6.3.21) [Main Lemma]. The formation $(\mathrm{Gal}_F, C_{F^{\mathrm{sep}}}, \mathrm{inv}_F)$ is a class formation(14.6.1.1). ⌟

Proof: □

Thm. (14.6.3.22) [Artin's Reciprocity Law, Artin1927]. By(14.6.1.4), cup product with fundamental classes $u_{L/F} \in H^2(L/F)$ define an isomorphism

$$\theta_{L/F} : \mathrm{Gal}^{\mathrm{ab}}(L/F) \cong H^{-2}(\mathrm{Gal}(L/F), \mathbb{Z}) \to H^0(L/F) = C_F / \mathrm{Nm}_{L/F} C_L,$$

called the **Nakayama isomorphism**. And the reverse map is called the **norm residue symbol** map $(-, L/F)$

$$1 \to \mathrm{Nm}_{L/F} C_L \to C_F \xrightarrow{(-,L/F)} \mathrm{Gal}^{\mathrm{ab}}(L/F) \to 1.$$

These norm residue symbols induce an **Artin map**

$$\mathrm{Art}_F = (-, F) : C_F \to \mathrm{Gal}_F^{\mathrm{ab}}$$

⌟

Prop. (14.6.3.23) [Local-Global Compatibility]. For L/F Abelian and $\mathfrak{a} \in I_F$:

$$(\mathfrak{a}, L/F) = \prod_{\mathfrak{p}} (a_{\mathfrak{p}}, L_{\mathfrak{P}}/K_{\mathfrak{p}}) \in \mathrm{Gal}^{\mathrm{ab}}(L/F)(14.6.2.12).$$

In particular, if $v \in \Sigma_F^{\mathrm{fin}}$ is unramified in L, then

$$([\varpi_{\mathfrak{p}}]_{\mathfrak{p}}, L/F) = \mathrm{Frob}_{L_{\mathfrak{P}}/F_{\mathfrak{p}}} \in \mathrm{Gal}_{L_{\mathfrak{P}}/F_{\mathfrak{p}}} \subset \mathrm{Gal}_F .$$

⌟

Proof: Cf.[Neukirch CFT P154]. □

Prop. (14.6.3.24). There are commutative diagrams:

$$\begin{array}{ccc} C_F & \xrightarrow{(-,N/F)} & \mathrm{Gal}(N/F)^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{pr}} \\ C_F & \xrightarrow{(-,L/F)} & \mathrm{Gal}(L/F)^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} C_F & \xrightarrow{(-,N/F)} & \mathrm{Gal}(N/F)^{\mathrm{ab}} \\ {\scriptstyle \mathrm{Nm}_{L/F}}\uparrow\downarrow{\scriptstyle i} & & {\scriptstyle i}\uparrow\downarrow{\scriptstyle \mathrm{Ver}} \\ C_L & \xrightarrow{(-,N/L)} & \mathrm{Gal}(N/L)^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} C_L & \xrightarrow{(-,N/L)} & \mathrm{Gal}(N/L)^{\mathrm{ab}} \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma^*} \\ C_{\sigma L} & \xrightarrow{(-,\sigma N/\sigma L)} & \mathrm{Gal}(\sigma N/\sigma L)^{\mathrm{ab}} \end{array}$$

Where Ver is the transfer map defined in**??**. ⌟

Proof: □

Cor. (14.6.3.25). By(14.6.1.8), the map $L \mapsto \mathcal{N}_{L/F} = \mathrm{Nm}_{L/F} C_L$ defines a inclusion reversing isomorphism between the lattice of Abelian extension L/K and the lattice of norm groups of C_F, i.e.:

$$\mathcal{N}_{L_1L_2/F} = \mathcal{N}_{L_1/F} \cap \mathcal{N}_{L_2/F}, \quad \mathcal{N}_{L_1\cap L_2/F} = \mathcal{N}_{L_1/F}\cdot\mathcal{N}_{L_2/F}.$$

And any group that contains a norm group is a norm group. ⌟

Prop. (14.6.3.26) [Existence Theorem]. The norm groups of C_F are precisely the (open)closed subgroups of finite index. ⌟

Proof: Cf.[Neukirch P162] or notes taken by Chao Li.**?** □

Cor. (14.6.3.27) [The Kernel of Art_F].

- If $F \in$ `NField`, the kernel $\cap_{L/F}\mathcal{N}_{L/F}$ of Art_F is exactly the connected component D_F of $1 \in C_F$, which is the group of divisible elements in C_K(14.4.4.29). Moreover, $\mathrm{Art}_F : C_F/D_F \to \mathrm{Gal}_F^{\mathrm{ab}}$ is an isomorphism.
- If $F \in$ `FField`, then Art_F is injective but not surjective. In fact, there is an exact sequence(**?** by etale fundamental group)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{I}_F^1/F^\times & \longrightarrow & \mathbf{I}_F/F^\times & \longrightarrow & q^{\mathbb{Z}} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\cong} & & \downarrow{\scriptstyle(-,F)} & & \downarrow & & \\ 0 & \longrightarrow & I_F^{\mathrm{ab}} & \longrightarrow & \mathrm{Gal}_F^{\mathrm{ab}} & \longrightarrow & \mathrm{Gal}_k \cong \widehat{\mathbb{Z}} & \longrightarrow & 0 \end{array}$$

thus C_F can be regarded as the Weil group of F.

⌟

Proof: 1: As $\mathrm{Gal}_F^{\mathrm{ab}}$ is totally disconnected, it must factors through D_F. But C_F/D_F is a profinite group, thus D_F is an intersection of open subgroups of finite index, thus it is in the kernel, by(14.6.3.26).

2: The map is injective because by splitting it is a product of $q^{\mathbb{Z}}$ and a profinite group, thus the intersection of open subgroups of finite index is trivial(14.6.3.26). To show the diagram is commutative, it suffices to show that (x, F) acts as $\mathrm{Frob}_k^{|x|_F}$ on $\overline{k}$: This is because on any finite unramified Abelian extension L/F, (x, F) acts via $\varphi_{L_w/F_v}^{|x_v|_v}$ by definition(14.6.2.4), and these add up to $|x|_v$ as L/F is cyclic. □

4 Decomposition Law

Prop. (14.6.4.1). If L/F is an Abelian extension, then $\mathcal{N}_{L/K} \cap K_{\mathfrak{p}}^{\times} = \mathcal{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$. ⌟

Proof: For the non-trivial part, notice if $\mathfrak{a} \in N_{\mathfrak{P}} L_{\mathfrak{P}}^*$ is a norm times a $a \in K^*$, then it is a norm at all primes except $\mathfrak{p}$, thus it is also norm at $\mathfrak{p}$ by the multiplicative definition of the inv map(14.6.3.15). □

Cor. (14.6.4.2)[Ramifications]. Let L/K be an Abelian extension of global fields and $\mathcal{N} = \mathrm{Nm}_{L/K} C_L$ be the norm group, then

- $\mathfrak{p}$ is unramified in L iff $\mathcal{O}_{F,\mathfrak{p}}^* \subset \mathcal{N}_{L/F}$.
- $\mathfrak{p}$ splits completely in L iff $F_{\mathfrak{p}}^{\times} \subset \mathcal{N}_{L/F}$.

⌟

Proof: □

Prop. (14.6.4.3)[Decomposition Law]. Let L/F is an Abelian extension of degree n and $\mathfrak{p} \in \mathrm{Unr}(F)$ and $\varpi_{\mathfrak{p}}$ is a uniformizer, then if f is the smallest positive integer s.t. $[\varpi_{\mathfrak{p}}]_{\mathfrak{p}}^f \in \mathcal{N}_{L/F}$, then $\mathfrak{p}$ factors in the extension L into $r = n/f$ distinct primes of degree f.

Notice to determine whether a place is ramified or not, we can use criterion(14.6.4.17). ⌟

Proof: The degree the extension of $\mathfrak{p}$ is just the order of the Frobenius automorphism of $G_{\mathfrak{P}/\mathfrak{p}}$, which is just the order in $\mathrm{Gal}(L/F) \cong C_F/\mathrm{Nm}_{L/F} C_L$. The Frobenius of $\mathfrak{p}$ correspond exactly to $(\ldots, 1, \pi, 1, \ldots)$ by(14.6.3.23) and(14.6.2.4), so the result follows. □

Prop. (14.6.4.4) [Unramified Kummer Extensions are Rare]. Let F be a global field or the function field of a smooth curve over an alg.closed field k, and $S \subset \Sigma_F$ be a finite set of places, and $m \in \mathbb{Z} \cap F^*$, then there are only f.m. Kummer extensions over F that have Galois group of exponent m and are unramified at all finite places outside S. ⌟

Proof: We may add all the m-th roots of unity to F. Then by Kummer theory(3.2.8.9), Kummer extensions of exponent m over F corresponds to $F(\sqrt[m]{a})$, where $a \in F$. But we can only add those a s.t. $\mathrm{ord}_v(a) \equiv 0 \mod m$ in order to get unramified extensions, so the desired Kummer extensions correspond to

$$T_S = \{a \in F^{\times}/(F^{\times})^n \,|\, \mathrm{ord}_v(a) \equiv 0 \mod m, \forall v \in \Sigma_K^0 \backslash S\}.$$

If F is a global field, after enlarging S, we may assume $\mathcal{O}_{K,S}$ is PID, then this group is a quotient of $\mathcal{O}_{K,S}^*/\mathcal{O}_{K,S}^m$, which is finite by unit theorem(14.4.4.30). If $F = K(C)$, where C is a complete non-singular curve, then by Riemann-Roch there is an exact sequence

$$0 \to T_{\varnothing} \to T_S \to (\mathbb{Z}/(m))^{\#S} \to 0$$

And for $f \in T_{\varnothing}$, $\mathrm{div}(f) = mD_f$ for some $D_f \in \mathrm{Pic}(C)[m]$. Notice $\#\mathrm{Pic}(C)[m] < \infty$ by(6.12.2.18), thus the theorem follows. □

Ray Class Fields

Def. (14.6.4.5) [Notations].

- A **modulus** $\mathfrak{m}$ is a a formal product $\prod_{\mathfrak{p} \in \Sigma_F} \mathfrak{p}^{e_{\mathfrak{p}}}$ where $e_{\mathfrak{p}} \geq 0$, and $e_{\mathfrak{p}} = 0$ if $\mathfrak{p} \in \Sigma_F^{\mathbb{C}}$, and $e_{\mathfrak{p}} = 0, 1$ if $\mathfrak{p} \in \Sigma_F^{\mathbb{R}}$.

- For a modulus $\mathfrak{m}$,

$$U^{\mathfrak{m}} = \prod_{v\in\Sigma_F^\infty, e_v=0} F_v^\times \times \prod_{v\in\Sigma_F^{\mathbb{R}}, e_v=1} \mathbb{R}_+^\times \times \prod_{\mathfrak{p}\in\Sigma_F^{\text{fin}}, e_\mathfrak{p}=0} F_\mathfrak{p} \times \prod_{\mathfrak{p}\in\Sigma_F^{\text{fin}}, e_\mathfrak{p}>0} (1+\mathfrak{p}^{e_\mathfrak{p}}) \subset \mathbf{I}_F$$

and $C^{\mathfrak{m}}$ is the image of $U^{\mathfrak{m}}$ in C_F, which is an open subgroup of finite index.

⌟

Def. (14.6.4.6) [Ray Class Fields]. For a modulus $\mathfrak{m}$,

- $F_\mathfrak{m}$ is defined to be the Abelian extension of F corresponding to $C^{\mathfrak{m}}$ via(14.6.3.26), called the **ray class field** of $\mathfrak{m}$. in particular, $\text{Gal}(F_\mathfrak{m}/F) \cong C_F/C^{\mathfrak{m}}$ via Artin's map(14.6.3.22).
- $J^{\mathfrak{m}}$ is defined to be the group of all ideals of $\mathcal{O}_F$ relatively prime to $\mathfrak{m}$, $P^{\mathfrak{m}} = F^\times \cap U^{\mathfrak{m}}$, called the **ray mod** $\mathfrak{m}$.

⌟

Def. (14.6.4.7) [Ray Class Groups]. For a modulus $\mathfrak{m}$,

$$\text{Cl}_\mathfrak{m}(F) = J^{\mathfrak{m}}/P^{\mathfrak{m}} \cong C_F/C^{\mathfrak{m}} \cong \text{Gal}(F^{\mathfrak{m}}/F)$$

is finite, called the **ray class group** of $\mathfrak{m}$. ⌟

Proof: This is because $\text{Cl}_\mathfrak{m}(F)$ is a quotient group of $I_F/U^{\mathfrak{m}}$, which is finite. □

Prop. (14.6.4.8). Any finite Abelian extension is contained in a finite ⌟

Cor. (14.6.4.9) [Cyclotomic Fields]. When $F = \mathbb{Q}, m \in \mathbb{Z}_+$ and $\mathfrak{m} = m \cdot \infty$, $\mathbb{Q}_\mathfrak{m} = \mathbb{Q}(\zeta_m)$.

In particular, we can think of the ray classes fields for general function fields as "generalized cyclotomic fields". ⌟

Proof: For any $p \in \mathbf{P}$, let $m = \mathfrak{p}^{e_p} \times m'$, then $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{p^{e_p}})\mathbb{Q}(\zeta_{m'})$. Notice both $\mathcal{N}_{\mathbb{Q}(\zeta_{p^{e_p}})/\mathbb{Q}}$ and $\mathcal{N}_{\mathbb{Q}(\zeta_{m'})/\mathbb{Q}}$ contains $(1+\mathfrak{p}^{e_p})$ by(14.6.2.31)(14.6.2.27) and(14.6.2.5). Thus by(14.6.3.25), the $\mathcal{N}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}$ als contains $(1+\mathfrak{p}^{e_p})$. Thus $U^{\mathfrak{m}}$ is contained in $\text{Nm}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} I_{\mathbb{Q}(\zeta_m)}$.

To show the reverse inclusion, we calculate $(C_\mathbb{Q} : C^{\mathfrak{m}})$. As $(C_\mathbb{Q} : C_\mathbb{Q}^1) = \text{Cl}(\mathbb{Q}) = 1$,

$$(C_\mathbb{Q} : C^{\mathfrak{m}}) = (U_\mathbb{Q}^1\mathbb{Q}^\times : U_\mathbb{Q}^{m\infty}\mathbb{Q}^\times) = (U_\mathbb{Q}^1 : U_\mathbb{Q}^{m\infty})(U_\mathbb{Q}^1 \cap \mathbb{Q}^\times : U_\mathbb{Q}^{m\infty} \cap \mathbb{Q}^\times) = \varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}].$$

□

Cor. (14.6.4.10) [Kronecker]. Every Abelian extension $F/\mathbb{Q}$ is a subfield of $\mathbb{Q}(\zeta_m)$ for some $m \in \mathbb{Z}_+$. ⌟

Def. (14.6.4.11) [Hilbert Class Fields]. The ray class field of F mod 1 is called the **Hilbert class field** of F, denoted by F_1 or $\text{H}(F)$. Its Galois group is isomorphic to $C_F/C_F^1 \cong J_F/P_F = \text{Cl}(F)$(14.6.4.7). In particular, $[F_1 : F] = \text{cl}(F)$. ⌟

Conductors

Def. (14.6.4.12) [Admissible Modulus].

- For an Abelian extension of global fields L/F, an **admissible modulus** for L/F is a modulus $\mathfrak{m}$ s.t. $C^{\mathfrak{m}} \subset \text{Nm}_{L/F} C_L$ or equivalently $L \subset F_\mathfrak{m}$(14.6.4.6).
- All subgroups of $\text{Cl}_\mathfrak{m}(F)$(14.6.4.7) are called **ideal groups defined mod** $\mathfrak{m}$.

- If L/F is an Abelian extension with an admissible modulus $\mathfrak{m}$, then $H^{\mathfrak{m}}_{L/F} = \mathrm{Nm}_{L/F} J^{\mathfrak{m}}_L \cdot P^{\mathfrak{m}}_F$ is called the **ideal group defined mod** $\mathfrak{m}$.

⌟

Prop. (14.6.4.13). For an Abelian extension L/F, a modulus $\mathfrak{m}$ is admissible for L/F iff $U^{\mathfrak{m}} \subset N_{L/F}(I_L)$. ⌟

Proof: This is because $\mathcal{N}_{L/F} \cap K_p = \mathcal{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ by(14.6.4.1). □

Cor. (14.6.4.14). The norm subgroups of C_F are exactly those containing some $C^{\mathfrak{m}}$. ⌟

Proof: This is because $\mathcal{N}_{L/F} A_L$ is open in A_K, by(14.4.4.24), so it must contain some $U^{\mathfrak{m}}$. The converse is also clear. □

Def. (14.6.4.15) [Conductors]. For an Abelian extension of global fields L/F, by(14.6.4.14), there is a minimal admissible modulus for L/F, called the **conductor of** L/F, denoted by $\mathfrak{f}_{L/F}$. ⌟

Prop. (14.6.4.16) [Local and Global Conductors]. For an Abelian extension L/F,

$$\mathfrak{f}_{L/F} = \prod_{\mathfrak{p} \in \Sigma_F} \mathfrak{f}_{L_{\mathfrak{P}}/F_{\mathfrak{p}}} (14.6.2.16).$$

⌟

Proof: This follows from(14.4.4.24). □

Cor. (14.6.4.17) [Conductor Detects Ramifications]. Let L/F be an Abelian extension, then $\mathfrak{p} \in \Sigma_F$ is ramified in L/F iff $\mathfrak{p} \mid \mathfrak{f}_{L/F}$, by(14.6.2.16).

In particular, $\mathrm{Ram}(F_{\mathfrak{m}}/F) = S(\mathfrak{m})$. ⌟

Prop. (14.6.4.18). For a field K, if S is a finite set of primes that contains all the infinite primes and all the primes lying above the primes dividing n, and $I_K = I^S_K \cdot K^*$, then $C^n_K \cdot U^S_K$ is a norm group. If K contains the n-th roots of unity, then it corresponds to the Kummer extension $T = K(\sqrt[n]{K^S}/K)$. ⌟

Hilbert Class Fields

Prop. (14.6.4.19). The Hilbert class field F_1(14.6.4.11) is the maximal unramified Abelian extension of F, by(14.6.4.17). ⌟

Def. (14.6.4.20) [Hilbert Class Field Tower]. Let F be a global field, then let F_1 be the Hilbert class field of F, and for any $n \in \mathbb{Z}_+$, let F_{n+1} be the Hilbert class field of F_n, then such a series of extensions is called the **Hilbert class field tower** of F.

Similarly for $p \in \mathbf{P}$, we can consider the maximal Abelian p-extensions of F, which gives us a series

$$F \subset F^{(p)}_1 \subset F_2(p) \subset \ldots \subset F^{(p)}_\infty.$$

⌟

Prop. (14.6.4.21). Let F be a global field, then each F_n is Galois over F, and F_1 is the largest Abelian subfield of F_2/F. ⌟

Proof: For the last assertion, notice that that largest Abelian subfield of F_2/F is unramified Abelian over F, then use(14.6.4.19). □

Prop. (14.6.4.22) [Principal Ideal Theorem]. In the Hilbert class field over F, every ideal $\mathfrak{a}$ of F becomes a principal ideal. ⌟

Proof: As $J_F/P_F \cong C_F/C_F^1$, It suffices to show that the map $i: C_F \to C_{F_1}$ has image in $C^1_{F_1}$. By the commutative diagram(14.6.3.24)

$$\begin{array}{ccccccccc} & & & & C_K & \xrightarrow{(-,F_2/F)} & \mathrm{Gal}(F_2/F)^{\mathrm{ab}} & & \\ & & & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \mathrm{Ver}} & & \\ 0 & \longrightarrow & C^1_{F_1} & \longrightarrow & C_{F_1} & \xrightarrow{(-,F_2/F_1)} & \mathrm{Gal}(F_2/F_1)^{\mathrm{ab}} & \longrightarrow & 0 \end{array}$$

It suffices to show that Ver is trivial. Then this follows from(14.6.4.21) and(3.1.9.3). □

Thm. (14.6.4.23) [Brumer]. Let $F \in \texttt{NField}, p \in \mathbf{P}$, and $t_F^{(p)}$ be the number of primes $\ell \in \mathbf{P}$ s.t. $p|e_{\mathfrak{L}/\ell}$ for any prime $\mathfrak{L}$ above ℓ, then

$$\dim_{\mathbb{F}_p} \mathrm{Cl}(F)/(p) \geq t_F^{(p)} - 2(d-1)$$

⌟

Proof: □

Prop. (14.6.4.24)[Golod-Šafarevič]. Let F be a number field of degree d and $p \in \mathbf{P}$, if $[F_\infty^{(p)} : F] < \infty$, then

$$\dim_{\mathbb{F}_p} \mathrm{Cl}(F)/p\,\mathrm{Cl}(F) \leq 1 + 2\sqrt{d+1}.$$

⌟

Proof: □

Cor. (14.6.4.25). By(14.6.4.23), if $t_F^{(p)} \geq 2d + 2\sqrt{d+1}$, then $[F_\infty^{(p)} : F] = \infty$.

For example, if we take $F = \mathbb{Q}(\sqrt{d})$ where d is square-free with at least 8 different prime factors, then $[F_\infty^{(p)} : F] = \infty$. ⌟

Classical Formulation

Def. (14.6.4.26) [Artin Symbols]. There is a homomorphism $J^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ called the **Artin symbol** $(\frac{L/K}{-})$. On primes $\mathfrak{p}$, it maps a prime $\mathfrak{p}$ which is unramified by(14.6.4.12) to its local Frobenius $\mathrm{Frob}_{\mathfrak{p}} \in G_{\mathfrak{P}/\mathfrak{p}} \subset G_{L/K}$. This is well-defined only up to conjugacy in $\mathrm{Gal}(L/K)$, and thus well-defined when L/K is Abelian. ⌟

Lemma (14.6.4.27). If $\mathfrak{m}$ is an admissible modulus for L/K, the restriction to finite part defines isomorphism $\mathcal{N}_{L/F}/C^{\mathfrak{m}} \cong H^{\mathfrak{m}}_{L/F}/P^{\mathfrak{m}}$. ⌟

Proof: Cf.[Neukirch CFT P176]. □

Prop. (14.6.4.28) [Classical Artin Reciprocity Law]. If L/K is an Abelian extension and $\mathfrak{m}$ is an admissible modulus, then there is a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{N}_{L/K} & \longrightarrow & C_K & \xrightarrow{(-,L/K)} & G_{L/K} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & H^{\mathfrak{m}}_{L/K}/P^{\mathfrak{m}} & \longrightarrow & J^{\mathfrak{m}}/P^{\mathfrak{m}} & \xrightarrow{\left(\frac{L/K}{-}\right)} & G_{L/K} & \longrightarrow & 1 \end{array}$$

Thus the second row is exact by(14.6.3.22), and $\mathrm{Gal}(L/K) \cong J^{\mathfrak{m}}/H^{\mathfrak{m}}_{L/K}$. ⌟

Proof: Cf.[Neukirch CFT, P178]. □

Prop. (14.6.4.29) [Decomposition Law]. Let L/F is an Abelian extension of degree n with an admissible modulus $\mathfrak{m}$(e.g. the conductor) and $\mathfrak{p} \nmid \mathfrak{m}$. then if f is the smallest number that $\mathfrak{p}^f \in H^{\mathfrak{m}}_{L/F}$, then $\mathfrak{p}$ factors in the extension L into $r = n/f$ distinct primes of degree f. ⌟

Proof: The degree the extension of $\mathfrak{p}$ is just the order of the Frobenius automorphism of $G_{\mathfrak{P}/\mathfrak{p}}$, which is just the order in $G_{L/K} \cong J^{\mathfrak{m}}/H^{\mathfrak{m}}$. The Frobenius of $\mathfrak{p}$ correspond exactly to $\mathfrak{p}$ by(14.6.2.4), so the result follows. □

n-th Powers

Cf.[A-T67]Chap9,10.

Prop. (14.6.4.30) [Grünwald-Wang]. Let $F \in \mathtt{GField}$, $n = 2^t \cdot m \in \mathbb{Z}_+$, and assume $F \in \mathtt{FField}$ or $F(\zeta_{2^t})/F$ is cyclic. Then $a \in F$ is in F^n iff $a \in F_v^n$ for a.e. $v \in \Sigma_F$. ⌟

Proof: Cf.[Chao Li's notes] or [Mil20]P229. □

Thm. (14.6.4.31) [Grünwald-Wang]. Let $F \in \mathtt{GField}$, then for any $S \subset \Sigma_F$ finite, if for each $v \in S$, χ'_v is a continuous character of $F_v^\times$ of finite order n_v, then there exists a Hecke character χ of F with the $\chi_v = \chi'_v$. Moreover, if $n = \mathrm{lcm}(n_v), t = \mathrm{ord}_2(n)$, and assume $F \in \mathtt{FField}$ or $F(\zeta_{2^t})/F$ is cyclic, then χ can be taken to be of order n. ⌟

Proof: Cf.[Chao Li's notes] or [Artin-Tate, Class Field Theory, Thm10.5].? □

Cor. (14.6.4.32) [Local-Global Compatibility for Cyclic Extensions]. Let $F \in \mathtt{GField}$ and for each $v \in \Sigma_F$, a positive integer n_v is given s.t.

- For a.e. v, $n_v = 1$.
- For $v \in \Sigma_F^{\mathbb{R}}$, $n_v \in \{1, 2\}$.
- For $v \in \Sigma_F^{\mathbb{C}}$, $n_v = 1$.

⌟

Proof: The point is that we can choose χ_v s.t. the exceptions in(14.6.4.31) can be avoided, and then get a Hecke character χ of F or order n which corresponds to a cyclic extension via cyclic class formation. ?Cf.[Artin-Tate, Class Field Theory, Thm10.5, P105].? □

Higher Reciprocity Law

Cf.[Mil20]Chap8.

Prop. (14.6.4.33) [Quadratic Reciprocity]. ⌟

Prop. (14.6.4.34) [Cubic Reciprocity]. ⌟

Prop. (14.6.4.35) [Quadric Reciprocity]. ⌟

5 L-Series and Dirichlet Density

Def. (14.6.5.1). In this subsection, for two functions $f(s), g(s) : (1,\infty) \to \mathbb{C}$, write $f \overset{1}{\sim} g$ iff $f - g$ is bounded on $(1, 1+\varepsilon)$ for some $\varepsilon > 0$. ⌟

Def. (14.6.5.2) [Densities]. Let $F \in \texttt{NField}$ and $T \subset \Sigma_F^{\text{fin}}$, then T is said to have

- **polar density** $m/n \in \mathbb{Q}$ if
$$\zeta_{F,T} = \prod_{v\in T} \frac{1}{1 - ||v||^{-s}}$$
satisfies $\zeta_{F,T}^n$ extends to a nbhd of $s = 1$ with a pole of order n.
- **Dirichlet density** $\delta \in [0,1]$ iff
$$\sum_{\mathfrak{p}\in T} \frac{1}{||\mathfrak{p}||^s} \overset{1}{\sim} \frac{\delta}{s-1}.$$
- **natural density** $\delta \in [0,1]$ if
$$\lim_{X\to\infty} \frac{\#T \cap \{\mathfrak{p} \in \Sigma_F^0 : ||\mathfrak{p}|| \leq X\}}{\#\{\mathfrak{p} \in \Sigma_F^0 : ||\mathfrak{p}|| \leq X\}} = \delta.$$

⌟

Prop. (14.6.5.3). If the polar density exists, then so does the Dirichlet density, and they are equal. If the natural density exists, then so does the Dirichlet density, and they are equal. ⌟

Proof: Cf.[Mil20]P194. □

Thm. (14.6.5.4)[Effective Chebotarev]. For a Galois extension of number fields L/F and any subset $C \subset \mathrm{Gal}(L/F)$ that is stable under conjugation, for $X > 0$, let

$$\pi_C(X) = \{\mathfrak{p} \in \Sigma_F | e_{\mathfrak{p}} = 1, (\mathfrak{p}, L/F) \in C, ||\mathfrak{p}|| \leq X\},$$

then

$$\#\pi_C(X) = \frac{\#C}{\#\,\mathrm{Gal}(L/F)} \frac{X}{\log X} + O(\frac{X}{\log X}).$$

⌟

Proof: Cf.[Lagarias and Odlysko, Effective Chebotarev]. □

Cor. (14.6.5.5) [Chebotarev]. Let L/F be a Galois extension of number fields, then for any subset $C \subset \mathrm{Gal}(L/F)$ that is stable under conjugation, let

$$T = \{\mathfrak{p} \in \mathrm{Unr}(F)|, (\mathfrak{p}, L/F) \subset C\},$$

then T has Dirichlet density $\delta(T) = \#C/\#\,\mathrm{Gal}(L/F)$. ⌟

Proof: This follows from(14.6.5.4) and the prime ideal theorem(21.4.10.2). □

Prop. (14.6.5.6) [Chebotarev for Function Fields]. Cf.[Sta]. ⌟

Proof: □

Prop. (14.6.5.7) [Every Ideal Class Contains a Prime]. For $F \in$ `NField`, each ideal class of F contains a prime ideal. In fact, the primes contained in any fixed ideal class has natural density $1/\operatorname{cl}(F)$. ⌟

Proof: Consider the Hilbert class field $\mathrm{H}(F)$ of F, then $\mathrm{Cl}(F) \cong \mathrm{Gal}(\mathrm{H}(F)/F)$ via the norm residue map. Then the assertion follows from(14.6.5.4). □

Splitting of Primes

Def. (14.6.5.8) [Splitting Sets]. Let L/F be a finite separable extension of global fields, let $\mathrm{Spl}(L/F) \subset \Sigma_F^{\mathrm{fin}}$ be the set of finite places of F that splits completely in L. By(5.2.7.28), If N/F is the Galois closure of L/F, then $\mathrm{Spl}(N/F) = \mathrm{Spl}(L/F)$. ⌟

Prop. (14.6.5.9) [Splitting in Cyclotomic Fields]. Let $L/\mathbb{Q}$ be Galois, then $L \in \mathbb{Q}(\zeta_m)$ for some $m \in \mathbb{Z}_+$ by(14.6.4.10), and let $\Lambda = \mathcal{N}_{L/\mathbb{Q}}/C^{\mathfrak{m}} \subset (\mathbb{Z}/(m))^*$ corresponds to L, then $p \in \mathbf{P}$ splits in L iff $p(\mathrm{mod}\ m) \in \Lambda$. ⌟

Cor. (14.6.5.10) [Dirichlet's Problem]. By(14.6.5.4) and(14.6.5.9), for any $m \in \mathbb{Z}_+$ and $[a] \in (\mathbb{Z}/(m))^\times$, there exists i.m. $p \in \mathbf{P}$ s.t. $p \equiv a(\mathrm{mod}\ m)$. ⌟

Prop. (14.6.5.11) [Frobenius]. If L/K is a finite Galois extension of global fields, then $\mathrm{Spl}(L/K)$ has Dirichlet density $1/[L:K]$. ⌟

Proof: For $v \in \Sigma_F^{\mathrm{fin}}$ unramified, it splits in L iff $(\mathfrak{p}_v, L/F) = \mathrm{id}$, by(14.6.3.23). So we can use Chebotarev theorem(14.6.5.5) for $C = \{\mathrm{id}\}$. □

Cor. (14.6.5.12). If $L/F, L/F'$ satisfies $\mathrm{Spl}(L/F) = \mathrm{Spl}(L'/F)$, then $L = L'$. ⌟

Proof: The hypothesis implies that $\mathrm{Spl}(L/F) = \mathrm{Spl}(LL'/F) = \mathrm{Spl}(L'/F)$, which then implies $L = LL' = L'$, by(14.6.5.11). □

Cor. (14.6.5.13). If L/K is a finite separable extension of global fields s.t. $\mathrm{Spl}(L/K)$ has Dirichlet density $[L:K]$, then L/K is Galois, by(14.6.5.8). ⌟

Cor. (14.6.5.14). If L/K is a finite separable extension of global fields s.t. $\mathrm{Spl}(L/K)$ has Dirichlet density 1, then $L = K$, by(14.6.5.8). ⌟

6 Explicit Construction of Class Fields

The explicit class field theory is the subject that tries to write the maximal Abelian extension of a field K as splitting field of polynomials.

Prop. (14.6.6.1) [Known Cases].

- $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\zeta_\infty)$(14.6.4.10).
- If $F \in$ `FField`, the theory of Drinfeld modules gives most Abelian extensions of F**?**.

- If $K \in p$-NField, K^{ab} is given by adjoining all torsion points of Lubin-Tate formal groups over K(14.6.2.29).
- If $F \in$ NField is a CM field, then by Kronecker's Jugendtraum(15.8.6.9), the Abelian extensions of F are given by j-invariants and torsion points of elliptic curves over F with CM.
- If $F \in$ NField is totally real, the conjecture of Stark gives all the Abelian extensions.?

⌟

7 Explicit Reciprocity Law

Cf.[Iwasawa] [Kummer], [Chao Li] and [Kato].

8 Local Field cases

Poitou-Tate Duality

Artin-Verdier Duality

9 Global Field cases

Poitou-Tate Duality

Artin-Verdier Duality

10 Inverse Galois Problem

p-adic Case

Prop. (14.6.10.1) [Abhyankar's conjecture, Raynaud]. A finite group Γ is the Galois group of an unramified Galois covering of $\mathbb{A}^1_{\overline{\mathbb{F}_p}}$ iff it is generated by its p-Sylow subgroups. ⌟

Proof: □

Solvable Groups

Thm. (14.6.10.2) [Šafarevič]. For $F \in$ GField and $G \in \mathcal{A}\mathrm{b}^{\mathrm{fin}}$ is solvable, then there exists a Galois extension L/F s.t. $\mathrm{Gal}(L/F) \cong G$. ⌟

Proof: Cf.[Cohomology of Number Fields, Neukirch]. □

11 Arithmetic Statistics

Thm. (14.6.11.1) [Davenport-Heilbronn]. For $\xi, \eta \in \mathbb{R}$, let $N_3(\xi, \eta)$ be the isomorphism classes of cubic number fields $\mathcal{K}$ s.t. $d_{\mathcal{K}} \in (\xi, \eta)$. Then

$$\lim_{X\to\infty} \frac{N_3(0, X)}{X} = \frac{1}{12\zeta(3)}, \quad \lim_{X\to\infty} \frac{N_3(-X, 0)}{X} = \frac{1}{4\zeta(3)}.$$

⌟

Proof: Cf.[On the density of discriminants of cubic fields, Davenport-Heilbronn]. □

Thm. (14.6.11.2) [Bhargava]. For $\xi, \eta \in \mathbb{R}$, let $N_n(\xi, \eta)$ be the isomorphism classes of cubic fields $\mathcal{K}$ s.t. $d_{\mathcal{K}} \in (\xi, \eta)$. Then for $n = 4$ or 5,

$$\lim_{X \to \infty} \frac{N_n(-X, X)}{X}$$

exists. ⌟

Proof: Cf.[The density of discriminants of quartic rings and fields], [The density of discriminants of quintic rings and fields]. □

14.7 Transcendental Number Theory

References are [Baker, Transcendental Number Theory].

1 Transcendental Numbers

Def. (14.7.1.1) [Logarithm of Algebraic Numbers]. Define the set of **Logarithms of Algebraic numbers**

$$\mathbb{L} = \{\lambda \in \mathbb{C} | e^\lambda \in \overline{\mathbb{Q}}\}.$$

⌟

Conj. (14.7.1.2) [Schanuel]. Suppose $z_1, \ldots, z_n \in \mathbb{C}$ are linearly independent over $\mathbb{Q}$, then

$$\text{tr.deg}(\mathbb{Q}(z_1, \ldots, z_n, e^{z_1}, \ldots, e^{z_n})/\mathbb{Q}) \geq n.$$

⌟

Conj.Cor. (14.7.1.3). If $\lambda_1, \ldots, \lambda_n \in \mathbb{L}$ are linearly independent over $\mathbb{Q}$, then they are alg.independent over $\mathbb{Q}$. ⌟

Thm. (14.7.1.4) [Hermite-Lindemann-Weierstrass].

- If $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ are pairwise distinct, then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are linearly independent over $\overline{\mathbb{Q}}$.
- If $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ are linearly independent over $\mathbb{Q}$, then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are alg.independent over $\mathbb{Q}$. In particular, if $\alpha \in \overline{\mathbb{Q}}$, then $e^\alpha \notin \overline{\mathbb{Q}}$.

⌟

Proof: Cf.[Baker, Thm1.4]. □

Cor. (14.7.1.5). π and e are not in $\overline{\mathbb{Q}}$. ⌟

Proof: $e^{2\pi\,\mathrm{i}} = 1$, and $e^1 = e$. □

Conj. (14.7.1.6) [p-adic Lindemann-Weierstrass Conjecture]. Suppose $p \in \mathbf{P}$ and $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}} \cap \mathbb{Q}_p$ s.t. $|\alpha_i|_p < 1/p$ for any i. Then $\exp_p(\alpha_1), \ldots, \exp_p(\alpha_n) \in \mathbb{C}_p$ are alg.independent over $\mathbb{Q}$. ⌟

Proof: □

Conj. (14.7.1.7) [Modular Conjecture, Bertrand]. Denote $j(\tau) = J(e^{2\pi\,\mathrm{i}\,\tau})$. Suppose $\tau_1, \ldots, \tau_n \in \mathscr{H}$ s.t.

$$\{J(e^{2\pi\,\mathrm{i}\,\tau_1}), J'(e^{2\pi\,\mathrm{i}\,\tau_1}), J''(e^{2\pi\,\mathrm{i}\,\tau_1}), \ldots, J(e^{2\pi\,\mathrm{i}\,\tau_n}), J'(e^{2\pi\,\mathrm{i}\,\tau_n}), J''(e^{2\pi\,\mathrm{i}\,\tau_n})\}$$

are alg.independent over $\mathbb{Q}$, then there exists two τ_i, τ_j that are linearly independent. ⌟

Proof: □

Thm. (14.7.1.8) [Gelfond-Schneider]. If $\alpha, \beta \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$ with $\alpha \neq 0, 1$, then $\alpha^\beta \notin \overline{\mathbb{Q}}$. ⌟

Proof: Cf.[Sil16]P286. □

Cor. (14.7.1.9). $(\sqrt{2})^{\sqrt{2}} \notin \overline{\mathbb{Q}}$. ⌟

Logarithmic Forms

Thm. (14.7.1.10) [Baker-Wüstholz]. Suppose $n \in \mathbb{Z}_+, \alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}} \setminus \{0,1\}, K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, and $d = [K : \mathbb{Q}]$. Let $b_1, \ldots, b_n \in \mathbb{Z}$, and $L(z_1, \ldots, z_n) = \sum b_i z_i$ be the linear form. If $\log(\alpha_i)$ is any logarithmic root of α_i for any i, and we define the modified heights

$$h'(\alpha_i) = \max(h^+(\alpha), \frac{1}{d}|\log \alpha|, \frac{1}{d}), \quad h'(L) = \max(h(L), \frac{1}{d}),$$

then if $L(\log(\alpha_1), \ldots, \log(\alpha_n)) \neq 0$, then

$$\log |L(\log(\alpha_1), \ldots, \log(\alpha_n))| > -18(n+1)! n^{n+1} (32d)^{n+2} \log(2nd) h'(\alpha_1) \ldots h'(\alpha_n) h'(L).$$

⌟

Proof: Cf.[Logarithmic Forms and Group Varieties]. □

Cor. (14.7.1.11). Situation as above, if each $\log(\alpha_i)$ is a principle value, and $B = \max(|b_i|, e), A = \max(H(\alpha_i), e)$, then

$$\log |L(\log(\alpha_1), \ldots, \log(\alpha_n))| > -(16nd)^{2(n+2)} (\log A)^n \log B.$$

⌟

Proof: □

2 Periods

Main references are [Periods, Zagier].

Def. (14.7.2.1) [Algebraic Functions]. Let F be a field contained in $\mathbb{C}$, then an **algebraic function** of degree $d \in \mathbb{Z}_+$ in n variable over F is a function $f(\underline{X}) \in C(\mathbb{R}^n)$ that is continuous in its domain and satisfies an equation $P(\underline{X}, f(\underline{X})) = 0$ where $P \in F[\underline{X}, T]$ that is of degree d in T. ⌟

Def. (14.7.2.2) [Periods]. A **period number** is a complex number that is an integral combinations of real numbers of the form $\int_U f(x)dx$ where f is an algebraic function over $\mathbb{Q}$(14.7.2.1) and U is a precompact connected open domain of $\mathbb{R}^n$ defined by polynomial inequalities with rational coefficients, for some $n \in N$. The set of periods is denoted by $\mathbb{P}$. The **extended Period ring** is defined to be $\widehat{\mathbb{P}} = \mathbb{P}[\frac{1}{2\pi i}]$.

Clearly $\overline{\mathbb{Q}} \subset \mathbb{P} \subset \mathbb{C}$, and they form an algebra. Also, $\#\mathbb{P} = \aleph_1$. ⌟

Prop. (14.7.2.3). In defining periods, we can even consider domains defined by inequalities by algebraic functions over $\mathbb{Q}$(14.7.2.1) defined on a larger open subset. ⌟

Proof: If U satisfies $f < a$ and f satisfies a polynomial function $P(\underline{X}, f(\underline{X})) = 0$, then U satisfies $P(\underline{X}, a) > 0$ or $P(\underline{X}, a) < 0$. We can assume the first one holds, and we can isolate the part $P(\underline{X}, a) > 0, f(\underline{X}) < a$ and the part $P(\underline{X}, a) > 0, f(\underline{X}) > a$ by segments, so we are reduced to the polynomial case. □

Prop. (14.7.2.4) [Algebraic Varieties]. If X is a smooth variety of dimension d over $\mathbb{Q}$ and $D \subset X$ a divisor with normal crossing, $\omega \in \Omega^d(X)$ vanishing on D, and $\gamma \in H_d(X(\mathbb{C}), D(\mathbb{C}), \mathbb{Q})$ is a singular n-chain with boundary in $Y(\mathbb{C})$, then the integral $\int_C \omega \in \mathbb{P}$.

In fact, any integration on a variety over $\mathbb{Q}$ can be reduced to this case, by resolution of singularity and restriction of divisors, and any period number comes from these.**?** ⌟

Proof: Roughly because we can represent γ by a semi-algebraic chain.**?** □

Example (14.7.2.5).
- $\sqrt{2}=\int_{2x^2<1}dx\in\mathbb{P}$.
- $\pi=\int_{x^2+y^2<1}dxdy\in\mathbb{P}$.
- $\log 2=\int_1^2\frac{dx}{x}\in\mathbb{P}$.

⌟

Prop. (14.7.2.6). For $n\in\mathbb{Z}_+,n\geq 2$, $\zeta(n)\in\mathbb{P}$. ⌟

Conj. (14.7.2.7) [Non-Examples]. There are no natural examples of numbers proven to be non-period. e, $1/\pi$ and Euler-Mascheroni constant γ are conjectured to be non-periods. Notice e is known to be transcendental but γ is not known to be rational or not yet! ⌟

Remark (14.7.2.8) [How to Distinguish Different Periods]. There may be numbers that can be written in different ways, such as

$$\sqrt{11+2\sqrt{29}}+\sqrt{16-2\sqrt{29}+2\sqrt{55-10\sqrt{29}}}=\sqrt{5}+\sqrt{22+2\sqrt{5}}.$$

But as they are both algebraic numbers we can check this by brutal force:
1. Find polynomials satisfied by them and use Euclidean division to find their common divisor, and use inequalities to bound its roots.
2. Calculate these two numbers to sufficiently high precision and use the fact two algebraic numbers of bounded degree cannot be too close to each other by Diophantine geometry.

But how to do this for periods? ⌟

Proof: They are both equal to the expression

$$\sqrt{11+2\sqrt{29}}+\sqrt{11-2\sqrt{29}}+\sqrt{5}$$

by using the equality $\sqrt{a}+\sqrt{b}=\sqrt{a+b+\sqrt{ab}}$. □

Conj. (14.7.2.9) [Periods Conjecture]. Any two integral representations of a period can be transformed to each other by means of , cut-and-paste, change of variables and Stoke's formula. ⌟

Prop. (14.7.2.10) [Calabi]. We give one indication of this conjecture by proving $\zeta(2)=\pi^2/6$:

$$(1-\frac{1}{4})\zeta(2)=1^{-2}+3^{-2}+5^{-2}+\cdots=\int_{(0,1)^2}\frac{1}{(1-x^2y^2)}dxdy.$$

But the change of variables

$$(x,y)=(\frac{\sin u}{\cos v},\frac{\sin v}{\cos u})$$

has Jacobian $(1-x^2y^2)$ and maps the triangle $T=\{u,v>0,u+v<\pi/2\}$ bijectively to $(0,1)^2$, so

$$\int_{(0,1)^2}\frac{1}{(1-x^2y^2)}dxdy=\int_T dudv=\mathrm{Vol}(T)=\pi^2/8$$

⌟

Def. (14.7.2.11) [Exponential Periods]. An **exponential period number** is a complex number that is an integral combinations of real numbers of the form $\int_U f(x)\exp(g(x))dx$ where f,g are algebraic functions over $\mathbb{Q}$(14.7.2.1) and U is a precompact connected open domain of $\mathbb{R}^n$ defined by polynomial inequalities with rational coefficients, for some $n\in N$. The set of periods is denoted by $\mathbb{P}_{\exp}$. ⌟

3 Periods and Differential Equations

4 Periods and L-Functions

5 Periods and Motives

15 Arithmetic Geometry

15.1 Pseudo-Algebraically Closed Fields

References are [Field Arithmetic].

1 Pseudo-Algebraically Closed Fields

Def. (15.1.1.1). $k \in$ `Field` is called a **pseudo-algebraically closed field** or **PAC field** if every variety over k has a k-point. ⌟

Example (15.1.1.2) [PAC Fields].
- Separably closed fields are PAC.
- Infinite algebraic extensions of finite fields are PAC.
- Ultraproducts of distinct finite fields are PAC.

⌟

Proof: □

2 Hilbertian Fields

Cf.[Field Arithmetics] or [Mordell-Weil Theorem notes, Serre, 1997].

Hilbert Subsets

Def. (15.1.2.1) [Hilbert Subsets]. For $k \in$ `Field` and two set of variables $T_1, \ldots, T_r$ an $X_1, \ldots, X_n$, let $f_1(\underline{T}, \underline{X}), \ldots f_m(\underline{T}, \underline{X}) \in k[\underline{X}, \underline{X}]$ that is irreducible in $k(\underline{T})[\underline{X}]$, and let $g \in j[\underline{T}]$. Then a **Hilbert subset** of k^r is a subset of the form

$$\{(a_1, \ldots, a_r) \in k^r | g(\underline{a}) \neq 0, f(\underline{a}, \underline{X}) \text{ are irreducible in } k[\underline{X}]\}.$$

A **separable Hilbert subset** is a Hilbert set of this form s.t. $n = 1$ and each f_i is separable in X. ⌟

Def. (15.1.2.2) [Hilbertian Fields]. $k \in$ `Field` is called a **Hilbertian field** if each separable Hilbert subset of k is non-empty. Thus a Hilbert field must be infinite. ⌟

Prop. (15.1.2.3) [Separable Extensions]. If L/K is a finite separable extension, then any Hilbert subset of L^r contains a Hilbert subset of K^r. In particular, if K is Hilbertian, then so is L. ⌟

Proof: Cf.[Field Arithmetic, P223]. □

Remark (15.1.2.4). The converse is false, Cf.[Field Arithmetic, 13.9.5]. ⌟

Examples of Hilbertian Fields

Example (15.1.2.5) [Hilbertian Fields].

- Global fields are Hilbertian.
- If $k \in$ `Field` and K is a f.g. transcendental extension of k, then K is Hilbertian.

⌟

Proof: Cf.[Field Arithmetic, Chap13]. □

3 Haar Measures

4 Problems

5 Frobenius Fields

6 Undecidability

15.2 Heights and Diophantine Approximations

References are [Galois Cohomology, Serre]Chap2.4.5, [B-G06], [Fundamentals of Diophantine Geometry, Lang], [Weil50].

1 Heights

Def. (15.2.1.1) [Equivalent Height function]. Let X be a projective scheme, two height functions $X(\overline{K}) \to \mathbb{R}$ are called equivalent iff they differ by a bounded function. ⌟

Prop. (15.2.1.2). There is a way of constructing the Weil heights as a special case of the global heights, which are sum of local heights, Cf.[Diophantine Geometry, Chap2]. ⌟

Heights on Projective Spaces

Def. (15.2.1.3) [Canonical Heights on Projective Spaces]. For $K \in$ `LField` with base field K_0, let $x = (x_0, \ldots, x_n) \in K^{n+1} \setminus \{0\}$, then for a normalized place u on $\overline{K}$ and a normalized place v of K that $u|v$, suppose $\log(0) = -\infty$ and define

$$h_u((x_0, \ldots, x_n)) = \max_i(\log|x_i|_u), \quad H_u((x_0, \ldots, x_n)) = \exp(h_u((x_0, \ldots, x_n)))$$

$$h_v((x_0, \ldots, x_n)) = [K_v : (K_0)_{v_0}]h_u((x_0, \ldots, x_n)), \quad H_v((x_0, \ldots, x_n)) = \exp(h_v((x_0, \ldots, x_n))).$$

And if $F \in$ `GField` over base field F_0, for $x \in \mathbb{P}^n(F)$, define

$$h(x) = \frac{1}{[F : F_0]} \sum_{v \in \Sigma_F} h_v((x_0, \ldots, x_n)), \quad H(x) = \exp(h(x))$$

- $h_u((x_0, \ldots, x_n))$ is invariant under finite extensions of fields K'/K, thus this local height is defined on all $\overline{K}^{n+1}$.
- $h(x)$ is well-defined.
- $h(x) \geq 0$.
- $h(x)$ is invariant under finite extensions of fields F'/F, thus the height is defined on all $\mathbb{P}^n(\overline{F})$.
- For $\sigma \in \mathrm{Gal}(\overline{F}/F)$, $h(\sigma(x)) = h(x)$.

These are called **canonical heights** and **multiplicative canonical heights** on $\mathbb{P}^n$. ⌟

Proof: 1 is a consequence of the product formula(14.4.4.16). 2 follows from 1 because we can divide a constant to make a coordinate unit in K^*, thus clearly $h(x) \geq 0$. 3 follows from the fundamental identity. □

Prop. (15.2.1.4). If $P_1, \ldots, P_r \in \overline{K}^n$, then

$$h_u(P_1 + \ldots + P_r) \leq h_u(P_1) + \ldots + h_u(P_r) + \varepsilon_u \log|r|_u,$$

where $\varepsilon_u = 0$ if u is non-Archimedean and 1 otherwise. ⌟

Def. (15.2.1.5) [Height on Affine Spaces]. For $F \in \texttt{NField}$ and $\underline{x} = (x_1, \ldots, x_n) \in F^n$, the **affine height** is defined to be:

$$h^+(\underline{x}) = h([1, \underline{x}] \in \mathbb{P}^n(F)).$$

and similarly we define $H^+(\underline{x})$.

In particular, if $\alpha \in F$, then the height of α is

$$h^+(\alpha) = \frac{1}{[F:\mathbb{Q}]} \sum_{v \in \Sigma_F} \max(0, \log |\alpha|_v).$$

⌟

Lemma (15.2.1.6). For $\alpha \in \overline{\mathbb{Q}}$ and $\lambda \in \mathbb{Q}$, we have $h(\alpha^\lambda) = |\lambda| h(\alpha)$. ⌟

Proof: For $\lambda > 0$, this is easy. So it suffices to consider $\lambda = -1$. Notice

$$\log |\alpha|_v = \max\{0, \log |\alpha|_v\} - \max\{0, \log |1/\alpha|_v\},$$

summing over all places v and use the product formula, we get the desired results. □

Lemma (15.2.1.7) [Northcott]. Let $F \in \texttt{GField}$ and $C > 0, d > 0$, then $\#\{x \in \mathbb{P}^n(\overline{F}) | h(x) \leq C, \deg(x) \leq d\} < \infty$. ⌟

Proof: We first reduce to the case $k(x) = \mathbb{Q}$ or $\mathbb{F}_p(t)$: for a point x with $[k(x) : \mathbb{Q}] \leq d$, consider the point $(X_0, \ldots, X_m)$ in the projective space $\mathbb{P}^m$ of forms of degree $\deg(x)$ in $n+1$ variables corresponding to $\mathrm{Nm}(\sum x_i T_i)$. Notice the inverse image of any closed point in $\mathbb{P}^m$ is a finite set in $\mathbb{P}^n(\overline{K})$, and the height of $h((X_0, \ldots, X_m)) \leq d!(n+1)h(x)$, so it suffices to prove for $\mathbb{P}^m(\mathbb{Q})$. In this case, we normalize a point to a unique point with integral coordinates with no common divisors, then $\max_i \log |x_i|_p = 0$ for any p, thus $h(x) = h_\infty(x)$, and clearly only f.m. points has bounded heights. □

Prop. (15.2.1.8) [Change of Coordinates]. Let h_1, h_2 be heights of $\mathbb{P}(\overline{K})$ defined w.r.t. two coordinates systems, then $h_1 \sim h_2$. Thus we can consider heights in any particular coordinates that is convenient. ⌟

Proof: The proof is straightforward. □

Heights of Polynomials

Def. (15.2.1.9) [Heights and Mahler Heights]. The height of a polynomial $f(T) = x_0 + x_1 T + \ldots + x_d T^d$ is defined to be $h^+(f) = h^+((x_0, \ldots, x_d))$, and similarly for $H^+(f)$.

The **Mahler height** of f is defined to be? ⌟

Lemma (15.2.1.10) [Gelfond]. ⌟

Prop. (15.2.1.11). Let $f_1, \ldots, f_m \in \overline{\mathbb{Q}}[X_1, \ldots, X_n]$ of degree d, then

$$-d \log 2 + \sum_{j=1}^m h(f_j) \leq h(f) \leq d \log 2 + \sum_{j=1}^m h(f_j).$$

⌟

Proof: Cf.[Bombieri, P28].? □

Cor. (15.2.1.12). Let $d \in \mathbb{Z}_+$, then there exists constants $C_1, C_2 \in \mathbb{R}_+$ depending on d s.t. for any $\alpha \in \overline{\mathbb{Q}}$ with $\deg(\alpha) = d$, if $f_\alpha \in \mathbb{Z}[T]$ be a minimal polynomial of α with coprime coefficients, then

$$dh^+(\alpha) - C_1 \leq h(f_\alpha) \leq dh^+(\alpha) + C_2.$$

⌟

Arakelov Heights

Def. (15.2.1.13)[Arakelov Heights]. For a local field K with base field K_0, let $x=(x_0,\ldots,x_n)\in K^n$, then for a normalized place u on $\overline{K}$ and a normalized place v of K that $u|v$, define

$$h_u^{Ar}((x_0,\ldots,x_n))=\begin{cases}\log\max_i(|x_i|_u) & ,K\in\texttt{p-Field}\\ \log\sqrt{\sum_{j=0}^n|x_j|_u^2} & ,K=\mathbb{R}\text{ or }\mathbb{C}\end{cases},\quad H_u^{Ar}((x_0,\ldots,x_n))=\exp(h_u^{Ar}((x_0,\ldots,x_n)))$$

$$h_v^{Ar}((x_0,\ldots,x_n))=[K_v:(K_0)_{v_0}]h_u((x_0,\ldots,x_n)),\quad H_v^{Ar}((x_0,\ldots,x_n))=\exp(h_v^{Ar}((x_0,\ldots,x_n))).$$

And if F is a global field over base field F_0, for $x\in\mathbb{P}^n(F)$, define

$$h^{Ar}(x)=\frac{1}{[F:F_0]}\sum_{v\in\Sigma_F}h_v(x),\quad H^{Ar}(x)=\exp(h^{Ar}(x)).$$

Then $h^{Ar}(x),H^{Ar}(x)$ are well-defined, positive, and invariant under finite extensions of fields for the same reason as(15.2.1.3). Then they extends to the algebraic closure, called the **Arakelov heights** and **multiplicative Arakelov heights** on $\mathbb{P}^n$. ⌟

Cor. (15.2.1.14). The Arakelov height is the height associated to the locally bounded metrized line bundle on $\mathcal{O}_{\mathbb{P}^n}(1)$ with Fubini-Study metrics in the Archimedean places and standard metric in the non-Archimedean places, so it is equivalent to the canonical height. ⌟

Def. (15.2.1.15) [Arakelov Heights on Matrices]. The Arakelov heights induces a height function on the Grassmannians by the canonical embedding, and for any matrix $A\in M_{n\times m}(\overline{F})$ of rank m, let the Arakelov heights of A be defined as the height of the point in the Grassmannian $\mathrm{Gr}_m(\overline{F})$ associated to the space spanned by the columns of A. And if $A\in M_{m\times n}(F)$ of rank m, then its Arakelov height is defined to be $H^{Ar}(A)=H^{Ar}(A^t)$.

Equivalently, it is the height of the point in $\mathbb{P}^{\binom{n}{m}-1}(F)$ represented by the $m\times m$-minors of A. And we can also define the local heights of A in this form. ⌟

Prop. (15.2.1.16). Let $K=\mathbb{R}$ or $\mathbb{C}$ and $A\in M_{n\times m}(\overline{K})$ has rank m, then $H_u(A)=\det(A^*A)^{1/2}$, by Binet's formula(3.5.7.11). ⌟

Prop. (15.2.1.17). Let K be a local field and $A=[B,C]\in M_{n\times m}(\overline{K})$ has rank m, then

$$H_u^{Ar}(A)\leq H_u^{Ar}(B)H_u^{Ar}(C).$$

⌟

Prop. (15.2.1.18). Let $F\in\texttt{GField}$ and W be a subspace of F^n and $W^\perp\in(F^n)^*\cong F^n$ be the annihilator of W, then $h^{Ar}([W])=h^{Ar}([W^\perp])$. ⌟

Proof: Cf.[B-G06]P68. □

Prop. (15.2.1.19). Let K be a local field and V,W be subspaces of $\overline{K}^n$, then

$$h_u^{Ar}([V+W])+h_u^{Ar}([V\cap W])\leq h_u^{Ar}([V])+h_u^{Ar}([W]).$$

⌟

Proof: Cf.[B-G06]P69. □

Prop. (15.2.1.20) [Metric on Projective Space]. Let K be a local field, for a normalized place u on $\overline{K}$ and a normalized place v of K that $u|v$, for $x, y \in (\overline{K})^n \backslash \{0\}$, define

$$\delta_u(x,y) = \frac{H_u^{Ar}(x \wedge y)}{H_u^{Ar}(x) H_u^{Ar}(y)}, \quad \delta_v(x,y) = \delta_u(x,y)^{[K_v:(K_0)_{v_0}]},$$

then $\delta(x,y) \in [0,1]$ by(15.2.1.19), and defines a metric on $\mathbb{P}^n(\overline{K})$, called the **projective metric on** $\mathbb{P}^n$. In the complex case, it is just the Fubini-Study metric.

And if F is a global field over base field F_0, for $x, y \in \mathbb{P}^n(\overline{F})$, define

$$\delta(x) = \prod_v \delta_v(x,y)^{\frac{1}{[F:F_0]}}.$$

⌟

Proof: Cf.[B-G06]P70. □

Prop. (15.2.1.21). Let F be a global field and $x, y \in \mathbb{P}^1(\overline{F})$, then

- If $O = [0,1]$, then $H^{Ar}(x) = \frac{1}{\delta(x,O)}$.
- If $x = [1, \alpha], y = [1, \beta]$, then $\delta(x,y) = \frac{1}{H^{Ar}(\alpha) H^{Ar}(\beta)}$.

⌟

Weil Heights

Prop. (15.2.1.22). Let X be a complete variety over K and $\varphi : X \to \mathbb{P}^k, \psi : X \to \mathbb{P}^l$ are two K-morphisms. If $\varphi^*(\mathcal{O}_{\mathbb{P}^k}(1)) \cong \psi^*(\mathcal{O}_{\mathbb{P}^l}(1))$, then the induced height function $h_\varphi - h_\psi$ is bounded on $X(\overline{K})$. ⌟

Proof: Let $\varphi^*(\mathcal{O}_{\mathbb{P}^k}(1)) \cong \psi^*(\mathcal{O}_{\mathbb{P}^l}(1)) \cong L$, then L is very ample. Consider a basis $\{s_0, \ldots, s_n\}$ of $\Gamma(X, L)$, then it induces a closed embedding $\chi : X \to \mathbb{P}^n : x \mapsto [s_0(x), \ldots, s_n(x)]$ and $\chi^*(\mathcal{O}_{\mathbb{P}^n}(1)) \cong L$. Then it suffices by symmetry to prove $h_\varphi \sim h_\chi$.

We may assume $\varphi(X)$ is not contained in any proper linear subspace of X, so we can choose a basis $T_0, \ldots, T_k$ of $\varphi^*(\Gamma(\mathbb{P}^k, \mathcal{O}_{\mathbb{P}^k}(1)))$, and let $s_0, \ldots, s_k = T_0, \ldots, T_k$. Let $x \in X(\overline{K})$, let $(x_0, \ldots, x_n)$ be the coordinate of $\chi(x)$ and $(x_0, \ldots, x_k)$ the coordinates of $\varphi(x)$. Then by the formula(15.2.1.3) clearly $h_\varphi \leq h_\chi$.

For the converse, let I be the homogenous ideal corresponding to $X \subset \mathbb{P}^n$, then X has coordinate ring $R = K[T_0, \ldots, T_n]/I$. The $T_0, \ldots, T_k$ generates a radical ideal equal to $(T_0, \ldots, T_n)$, because they have no common zero on X. Now there is an integer q and homogenous ideals F_{ij} that

$$T_{k+i}^q - \sum_{j=0}^k F_{ij}(T_0, \ldots, T_n) T_j \in I$$

so

$$q \log |x_{k+i}|_v \leq (q-1) \max_{j \leq n} \log |x_j|_v + \max_{j \leq k} \log |x_j|_v + C_v$$

where $C_v = 0$ unless v is Archimedean. Hence

$$\max_{j \leq n} \log |x_j|_v \leq \max_{j \leq k} \log |x_j|_v + C_v \Rightarrow \quad h_\chi \leq h_\varphi + C.$$

□

Prop. (15.2.1.23) [Weil Heights]. Let X be a projective variety over $F \in \texttt{NField}$, then for each element $\mathcal{L} \in \mathrm{Pic}(X)$, we can assign a unique **Weil height** $h_{\mathcal{L}}$, determined up to equivalence, that

- $h_{L_1 \otimes L_2} \sim h_{L_1} + h_{L_2}$.
- If $X = \mathbb{P}^n$, then $h_{\mathcal{O}(1)}$ is the height defined in(15.2.1.3).
- For any K-morphism $\varphi : X \to Y$ and $L \in \mathrm{Pic}(Y)$, $h_{\varphi^*(L)} \sim h_L \circ \varphi$.

⌟

Proof: The uniqueness follows from the fact that $\mathrm{Pic}(X)$ is generated by very ample line bundles because X is projective. For the existence, we may take item3 as definition, extend it to all $\mathrm{Pic}(X)$, and it is essential to verify item1.

Let $L_1 = \varphi^*(\mathcal{O}(1)), L_2 = \psi^*(\mathcal{O}(1))$, where $\varphi : X \to \mathbb{P}^k, \psi : X \to \mathbb{P}^l$. Denote $\sigma : \mathbb{P}^k \times \mathbb{P}^l \to \mathbb{P}^{kl+k+l}$ the Segre embedding, then $L_1 \otimes L_2 \cong \chi^*(\mathcal{O}_{\mathbb{P}^{kl+k+l}}(1))$ where $\chi : X \xrightarrow{(\varphi,\psi)} \mathbb{P}^k \times \mathbb{P}^l \xrightarrow{\sigma} \mathbb{P}^{kl+k+l}$. And we check $h_\chi \sim h_\varphi + h_\psi$. □

Thm. (15.2.1.24) [Northcott]. Let X be a projective variety over a global field F and let h_c be a height function associated to an ample class $\mathcal{L} \in \mathrm{Pic}(X)$, then the set

$$\{P \in X(\overline{K}) | h_{\mathcal{L}}(P) \leq C, [K(P) : K] \leq d\}$$

is finite for any constant C, d. ⌟

Proof: There is a $m > 0$ that mc is very ample. Because $mh_{\mathcal{L}}$ is the height function associated to $m\mathcal{L}$, we can assume that $\mathcal{L}$ is very ample, thus reducing to $X = \mathbb{P}^n$ and $\mathcal{L} = \mathcal{O}(1)$ by(15.2.1.23). This follows from(15.2.1.7). □

Prop. (15.2.1.25). Let $F \in \texttt{Field}, X \in \mathcal{S}m\mathcal{P}roj\mathcal{V}ar/F$ and $c \in \mathrm{Pic}(X)$ an ample line bundle, $c' \in \mathrm{Pic}^0(X)$, then

$$h_{c'} = O(|h_c|^{1/2} + 1).$$

⌟

Proof: By base change of fields, we may assume X has a rational point P_0. Consider the double Picard map $\varphi : X \to \widehat{\underline{\mathrm{Pic}}^0(X)} = \widehat{A}$. Viewing c' as a rational point of A, consider $c'' = (p_A)_{c'} \in \mathrm{Pic}(\widehat{A})$, then $\varphi^*(c'') = (\mathrm{id} \times \varphi)^*(p_A)|_{c'} = (p_X)_{c'} = c'$. Thus $h_{c'} \sim h_{c''}$.

Let $\widehat{c}$ be an even ample line bundle on $\widehat{A}$(15.7.1.28), then for for some n large, $nc - \varphi^*(\widehat{c})$ is base-point-free, thus by(15.2.1.23), $h_{\widehat{c}} \circ \varphi = O(|h_c| + 1)$. Thus it suffices to prove for c', c changed to $c'', \widehat{c}$, which is true by(15.13.1.10). □

Prop. (15.2.1.26) [Weil Heights in Intersection Theory]. Cf.[B-G06]P44**?** ⌟

Bounded Sets

Def. (15.2.1.27) [Bounded Sets]. Let $k \in \texttt{Field}$ and $|\cdot|$ a valuation on its alg.closure $\overline{k}$, $X \in \mathcal{V}ar/k$. Then:

- If X is an affine variety, then a subset $E \subset X(\overline{K})$ is called **bounded** if for any $f \in K[X]$, $|f|$ is bounded on E.
- If X is arbitrary, then a subset $E \subset X(\overline{K})$ is called **bounded** if there is a finite open affine covering U_i of X and sets $E_i \subset U_i(\overline{K})$ that E_i is bounded in U_i and $E = \cup E_i$.

⌟

Prop. (15.2.1.28) [Properties of Bounded Sets].
- For a bounded set E in X and any finite open affine covering U_i of X, there is a division of E:
$$E = \cup E_i, \quad E_i \subset U_i(\overline{K})$$
and E_i being bounded in U_i.
- If E is bounded in X and Y is a closed subscheme of X, then $E \cap Y(\overline{K})$ is bounded in Y.
- The image of a bounded set under a morphism is also bounded.
- $\mathbb{P}^n(\overline{K})$ is bounded in $\mathbb{P}^n$.
- The inverse image of bounded set under a proper morphism is bounded. In particular, if X is a complete variety over a field K, then $X(\overline{K})$ is bounded in X.

⌟

Proof: 1: Because X is separated, it suffices to prove for X affine. And we can also take a refinement of the covering, thus assuming $U_i = X_{h_i}$. Suppose $\sum g_i h_i = 1$, and let $E_i = \{P \in E || h_i(P)| = \max_k |h_k(P)|\}$, then $E_i \subset U_i(\overline{K})$. To show E_i is bounded in U_i, it suffices to show $|1/h_i|$ is bounded in E_i. But this is clear, because $|g_i|$ is bounded on E.

2: Use local coordinates.

4: Use the affine open covering $X_i = \{x_i \neq 0\}$, and let $E_i = \{|x_i| = \max_{j=0,\ldots,n} |x_j|\}$, then clearly E_i is bounded in X_i.

5: Cf.[Diophantine Geometry, P55], may use Chow's lemma**?**. □

Prop. (15.2.1.29) [M-Bounded]. We can define the notion of M-boundedness similar to that of(15.2.1.27), where M is a set of places on K that for any $\alpha \neq 0 \in K$, only f.m. of M have nontrivial valuation. Then (E^u) is said to be **M-bounded** in an affine variety X if for any $f \in K[X]$,
$$C_v(f) = \sup_{u \in M, u|v} \sup_{P \in E^u} |f(P)|_u$$
is finite for any $v \in M_K$ and $C_v(f) > 1$ for only f.m. v.

Then similar properties as in(15.2.1.28) hold for M-bounded sets. ⌟

Def. (15.2.1.30). A real function f on $X(\overline{K})$ is called **locally bounded** if $f(E)$ is bounded for every bounded set E in X. ⌟

Distance Functions

Def. (15.2.1.31) [Distance Function on Curves]. Let C be a curve over a valued field K, let for $P, Q \in C(K)$, the **v-adic distance** function $d_v(P;Q)$ be defined to be $d_v(P;Q) = \min(|t_Q(P)|_v^{1/e}, 1)$, where t_Q is a function with only one zero of order e at Q.

To understand this definition, it is just same as the pullback of the local height via t_Q. It is a special case of local heights. ⌟

Prop. (15.2.1.32). Let C be a curve over a valued field K and $F \in K(C)$, then
$$\varinjlim_{P \in C(K), d_v(P,Q) \to 0} \frac{\log |F(P)|_v}{\log d_v(P,Q)} = \mathrm{ord}_Q(F).$$

⌟

Proof: In taking limit, scaling t_Q by a constant doesn't matter, so If we change $h_{\mathcal{O}(-Q)}$ to $h^{1/k}_{\mathcal{O}(-kQ)}$, the limit won't change, so we will do so and assume k is large enough s.t. there is a function that has only zeros at P of order k, so $f^*\mathcal{O}(1) = O(-kP)$, and thus we may change $O(kP)$ to $f^*\mathcal{O}(1)$ and then we see $f^{\mathrm{ord}_Q(F)}/F^k$ is regular and non-vanishing at Q, thus we can easily get the desired result. □

Prop. (15.2.1.33). If $\varphi : C_1 \to C_2$ is a non-constant map of curves over a valued field K, then for $Q \in C_1$,

$$\varinjlim_{P\in C(K), d_v(P,Q)\to 0} \frac{\log d_v(\varphi(P),\varphi(Q))}{\log d_v(P,Q)} = e_Q(\varphi).$$

⌟

Proof: Similar as that of(15.2.1.32). In fact(15.2.1.32) can be derived from this one. □

Metricized Line Bundles

Chevalley-Weil Theorem

Prop. (15.2.1.34)[Local Chevalley-Weil]. Let K be a non-Archimedean valued field. Let $\varphi : Y \to X$ be a finite unramified morphism of K-varieties and E a bounded set in $X(\overline{K})$. Then there is an $\alpha \neq 0 \in \mathcal{O}_K$ that $\alpha \in \widehat{\delta}_{P/Q}$ whenever $P \in Y(\overline{K})$ and $Q = \varphi(P) \in E$. ⌟

Proof: An unramified map is locally of the form a closed embedding of a standard étale morphism**?**, thus there are f.m. U_i, V_i covering X, Y respectively that $V_i \to U_i$ is closed embedding $V_i \to W_i$ of a standard étale morphism $W_i \to U_i$. Because φ is finite hence proper, $\varphi^{-1}(E)$ is bounded by(15.2.1.28), thus there is a decomposition of $\varphi^{-1}(E)$ into bounded sets $E'_i \subset V_i$. Then it suffices to prove for standard étale morphisms, because we can then multiply them.

The image of E_i in W_i is also bounded. Let $W_i \to U_i : \mathrm{Spec}(A[t]/f) \to \mathrm{Spec}\, A$, where

$$f = t^d + a_1 t^{d-1} + \ldots + a_d, \quad a_i \in A.$$

By boundedness, there is an $a \neq 0 \in R$ that

$$\max_{i=1,\ldots,d} \sup_{P\in E'} |a_i(\varphi(P))| \leq |a|^{-1}.$$

Then $\xi = at_P$ is a root of the polynomial

$$g_Q(t) = t^d + aa_1(Q)t^{d-1} + \ldots + a^d a_d(Q),$$

and it is easily verified that $|\xi| \leq 1$ thus $\xi \in R_P$. Now let g_ξ be the minimal polynomial of ξ over $\widehat{K(Q)}$, then $g_Q = g_\xi h$, $h \in \widehat{K(Q)}[t]$. By Gauss lemma in fact $g_\xi, h \in \widehat{R}_Q[t]$.

Now the elements $1, \xi, \ldots, \xi^{\widehat{d}-1}$ form a basis of $\widehat{K(P)}/\widehat{K(Q)}$, so the discriminant $D_{g_\xi} \in \delta_{\widehat{K(P)}/\widehat{K(Q)}}$. By**??** and(5.2.7.37), $|D_{g_\xi}| = |N_{\widehat{K(P)}/\widehat{K(Q)}}(g'_\xi(\xi))| = |g'_\xi(\xi)|^{\widehat{d}}$. But

$$g'_\xi(\xi)h(\xi) = g'_Q(\xi) = a^{d-1}f'_Q(\xi) = a^{d-1}f'_Q(t_P) = a^{d-1}f'(P).$$

Because f' is unit, we have $|D^{-1}_{g_\xi}|$ is bounded on E'. So there is an $\alpha \neq 0 \in R$ that $|D_{g_\xi}| \geq |\alpha|$, independent of P. Then we are done, as $D_{g_\xi} \in \delta_{\widehat{K_P}/\widehat{K_Q}}$. □

Lemma (15.2.1.35) [Global Chevalley-Weil]. Let Σ be a set of discrete valuations of a field F that any element α has only f.m. nonzero valuations, $\varphi : Y \to X$ be an unramified finite F-morphism of complete K-varieties, and $(E^u)_{u\in\Sigma}$ is an Σ-bounded family in X(15.2.1.29), then for every $v \in \Sigma$ there is a nonzero $\alpha_v \in \mathcal{O}_{F,v}$ that $\alpha_v \in \widehat{\delta}^u_{P/Q}$ whenever $u|v$ and $P \in Y(\overline{K})$ with $\varphi(P) = Q \in E^u$. Moreover, $\alpha_v = 1$ for a.e. $v \in \Sigma$. ⌟

Proof: The proof is exactly the same as that of(15.2.1.34), noticing that a, α depend only on v but not $u|v$, and also $a = \alpha = 1$ for a.e. v.(15.2.1.29). □

Lemma (15.2.1.36) [Global Chevalley-Weil Theorem for Discrete Valuations]. Let Σ_K be a set of discrete valuations of a field K that any element $\alpha \in K^*$ has only f.m. nonzero valuations, $\varphi : Y \to X$ be an unramified finite K-morphism of complete K-varieties, then there are a finite set $S \subset M_K$ and for any $v \in S$ a nonzero element $\alpha_v \in \mathfrak{m}_v$ s.t. for any $P \in Y(\overline{F}), Q = \varphi(P)$ and any place $w_0|v$ of $K(Q)$, $K(P)/K(Q)$ is unramified outside S and if $v \in S$, $\alpha_v \in \delta^{w_0}_{P/Q}$. ⌟

Proof: We may assume φ is surjective because it is closed(finite is proper). Notice $X(\overline{K})$ is M-bounded in X(15.2.1.28), where M is the set of valuations of $\overline{K}$ extending that of M_K. Then we can use global Chevalley-Weil theorem(15.2.1.35) to find elements α_v for $v \in M_K$. Now notice

$$\delta^{w_0}_{P/Q} = \prod_{w|w_0} (\widehat{\delta}^w_{P/Q} \cap \mathcal{O}_{Q,v})$$

by(5.2.7.40), and the number of $w \in M_{K(P)}, w|w_0$ is bounded by $[K(P) : K(Q)]$, which is further bounded by $\deg(f)$ as in(15.2.1.34). Hence we can take $\alpha_v = \alpha_v^{\deg(f)}$ to finish the proof. □

Prop. (15.2.1.37). Let F be a global field or the function field of a non-singular curve over a field k, and let $\varphi : Y \to X$ be a finite unramified morphism of F-varieties. If X is complete, then there is an $\alpha \neq 0 \in \mathcal{O}_F$ that for any $P \in X(\overline{F})$ that $Q = \varphi(P)$, the discriminant $\delta_{P/Q}$ contains α. ⌟

Proof: By(6.12.1.14), we can use the above lemma(15.2.1.36) to $\Sigma = \Sigma_F$. Notice because $\delta_{P/Q} = \prod_{w_0\in\Sigma^0_{k(Q)}} (\delta^{w_0}_{P/Q} \cap \mathcal{O}_{X,Q})$, we can assume $\alpha_v \in \mathcal{O}_{X,Q}$, then take $\alpha = \prod_{v\in S} \alpha_v$. □

Thm. (15.2.1.38) [Chevalley-Weil]. Let F be a global field or the function field of a non-singular curve over a field k, $\varphi : Y \to X$ be a finite unramified morphisms of F-varieties. If X is complete, then there is a finite extension L/K that $P \in Y(L)$ for any $P \in Y(\overline{K})$ that $\varphi(P) \in X(K)$. ⌟

Proof: By Chevalley-Weil theorem(15.2.1.37), there is an $\alpha \in \mathcal{O}_F$ that $\alpha \in \delta_{P/Q}$ for any $P \in Y(F^s)$ that $\varphi(P) \in X(K)$, thus $K(P)/K(Q)$ is unramified outside $S(\alpha)$. But then(14.4.1.28) shows there are only f.m. possibilities of $k(P)$. Thus we are done. □

2 Canonical Heights

References are [Call-Silverman. Canonical heights on varieties with morphisms].

Prop. (15.2.2.1) [Tate's Limiting argument]. ⌟

Proof: Cf.[B-G06]P285.? □

Cor. (15.2.2.2). Tate's limiting argument gives another way of constructing Néron-Tate heights. More generally, for any projective variety X over a global field K, if $\varphi : X \to X$ a morphism over K, $\mathcal{L}$ a line bundle on X and $k, l \in \mathbb{Z}, |k| > |l|$ that

$$l\varphi^*(\mathcal{L}) = k\mathcal{L},$$

then there is a unique function $\widehat{h}_{\varphi,\mathcal{L}}$ in the equivalent class of $h_{\mathcal{L}}$ that

$$l\widehat{h}_{\varphi,\mathcal{L}}(\varphi(x)) = k\widehat{h}_{\varphi,\mathcal{L}}(x).$$

In particular, the Néron-Tate heights on an Abelian variety for an even or odd line bundle is obtained by taking $\varphi = [m]$ for some $m \geq 2$. ⌟

Proof: Assume $l \neq 0$, consider the subgroup $\mathcal{N} = \{\lambda^r | r \in \mathbb{N}\}$, where $\lambda = k/l$, and $\mathcal{N}$ acts on $X(\overline{K})$ by $\lambda^r \cdot x = \varphi^r(x)$, then $h_{\mathcal{L}}$ is quasi-homogenous of degree 1, so Tate's limiting argument(15.2.2.1) shows

$$\widehat{h}_{\varphi,\mathcal{L}}(x) = \lim_{r\to\infty} \lambda^{-r} h_{\mathcal{L}}(\varphi^r(x))$$

satisfies the requirement. And similarly, it is non-negative if c is ample or base-free. □

3 Approximations of Algebraic Numbers

Subspace Theorem

References are [B-G06], [Sch70], [E-S02], [Eve96] and [F-W94].

Lemma (15.2.3.1). ⌟

Thm. (15.2.3.2)[Subspace Theorem, Schmidt/Vojta]. For $F \in \mathtt{NField}$ and $S \subset \Sigma_F$ a finite subset of places, $n \in \mathbb{N}, \varepsilon \in \mathbb{R}_+$. For $v \in S$, let $\{L_{v0}, \ldots, L_{vm_v}\}$ be a set of linear forms in $\overline{F_v}[X_0, \ldots, X_n]$ in general position. Then

- If $\Sigma_F^\infty \subset S$, then there are f.m. rational linear hyperspaces $T_1, \ldots, T_h$ of $\mathbb{A}_F^{n+1}$ s.t.

$$\Big\{\underline{x} \in \mathcal{O}_{F,S}^{n+1} \setminus \{0\} \Big| \prod_{v\in S} \prod_{i=0}^{m_v} |L_{vi}(\underline{x})|_v < H([\underline{x}])^{-\varepsilon}\Big\} \subset T_1 \cup \ldots \cup T_h.$$

- There exists f.m. rational hyperplanes $T_1, \ldots, T_h$ of $\mathbb{P}_F^n$ s.t.

$$\Big\{[\underline{x}] \in \mathbb{P}^n(F) \Big| \prod_{v\in S} \prod_{i=0}^{m_v} \frac{|L_{vi}(\underline{x})|_v}{H_v(\underline{x})} < H([\underline{x}])^{-n-1-\varepsilon}\Big\} \subset T_1 \cup \ldots \cup T_h.$$

⌟

Proof: 2: Firstly, it suffices to prove for $m_v = n$ for any v: We may assume $m_v \geq n$ by adding coordinate functions. And after partitioning into f.m. cases and reordering, we may assume that

$$|L_{v0}(\underline{x})|_v \leq |L_{v1}(\underline{x})|_v \leq \ldots \leq |L_{vm_v}(\underline{x})|_v.$$

As $L_{v0}, \ldots, L_{vn}$ are linearly independent, they form a basis for $\mathcal{O}_{\mathbb{P}^n}(1)$, so there are constants C_v s.t.

$$H_v(\underline{x}) \leq C_v \max_{0\leq i\leq n} |L_{vi}(\underline{x})|_v = C_v|L_{vn}(\underline{x})|_v \leq C_v|L_{vk}(\underline{x})|_v, \forall k > n.$$

Thus

$$\prod_{v\in S}\prod_{i=0}^{n}\frac{|L_{vi}(\underline{x})|_v}{H_v(\underline{x})}\leq C\prod_{v\in S}\prod_{i=0}^{m_v}\frac{|L_{vi}(\underline{x})|_v}{H_v(\underline{x})},$$

and the assertion follows from the case $m_v=n$, as the constant C can be eliminated by applying Northcott's theorem(15.2.1.24).

Secondly, item2 implies item1: For $\underline{x}\in\mathcal{O}_{F,S}^{n+1}$,

$$H([\underline{x}])=\prod_{v\in\Sigma_F}H_v(\underline{x})\leq\prod_{v\in S}H_v(\underline{x}),$$

so $[\underline{x}]$ is in the set considered in item2. And any two $\underline{x},\underline{x}'$ with $[\underline{x}]=[\underline{x}']$ are contained in the same hyperplane.

Conversely, item1 implies item2: We may assume that S is sufficiently large that $\Sigma_F^\infty\subset S$ and $\mathrm{cl}(\mathcal{O}_{F,S})<\infty$, because if we add a place v and take $L_{vi}(\underline{x})=x_i$, then $|L_{vi}(\underline{x})|_v\leq H_v(\underline{x})$ for each i. Then for any $[\underline{x}]$ satisfying the inequality of item2, take the fractional ideal

$$\mathfrak{X}=\sum x_i\mathcal{O}_{F,S},$$

then $\mathfrak{X}=(\delta)$ for some $\delta\in K^\times$. And If $v\notin S$, we can see that $|\delta|_v=\max_i|x_i|_v=H_v(\underline{x})$. So we may change $\underline{x}$ to $\underline{x}'=\delta^{-1}\underline{x}$, in which case, $\underline{x}'\in\mathcal{O}_{F,S}^{n+1}\setminus\{0\}$, and $H_v(\underline{x}')=1$ for $v\notin S$. So $\prod_{v\in S}H_v(\underline{x}')=H([\underline{x}'])=H([\underline{x}])$, and the inequality in item2 implies $\underline{x}'$ is in the subset in item1. Thus we are done.

Thus it suffices to prove item1: For this, Cf.[B-G06]P197.? □

Cor. (15.2.3.3) [Schmidt]. Let $\alpha_0,\dots,\alpha_n\in\overline{\mathbb{Q}}$, then for any $\varepsilon\in\mathbb{R}_+$, there are only f.m. $\underline{x}\in\mathbb{Z}^{n+1}$ s.t.

$$0<|\alpha_0x_0+\ldots+\alpha_nx_n|\leq H(\underline{x})^{-n-\varepsilon}.$$

⌟

Proof: Use induction on n. For $n=0$, this is trivial. For $n\geq1$, the subspace theorem(15.2.3.2) with

$$F=\mathbb{Q},S=\{\infty\},L_{v0}=\alpha_0X_0+\ldots+\alpha_nX_n,\quad L_{vi}=X_i,1\leq i\leq n$$

implies that the desired set is contained in f.m. rational linear subspaces of $\mathbb{A}_{\mathbb{Q}}^{n+1}$. Thus we can assume that the desired set all satisfy a linear relation of the form $\sum_j A_jX_j=0$, with $A_n\neq0$. Then with $\beta_n=\alpha_i-\alpha_nA_i/A_n$,

$$0<|\alpha_0x_0+\ldots+\alpha_nx_n|=|\beta_0x_0+\ldots+\beta_{n-1}x_{n-1}|\leq H(x)^{-n-\varepsilon}\leq H(x)^{-n+1-\varepsilon}.$$

Thus the assertion follows from induction hypothesis. □

Cor. (15.2.3.4) [Schmidt]. Let $\alpha\in\overline{\mathbb{Q}}$ and $d\in\mathbb{Z}_+,\varepsilon\in\mathbb{R}_+$, then there exists only f.m. $\xi\in\overline{\mathbb{Q}}$ with $\deg(\xi)=d$ and

$$|\alpha-\xi|\leq H^+(\xi)^{-d(d+1)-\varepsilon},$$

⌟

Proof: For any such ξ, $|\xi-\alpha|\leq1$, and we may assume that ξ is not conjugate to α, so $f_\xi(\alpha)\neq0$. Suppose $f_\xi=x_0+x_1T+\ldots+x_dT^d\in\mathbb{Z}[T]$ with coprime coefficients, then $H(f_\xi)=\Theta(H^+(\xi)^d)$ by(15.2.1.12). Thus by mean-value theorem,

$$0<|f_\xi(\alpha)|=|x_0+x_1\alpha+\ldots+x_d\alpha^d|\leq C_\alpha|\alpha-\xi|H(f_\xi)\leq H(f_\xi)^{-d-\frac{\varepsilon}{d}}=H(\underline{x})^{-d-\frac{\varepsilon}{d}}.$$

So the assertion follows from(15.2.3.3). □

Prop. (15.2.3.5) [Absolute Subspace Theorem, Evertse-Schlickewei]. [B-G06]P228.? ⌟

Roth's Theorem

Lemma (15.2.3.6) [Roth's Lemma]. ⌟

Thm. (15.2.3.7) [Roth]. Let $F \in \mathtt{NField}$ and $\Sigma_F^\infty \subset S \subset \Sigma_F$ be finite, and for each $v \in S$ a number $\alpha_v \in \overline{F_v}$. Then for any $\varepsilon > 0$, there are only f.m. $\beta \in F$ that

$$\prod_{v\in S} H_v(\beta - \alpha_v) = \prod_{v\in S} \min(1, |\beta - \alpha_v|_v) \leq H^+(\beta)^{-2-\varepsilon}(15.2.1.5).$$

Moreover, α_v can be ∞ as well, in the sense that $|\beta - \alpha_v|_v = |\beta|_v^{-1}$. ⌟

Proof: It is clear that it suffices to show that there are only f.m. $\beta \in F$ s.t.

$$\prod_{v\in S} |\beta - \alpha_v|_v \leq H^+(\beta)^{-2-\varepsilon}, \quad |\beta - \alpha_v|_v < 1.$$

Let $x = [1, \beta] \in \mathbb{P}^1(K)$ and let $L_{v0} = X_1 - \alpha_v X_0$(If $\alpha_v = \infty$, take $L_{v0} = X_0$), then for any such β,

$$\prod_{v\in S} \frac{|L_{v0}(x)|_v}{H_v(\underline{x})} = \prod_{v\in S} |\beta - \alpha_v|_v \max(1, |\beta|_v)^{-1} \leq H^+(\beta)^{-2-\varepsilon}.$$

Thus the assertion follows from the subspace theorem(15.2.3.2). □

Remark (15.2.3.8). The exponent in Roth's theorem is the best possible, by(15.2.4.3).

This theorem is ineffective in the sense it doesn't give a maximal bound on $H(\beta)$ for a solution β, but it is effective in the sense it gives a bound for the number of solutions. ⌟

Remark (15.2.3.9). This is not true for function fields, as if we choose F to be the splitting field of the separable polynomial $x^q - x + t$ over $\mathbb{F}_p(t)$, then there is a valuation w over the valuation v corresponding to (t) s.t. $F_w = \mathbb{F}_p((t))$, and $\alpha = t + t^q + t^{q^2} + \ldots$. Take $\beta_k = t + t^q + \ldots + t^{q^k}$, then $|\beta_k - \alpha|_v = c^{-q^{k+1}}$ with $H(\beta_k) = c^{q^k} = H(\beta)^{-q}$, thus cannot have a Roth's theorem. ⌟

Proof: □

Cor. (15.2.3.10) [Classical Roth's Theorem]. For any $\alpha \in \overline{\mathbb{Q}}$ and $\varepsilon > 0$, there are only f.m. $p/q \in \mathbb{Q}$ s.t. $|p/q - \alpha| \leq |q|^{-2-\varepsilon}$. ⌟

Proof: Take $F = \mathbb{Q}, S = \{\infty\}$ and $\alpha_\infty = \alpha$, then use Roth's theorem(15.2.3.7). □

Cor. (15.2.3.11). For an element $\alpha \in \mathbb{Q}_p$ and $\varepsilon > 0$, there are only f.m. $n \in \mathbb{Z}$ s.t. $|n - \alpha|_p \leq |n|^{-1+\varepsilon}$. ⌟

Proof: Take $F = \mathbb{Q}, S = \{\infty, p\}$ and $\alpha_\infty = \infty, \alpha_p = \alpha$, then use Roth's theorem(15.2.3.7). □

Cor. (15.2.3.12) [Another Interpretation]. Let $F \in \mathtt{GField}$ and v a valuation of $\overline{F}$, C be a complete curve over F and $Q \in C(\overline{F})$, then for $f \in K(C)^*$,

$$\varliminf_{P\in C(F), d_v(P,Q)\to 0} \frac{\log d_v(P;Q)}{\log H_F(f(P))} \geq -2.$$

⌟

Proof: Replacing f by $1/f$ if necessary, we can assume $f(Q)\neq\infty$. Let $f-f(Q)$ has order e at Q, then by(15.2.1.32),

$$\varinjlim_{P\in C(F),d_v(P,Q)\to 0}\frac{\log|f(P)-f(Q)|_v}{\log d_v(P,Q)}=e.$$

And Roth's theorem implies

$$H_K(f(P))^{2+\varepsilon}|f(P)-f(Q)|_v\geq 1$$

for a.e. P. Thus by taking limit and varying ε, the conclusion follows. □

Cor. (15.2.3.13) [Thue's Equation]. Let $F(x,y)\in\mathbb{Z}[x,y]$ be a homogenous polynomial that has at least three different linear factors in $\mathbb{C}[x,y]$, then for any $m\in\mathbb{Z}^\times$, there are only f.m. solutions of $F(x,y)=m$ in $\mathbb{Z}^2$. ⌟

Proof: Let $F_1,\ldots,F_r$ be non-isomorphic irreducible polynomials in $\mathbb{Z}[x,y]$ dividing F, suppose there are i.m. solutions to $F(x,y)=m$, then there are inf.m. rational points x_n/y_n converging but not equal to a root of F_i for each i. Thus $r=1$, and $\deg F_1\geq 3$ by hypothesis. And it is clear that for some root α of F_1 and some constant $C>0$, there are i.m. rational points n s.t. $|x_n/y_n-\alpha|\leq C|y_n|^{-3}$, contradicting Roth's theorem(15.2.3.10). □

Prop. (15.2.3.14) [Quantitative Bounds for Roth's Theorem]. Cf.[B-G06]Chap6.5. ⌟

Prop. (15.2.3.15) [Liouville]. Let $\alpha\in\overline{\mathbb{Q}},d=\deg(\alpha)\geq 2$, then there is a constant $C>0$ s.t. for all $p/q\in\mathbb{Q}$, $|p/q-\alpha|\geq C/q^d$. Notice only the $d=2$ case is not covered by Roth's theorem(15.2.3.10). ⌟

Proof: We can assume $\alpha\in\mathbb{R}$, because otherwise $C=\operatorname{Im}\alpha$ works. Let $f(T)\in\mathbb{Z}[T]$ be a minimal polynomial of α over $\mathbb{Q}$, then f has no roots in $\mathbb{Q}$. Suppose C_1 is the maximum of $|f'(t)|$ for $t\in[\alpha-1,\alpha+1]$. Suppose $|p/q-\alpha|\leq 1$, then $|f(p/q)|=|f(p/q)-f(\alpha)|\leq C_1|p/q-\alpha|$, and also $q^df(p/q)\in\mathbb{Z}$ thus $|q^df(p/q)|\geq 1$. Thus we get $|p/q-\alpha|\geq 1/C_1q^d$. Thus for general p/q, $C=\min(C_1^{-1},1)$ works. □

Diophantine Approximation on Abelian Varieties

Prop. (15.2.3.16) [Product Theorem, Faltings]. Suppose $k\in\texttt{Field}^0,k=\overline{k}$, $m,n_1,\ldots,n_m\in\mathbb{Z}_+$, $P=\mathbb{P}_k^{n_1}\times\ldots\times\mathbb{P}_k^{n_m}$, for any $f\in\Gamma(P,\mathcal{O}_P(d_1,\ldots,d_m))\setminus\{0\}$ where $d_1>d_2\ldots>d_m$ are positive integers, denote

$$Z_\sigma(f)=\{x\in P(K):\frac{\partial^\alpha}{\partial\underline{x}^\alpha}f=0,\quad\forall\alpha,\alpha/\underline{d}<\sigma\},\sigma\in\mathbb{R}_+.$$

Then for any $\varepsilon\in\mathbb{R}_+$, there exists $C>0$ satisfying the following: If $d_h/d_{h+1}\geq C$ for $h=1,2,\ldots,m-1$, then for any $\sigma\in\mathbb{R}_+$, any irreducible component Z of $Z_\sigma\cap Z_{\sigma+\varepsilon}$ is of the form $Z=Z_1\times\ldots Z_m$, where Z_i are closed subvarieties of $\mathbb{P}_K^{n_i}$ with $\deg(Z_i)$ bounded in terms of ε and $n_1+\ldots+n_m$ only. ⌟

Proof: ? □

4 Approximations by Algebraic Numbers

Rational Approximations and Continued Fractions

Def. (15.2.4.1) [Best Rational Approximations]. For $\alpha \in \mathbb{R}$, $\frac{a}{b} \in \mathbb{Q}$ is called a **best rational approximation** for α if

$$|b\alpha - a| = ||b\alpha|| < ||d\alpha||$$

for any $d \in \mathbb{Z}_+, d < b$. ⌟

Thm. (15.2.4.2). For any $\alpha \in \mathbb{R}$ and $n \in \mathbb{Z}_+$, there exists $b \in \mathbb{Z}_+, b \leq n$ s.t.

$$||b\alpha|| < \frac{1}{n+1}.$$

So there exists $\frac{a}{b} \in \mathbb{Q}$ with $1 \leq b \leq n$ s.t.

$$|\alpha - \frac{a}{b}| \leq \frac{1}{b(n+1)}.$$

⌟

Proof: Consider the $n+1$ numbers

$$0, \alpha, 2\alpha, \ldots, n\alpha \in \mathbb{R}/\mathbb{Z},$$

then there are two of them with distance$\leq \frac{1}{n+1}$. Thus their difference gives such a b. □

Thm. (15.2.4.3) [Dirichlet-Hurewitz]. For any $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, there are infinitely many $\frac{p}{q} \in \mathbb{Q}$ s.t. $|\frac{p}{q} - \alpha| \leq \frac{1}{\sqrt{5}q^2}$. ⌟

Proof: Cf. [G. H. Hardy and E. M. Wright. An introduction to the theory of numbers]Thm194**?**. We prove here for a weaker result:

For $N > 0$, consider the sets $\{\{q\alpha\} | q = 0, \ldots, N\}$, where $\{\beta\}$ are the fractional part of β. Then by pigeonhole principle gives two $0 \leq q_1 < q_2 \leq N$ s.t. $|(q_1 - q_2)\alpha - p| \leq 1/N \leq (q_2 - q_1)$. Let $q = q_2 - q_1$, then $|p/q - \alpha| \leq 1/q^2$. □

Def. (15.2.4.4) [Continued Fractions]. ⌟

Def. (15.2.4.5) [Diophantine Numbers]. For $\mu \in \mathbb{R}_{\geq 2}$, a (C, μ)-**Diophantine number** is a number $\theta \in \mathbb{R}$ s.t. there exists $C \in \mathbb{R}_+$ s.t. for any $p, q \in \mathbb{Z}_+, q \neq 0$,

$$|\theta - \frac{p}{q}| \geq \frac{C}{q^\mu}.$$

And a **badly approximable number** is a $(C, 2)$-Diophantine number for some $C \in \mathbb{R}_+$. ⌟

Prop. (15.2.4.6). $\xi \in \mathbb{R}$ is badly approximable iff the fractional expansion $\xi = [a_0; a_1, a_2, \ldots]$ satisfies $(a_n)_{n\in\mathbb{N}}$ is bounded. ⌟

Proof: Cf.[Distributions Modulo 1]P245. □

Prop. (15.2.4.7) [Approximation and Fractional Expansions]. Let $M \in \mathbb{Z}_+, \kappa, \mu \in [0, 1]$, $A \in \mathbb{R}_+, B \in \mathbb{R}_{>1}$, and $\frac{p}{q}$ is a fractional approximation of κ s.t. $q > 6M$. Let $\varepsilon = ||q\mu|| - M||q\kappa||$, then

- If $\varepsilon > 0$, then there is no solution of the inequality
$$|m\kappa - n + \mu| < AB^{-m}$$
for $m, n \in \mathbb{Z}$ with $\frac{\log(Aq/\varepsilon)}{\log B} \leq m \leq M$.
- (This may apply when $\kappa + \mu$ is close to 1)If $\varepsilon < 1/3$ but $\lfloor q\mu + 0.5 \rfloor = q - p$, then there is no solution of the inequality
$$|m\kappa - n + \mu| < AB^{-m}$$
for $m, n \in \mathbb{Z}$ with $\max(\frac{\log(3Aq)}{\log B}, 1) < m \leq M$.

⌟

Proof: 1: Assume $0 \leq m \leq M$, then
$$|m(q\kappa - p) + (mp - nq) + q\mu| < qAB^{-m},$$
so
$$qAB^{-m} > |mp - nq + q\mu| - m||q\kappa|| \geq ||q\mu|| - M||q\kappa|| = \varepsilon.$$
2: Assume $0 \leq m \leq M$, then
$$|m(q\kappa - p) + (mp - nq + r) + (q\mu - r)| < qAB^{-m},$$
so
$$|mp - nq + r| < qAB^{-m} + ||q\mu|| + M||q\kappa|| < qAB^{-m} + 2/3.$$
If $qAB^{-m} \leq 1/3$, then $mp - nq + r = 0$. But then the hypothesis implies that $m \equiv 1 (\mathrm{mod}\ q)$. As $q > 6M$, this means $m = 1$. □

Higher Degree case

Prop. (15.2.4.8) [Dirichlet-Hurewitz/Davenport-Schmidt]. For $d \in \mathbb{Z}_+$, let $k_d \in [-1, \infty]$ be the supremum of numbers $w \in \mathbb{R}_+$ s.t. for any $\alpha \in \mathbb{R}$ not an algebraic number of degree$\leq d$ and any $\varepsilon \in \mathbb{R}_+$, there exists a constant $C = C(\alpha, \varepsilon)$ s.t. there are inf.m. real algebraic number ξ of degree d satisfying
$$|\alpha - \xi| \leq CH^+(\xi)^{-dk_d+\varepsilon}.$$
Then
- $k_1 = 2$ by(15.2.4.3).
- $k_2 = 3$.
- $k_d \leq d + 1$.

⌟

Proof: 2: One direction is by(15.2.3.4), the other by [Davenport-Schmidt, Approximation to real number by quadratic irrationals]?.
3 follows from(15.2.3.4). □

Prop. (15.2.4.9) [Dirichlet-Hurewitz/Davenport-Schmidt/Roy]. For $d \in \mathbb{Z}_+$, let $k_d \in [-1, \infty]$ be the supremum of numbers $w \in \mathbb{R}_+$ s.t. for any $\alpha \in \mathbb{R}$ not an algebraic integer of degree$\leq d$ and any $\varepsilon \in \mathbb{R}_+$, there exists a constant $C = C(\alpha, \varepsilon)$ s.t. there are inf.m. real algebraic number ξ of degree d satisfying
$$|\alpha - \xi| \leq CH^+(\xi)^{-dk_d+\varepsilon}.$$
Then

- $k_1 = -1$ trivially.
- $k_2 = 3$.
- $k_3 = \frac{3+\sqrt{5}}{2}$.
- $\lfloor \frac{d+1}{2} \rfloor \leq k_d \leq d+1$.

⌟

Proof: 2: One direction is Roth's theorem, the other is [Davenport-Schmidt, Approximation to real number by algebraic integers].

3: [Davenport-Schmidt, Approximation to real number by algebraic integers] and [Approximation by cubic algebraic integers, Roy].

4: (15.2.3.4) and [Davenport-Schmidt, Approximation to real number by algebraic integers] and [Approximation by cubic algebraic integers, Roy]. □

5 Dynamics on $\mathbb{T}^1$

References are [Bug12].

Equidistributions

Thm. (15.2.5.1) [Weyl's Criterion]. Given $n \in \mathbb{Z}_+$ and a sequence $(\underline{x}_n) \in (\mathbb{R}^n)^{\mathbb{Z}_+}$, the following are equivalent:

- $(\underline{x}_n)$ is equidistributed modulo $\mathbb{Z}^n$.
- For any $\mathbb{Z}^n$-periodic function $f \in C(\mathbb{R};\mathbb{C})$,
$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^N f(\underline{x}_n) = \int_{[0,1]^n} f(x)\mathrm{d}x.$$
- For any $h \in \mathbb{Z}^n \setminus 0$,
$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^N e^{2\pi \mathrm{i} \sum_{i=1}^N h_i x_i} = 0.$$

⌟

Proof: 1 and 2 follows easily from the definition of Riemann integration.

2 and 3 follows from the Stone-Weierstrass theorem that the set of trigonometric functions is dense in $\mathrm{C}_{\mathbb{C}}([0,1])$(11.3.8.3). □

Cor. (15.2.5.2). For any $m \in \mathbb{Z}_+$, if $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$ and $\{1, \alpha_1, \ldots, \alpha_n\}$ is linearly independent over $\mathbb{Q}$, then $(n\alpha_1, \ldots, n\alpha_m)_{n\in\mathbb{Z}_+}$ is equidistributed modulo $\mathbb{Z}^m$. ⌟

Proof: The hypothesis implies that for any $h \in \mathbb{Z}^n \setminus 0$, $\sum h_i \alpha_i \notin \mathbb{Q}$. Thus it is easy to see that
$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^N e^{2\pi \mathrm{i} \sum_{i=1}^N h_i x_i} = 0.$$
□

Cor. (15.2.5.3). If $(x_n) \in \mathbb{R}^{\mathbb{Z}_+}$ is a sequence that is equidistributed modulo 1, and $(y_n) \in \mathbb{R}^{\mathbb{Z}_+}$ is a convergent sequence, then $(x_n + y_n)_{n\in\mathbb{Z}_+}$ is also equidistributed modulo 1. ⌟

Thm. (15.2.5.4) [Weyl]. Let $d \in \mathbb{Z}_+$ and $P(X) = a_d X^d + \ldots + a_1 X + a_0 \in \mathbb{R}[X]$ s.t. at least one of $a_1, \ldots, a_d$ is irrational, then the sequence $(P(n))_{n \in \mathbb{Z}_+}$ is equidistributed modulo 1. ⌟

Proof: Cf.[Bug12]P2.**?** □

Prop. (15.2.5.5). Given any sequence $(x_n)_{n \in \mathbb{Z}_+} \in \mathbb{R}^{\mathbb{Z}_+}$ s.t.

$$\liminf_{n \to \infty} (x_{n+1} - x_n) > 0,$$

then for Lebesgue-a.e. $\xi \in \mathbb{R}$, the sequence $(\xi x_n)_{n \in \mathbb{Z}_+}$ is equidistributed modulo 1.

In particular, this is true for $x_n = \alpha^n$ where $\alpha \in \mathbb{R}, |\alpha| > 1$. ⌟

Proof: Cf.[Distribution modulo 1]P6.**?** □

Prop. (15.2.5.6). Given any $\xi \in \mathbb{R}^\times$, then for Lebesgue-a.e. $\alpha \in \mathbb{R}$ with $|\alpha| > 1$, the sequence $(\xi \alpha^n)_{n \in \mathbb{Z}_+}$ is equidistributed modulo 1. ⌟

Proof: Cf.[Distribution modulo 1]P8.**?** □

Discrepency of Distributions

Def. (15.2.5.7)[Discrepancy]. For $N \in \mathbb{Z}_+$ and $x_1, \ldots, x_N \in \mathbb{R}$, the **discrepency** between $x_1, \ldots, x_N$ is defined to be

$$D_N(x_1, \ldots, x_N) \triangleq \sup_{0 \leq u < v \leq 1} \left|\frac{\#\{k \in [N]_+ | \{x_k\} \in [u, v)\}}{N} - (v - u)\right|.$$

⌟

Prop. (15.2.5.8). A sequence $(x_N) \in \mathbb{R}^{\mathbb{Z}_+}$ is equidistributed modulo 1 iff $\lim_{N \to \infty} D_N(x_1, \ldots, x_N) = 0$. ⌟

Proof: This follows from the uniform convergence theorem. □

Prop. (15.2.5.9). For any sequence $(x_N) \in \mathbb{R}^{\mathbb{Z}_+}$, there are infinitely many $N \in \mathbb{Z}_+$ s.t.

$$D_N(x_1, \ldots, x_N) \geq \frac{\log N}{25N}.$$

⌟

Proof: Cf.[Sequences, Discrepancies and Applications] or [Uniform distribution of sequences]. □

Multiplication by Rational Numbers

Prop. (15.2.5.10). If $b \in \mathbb{Z}_{\geq 2}$ and $\xi \in \mathbb{R} \setminus \mathbb{Q}$, the numbers $\{\xi b^n\}_{n \in \mathbb{Z}_+}$ cannot be contained in an interval of length strictly shorter than $1/b$.

And this bound is strict, by considering the Sturmian words(25.7.1.4). ⌟

Proof: Let $\{\xi\} = [0.a_1 a_2 \ldots]_b$, then we may assume that there exists some $l \in [b-2]$ s.t. $a_i \in \{l, l+1\}$ for any $i \in \mathbb{Z}_+$, otherwise it is easy to see that the assertion is true. In this case, by(25.7.1.3), for any $m \in \mathbb{Z}_+$, there exists a sequence W_m of m-blocks s.t. $0 \amalg W_m$ and $1 \amalg W_m$ both appear in the sequence $a_1, a_2, \ldots$. Then this will imply that there exists two $u_m, v_m \in \mathbb{Z}_+$ s.t. $\{\xi b^{u_m}\} - \{\xi b^{v_m}\} > b^{-1} - b^{-m}$. As m can be arbitrarily large, the assertion follows. □

Prop. (15.2.5.11) [Mahler]. For any $\varepsilon \in \mathbb{R}_+$, $p, q \in \mathbb{Z}, p > q \geq 2$, and $\gcd(p,q) = 1$, there exists $N \in \mathbb{Z}_+$ s.t. $||(\frac{p}{q})^n|| \geq 2^{-\varepsilon n}$ for any $n \in \mathbb{Z}_{\geq N}$. ⌟

Proof: ?Cf.[Mah57].

Apply Roth's theorem(15.2.3.7) with $K = \mathbb{Q}, S = \{\infty, 2, 3\}$ with $\alpha_\infty = 1, \alpha_2 = \infty, \alpha_3 = 0$, and $\beta_k = 3^k/n2^k$ with $n = \lceil (\frac{3}{2})^k \rceil$. Then $|\beta - \alpha_2|_2 \leq 2^{-k}, |\beta - \alpha_3|_3 \leq 3^{-k}|n|_3^{-1}$, and $H(\beta_k) = 3^k|n|_3$. Thus Roth's theorem says for any $\varepsilon > 0$,

$$|1 - 3^k/n2^k|_\infty \leq 2^k 3^k |n|_3 (3^k|n|_3)^{-2-\varepsilon}$$

holds for only f.m. k. This implies that $\lceil (\frac{3}{2})^k \rceil - (\frac{3}{2})^k \geq 3^{-\varepsilon k}$ holds for a.e. k. Thus we can apply(15.3.4.13). □

Def. (15.2.5.12) [Mahler's Z-Numbers]. $\xi \in \mathbb{R}_+$ is called a **Mahler's Z-number** if $0 < \{\xi(\frac{3}{2})^n\} < 1/2$ holds for any $n \in \mathbb{Z}_+$. ⌟

Multiplication by Algebraic Numbers

Def. (15.2.5.13)[Pisot and Salem Numbers]. A **Pisot number** is an algebraic number $\alpha \in \overline{\mathbb{Z}} \cap \mathbb{R}_{>1}$ s.t. all the Galois conjugates α_i of α except α itself satisfy $|\alpha_i| < 1$.

A **Salem number** is algebraic number $\alpha \in \overline{\mathbb{Z}} \cap \mathbb{R}_{>1}$ s.t. all the Galois conjugates α_i of α except α itself satisfy $|\alpha_i| \leq 1$, and $|\alpha_i| = 1$ for some i. ⌟

Prop. (15.2.5.14) [Pisot]. Let $\alpha \in \mathbb{R}_{>1}, \xi \in \mathbb{R}^\times$ s.t.

$$\sum_{n \in \mathbb{Z}_+} ||\xi \alpha^n||^2$$

converges, then α is a Pisot number(15.2.5.13), and $\xi \in \mathbb{Q}(\alpha)$. ⌟

Proof: Cf.[Distribution Modulo 1]P16.? □

Thm. (15.2.5.15) [Vijayaraghavan]. Let $\alpha \in \mathbb{R}_{>1}, \xi \in \mathbb{R}^\times$ s.t. $(\{\xi\alpha^n\})_{n \in \mathbb{Z}_+}$ has only f.m. limit points, then α is a Pisot number(15.2.5.13), and $\xi \in \mathbb{Q}(\alpha)$. ⌟

Proof: □

Cor. (15.2.5.16). If $\xi \in \mathbb{R}^\times$ and $p, q \in \mathbb{Z}, p > q \geq 2$, then the sequence $(\{\xi(\frac{p}{q})^n\})$ has infinitely many limit points. ⌟

Prop. (15.2.5.17). If $\alpha \in \mathbb{R}_{\geq 1} \cap \overline{\mathbb{Q}}$ with minimal polynomial $q_d X^d + \ldots + q_1 X + q_0 \in \mathbb{Z}[X]$, and

$$\limsup_{n \to \infty} ||\xi \alpha^n|| < \frac{1}{|q_0| + \ldots + |q_n|},$$

then α is a Pisot or Salem number, and $\xi \in \mathbb{Q}(\alpha)$. ⌟

Proof: □

Prop. (15.2.5.18). For any Salem number $\alpha \in \mathbb{R}$, the sequence $(\alpha^n)_{n \in \mathbb{Z}_+}$ is dense modulo 1, but not equidistributed modulo 1. ⌟

Proof: Cf.[Distributions Modulo 1]P57. □

Prop. (15.2.5.19). If $\alpha \in \mathbb{R}$ is a Pisot or Salem number, then there are infinitely many composite numbers in the sequence $(\lfloor \alpha^n \rfloor)_{n \in \mathbb{Z}_+}$. ⌟

Proof: Cf.[Integer parts of powers of Pisot and Salem numbers]?. □

Littlewood Conjecture

Conj. (15.2.5.20) [Littlewood]. For any $(\xi, \eta) \in \mathbb{R}^2$, $\inf_{q \in \mathbb{Z}_+} q.||q\xi||.||q\eta|| = 0$. ⌟

Proof: □

Conj. (15.2.5.21) [Mixed Littlewood Conjecture, Mathan-Teulié]. For any $p \in \mathbf{P}$ and $\xi \in \mathbb{R}$, $\inf_{q \in \mathbb{Z}_+} q.|q|_p.||q\xi|| = 0$. ⌟

15.3 Diophantine Geometry

References are [Galois Cohomology, Serre]Chap2.4.5, [B-G06], [Fundamentals of Diophantine Geometry, Lang], [Weil50].

Arithmetic of varieties(i.e. varieties over absolutely f.g. fields) that are not necessarily Abelian varieties are studied in this section. The Abelian variety case is studied in Arithmetic of Abelian Varieties.

1 Hilbert's 10-th Problem

Diophantine Sets

Def. (15.3.1.1) [Diophantine Sets]. For $m \in \mathbb{Z}_+$, a subset $E \subset (\mathbb{Z}_+)^m$ is called a **Diophantine set** if there exists $n \in \mathbb{N}$ and a polynomial

$$P(T_1, \ldots, T_m, X_1, \ldots, X_n) \in \mathbb{Z}[T_1, \ldots, T_m, X_1, \ldots, X_n]$$

s.t.

$$(t_1, \ldots, t_m) \in E \iff \exists (x_1, \ldots, x_n) \in \mathbb{Z}^n, P(t_1, \ldots, t_m, x_1, \ldots, x_n) = 0.$$

⌟

Prop. (15.3.1.2). Any Diophantine set is recursively denumerable(2.7.2.7). ⌟

Prop. (15.3.1.3). The class of Diophantine sets contains the level sets of integral polynomials, and is closed under finite direct sums, finite intersections and projections. ⌟

Prop. (15.3.1.4) [Diophantine Sets in $\mathbb{Z}_+$]. $S \subset \mathbb{Z}_+$ is a Diophantine subset iff there exists $n \in \mathbb{Z}_+$ and $P \in \mathbb{Z}[X_1, \ldots, X_n]$ s.t.

$$S = \{m \in \mathbb{Z}_+ | \exists (X_1, X_2, \ldots, X_n) \in \mathbb{Z}^n | P(X_1, \ldots, X_n) = m\}$$

⌟

Proof: One direction is clear. For the other, notice if there exists $n \in \mathbb{N}$ and $Q \in \mathbb{Z}[X_1, \ldots, X_n]$ s.t.

$$S = \{m \in \mathbb{Z}_+ | \exists (X_1, X_2, \ldots, X_n) \in \mathbb{Z}^n | P(m, X_1, \ldots, X_n) = 0\},$$

then take $P(X_0, X_1, \ldots, X_n) = X_0(1 - P^2(X_0, X_1, \ldots, X_n))$. □

Prop. (15.3.1.5) [Examples of Diophantine Sets].

- For $a, n \in \mathbb{Z}_+$, suppose

$$(a + \sqrt{a^2 - 1})^n = x_n(a) + y_n(a)\sqrt{a^2 - 1},$$

  where $x_n(a), y_n(a) \in \mathbb{Z}_+$, then the set $E = \{(y, n, a) \in (\mathbb{Z}_+)^3 | y = y_n(a)\}$ is a Diophantine set.
- The set $E_0 = \{(y, n, a) \in (\mathbb{Z}_+)^3 | y = a^n\}$ is a Diophantine set.
- The set $E = \{(r, k, n) \in (\mathbb{Z}_+)^3 | r = \binom{n}{k}, n \geq k\}$ is a Diophantine set.
- The set $E = \{(m, k) | m = k!\}$ is a Diophantine set.
- The set $E = \{(x, y, p, q, k) | \frac{x}{y} = \binom{p/q}{k}, p > qk\}$ is a Diophantine set.

⌟

Proof: Cf.[Manin, P99].
1: □

Cor. (15.3.1.6) [`Prime` is Diophantine]. `Prime` $\subset \mathbb{Z}_+$ is a Diophantine set. ⌟

Proof: This is because by Wilson's theorem(2.6.3.30), for $p \in \mathbb{Z}_+$, p is a prime iff it is the first coordinate of the following Diophantine equation

$$\{(p, f, a) \in \mathbb{Z}_+ | p = f + 1, \quad q = f!, \quad q - ap = 1\}.$$

□

Thm. (15.3.1.7) [Matiyasevich]. Any recursively denumerable subset of $(\mathbb{Z}_+)^n$ is a Diophantine subset. ⌟

Proof: Cf.[M. Davis, J. Matijasevic, and J. Robinson, Hilbert's 10th Problem. Diophantine equations: Positive aspects of a negative solution, in Mathematical Developments from Hilbert's Problems, F. Browder, ed., American Mathematical Societ, Providence, RI, 1976.] □

Cor. (15.3.1.8) [Hilbert's 10-th Problem, Matiyasevich]. Hilbert's 10-th problems is undecidable/computable/recursive(2.7.2.6). ⌟

Proof: □

Def. (15.3.1.9) [Simple Diophantine Sets]. A **simple Diophantine set** is a Diophantine set $G \subset \mathbb{Z}_+$ s.t. $\mathbb{Z}_+ \setminus G$ is not Diophantine, and for any infinite Diophantine subset $D \subset \mathbb{Z}_+$, $D \cap G \neq \varnothing$. ⌟

Prop. (15.3.1.10). There exists a simple Diophantine set(15.3.1.9). ⌟

Diophantine Coding

Prop. (15.3.1.11) [Cantor Numbering of Tuples]. We can encode the pair of natural numbers in the following way:

$$(0,0), (0,1), (1,0), (0,2), (1,1), (2,0), (0,3), \ldots.$$

Equivalently, the **Cantor numbering** is defined to be

$$\mathrm{Cant}(a, b) = \frac{(a+b)^2 + 3a + b}{2}.$$

And

$$\mathrm{Cant}(a, b) = c \iff \exists y[(a+y)^2 + 3a + y = 2c], \quad \mathrm{Cant}(a, b) = c \iff \exists x[(x+b)^2 + 3x + b = 2c].$$

Similar, for $n \in \mathbb{Z}_+$, we can define numbering for n-tuples inductively as

$$\mathrm{Cant}_1(a_1) = a_1, \quad \mathrm{Cant}_2(a_1, a_2) = \mathrm{Cant}(a_1, a_2), \quad \mathrm{Cant}_{k+1}(a_1, \ldots, a_{k+1}) = \mathrm{Cant}_k(a_1, \ldots, a_{k-1}, \mathrm{Cant}_2(a_k, a_{k+1})).$$

⌟

Unsolvability

Diophantine Forms of Problems

Prop. (15.3.1.12) [Riemann Hypothesis]. For a Diophantine form of the negation of Riemann hypothesis, Cf.[The Riemann Hypothesis and Diophantine Equations]. ⌟

2 Conjectures

Def. (15.3.2.1)[Arithmetic Varieties]. An **arithmetic variety** is a regular scheme that is projective and flat over $\mathbb{Z}$. ⌟

Weak Approximation

Prop. (15.3.2.2). If X is a smooth complete intersection of two quadrics in $\mathbb{P}_F^N$ for $N \geq 5$, and $X(F) \neq \varnothing$, then X satisfies weak approximation. ⌟

Proof: Cf.[Colliot-Thelene-Skorobogatov1987, R-equivalence on cubic bundles of degree 4]. □

Mazur's Conjecture

Conj. (15.3.2.3) [Mazur]. Let $X/\mathbb{Q}$ be a smooth algebraic scheme over a field, then the topological closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ consist of a finite union of connected components. ⌟

Proof: □

Remark (15.3.2.4). As the kernel of the Brauer-pairing(10.2.6.1) vanishes on all the infinite places, when the Brauer-Manin obstruction is sufficient, Mazur's conjecture holds. ⌟

Artin's Conjecture

Def. (15.3.2.5) [C_d-Fields]. A field K is called C_k or for any homogenous polynomial $F(X_1,\ldots,X_n)$ of degree d with coefficient in K that $d^k < n$ has a non-zero solution in K^n.

C_0 fields are just alg.closed fields, C_1 fields are also called **quasi-algebraically closed**. ⌟

Prop. (15.3.2.6). Algebraic extensions of a quasi-alg.closed field is quasi-alg.closed. ⌟

Proof: For a homogenous polynomial $F(X_1,\ldots,X_n)$, its coefficient lies in a finite extension of K contained in L, so we may assume L/K is finite. Then choose a basis $\{e_1,\ldots,e_m\}$ of L over K, then consider the function

$$f(x_{11},\ldots,x_{1m},\ldots,x_{n1},\ldots,x_{nm}) = \mathrm{Nm}_{L/K}(F(x_{11}e_1+\ldots+x_{1m}e_m,\ldots,x_{n1}e_1+\ldots+x_{nm}e_m)),$$

which is a homogenous polynomial of degree nm with coefficient in K, because it has values all in K. So it has a nonzero solution in K^{nm} by(6.11.2.3), Krull's height theorem and k is alg.closed. □

Prop. (15.3.2.7) [Chevalley-Waring]. Any finite field $\mathbb{F}_q$ is quasi-algebraically closed. In fact, for any system of homogenous polynomials f_i of n variables, if $\sum_{i=1}^r \deg f_i < d$, then the number of solutions to this equation on $\mathbb{F}_q$ is divisible by p, where q is a p-power. ⌟

Proof: The number of solutions to this system is equivalent to

$$\sum_{x\in\mathbb{F}_q^n}\prod(1-f_i^{q-1}(x))$$

modulo p.

But notice that if $i<q-1$, then $\sum_{x\in\mathbb{F}_q}x^i=0$ in $\mathbb{F}_q$ by(2.6.3.25), but as the degree of the highest term of $\sum_{x\in\mathbb{F}_q^n}\prod(1-f_i^{q-1}(x))$ modulo p is smaller than $n(q-1)$, some x_i has power smaller than $q-1$, thus when summed over $\mathbb{F}_q$, it vanishes. □

Remark (15.3.2.8). This may follow from the fact any smooth projective Fano variety over $\mathbb{F}_q$ has a rational point(15.14.6.3). ⌟

Prop. (15.3.2.9) [Tsen]. Algebraic function fields of dimension 1 over an alg.closed field K is quasi-alg.closed. ⌟

Proof: By(15.3.2.6), it suffice to consider the case $K=k(t)$ purely transcendental. for a polynomial F with coefficient in $k(t)$, we can assume it has coefficient in $k[t]$, then let δ be their maximal degree. If substituted with $X_i=\sum_{i=0}^N a_ijt^j$, the function becomes a system of $\delta+dN+1$ homogenous equation with $n(N+1)$ unknowns a_{ij}, since $d<n$, $\delta+dN+1<n(N+1)$ for N large. In this case, □

Prop. (15.3.2.10). If K is quasi-alg.closed, then $H^2(G(K_s/K),K_s^*)=0$. ⌟

Proof: Cf.[Etale Cohomology Fulei 5.7.15]. □

Cor. (15.3.2.11). By this and(15.3.2.6), the condition of(8.7.2.17) are satisfied. So if K is quasi-alg.closed, then $cd(G(K_s/K))\le 1$ and $H^i(G(K_s/K),K_s^*)=0$ for $i\ge 1$. ⌟

Prop. (15.3.2.12) [Ax-Kochen]. For any d, there is a N_d that if $p>N_d$, then any homogenous polynomial $f(X_1,\dots,X_n)$ of degree d with coefficient in $\mathbb{Q}_p$ that $d^k<n$ has a non-zero solution in $\mathbb{Q}_p^n$. ⌟

Proof: The proof uses Model theory.**?** □

3 Rational Points

Congruent Number Problem

Def. (15.3.3.1)[Congruent Numbers]. For $n\in\mathbb{Z}_+$, n is called a **congruent number** if there exists $(x,y,z)\in\mathbb{Q}^2$ s.t. $x^2+y^2=z^2$ and $\frac{xy}{2}=n$.

By(15.3.5.2), this is equivalent to the existence of $(r,s,t)\in\mathbb{Z}_+$ s.t.

$$rs(r^2-s^2)=nt^2.$$

⌟

Prop. (15.3.3.2). For any $n\in\mathbb{Q}_+$, there is a bijection of sets:

$$\{x<y<z\in\mathbb{Q}_+|x^2+y^2=z^2,\frac{xy}{2}=n\}\longleftrightarrow\{a\in\mathbb{Q}|a\in\mathbb{Q}^2,a+n\in\mathbb{Q}^2,a-n\in\mathbb{Q}^2\}$$

given by

$$(x,y,z)\mapsto a=(\frac{z}{2})^2,\quad a\mapsto(\sqrt{a+n}-\sqrt{a-n},\sqrt{a+n}+\sqrt{a-n},2\sqrt{a}).$$

In particular, $n\in\mathbb{Z}_+$ is a congruent number iff there exists $x\in\mathbb{Q}_+$ s.t. $x,x+n,x-n$ are all rational squares. ⌟

Prop. (15.3.3.3) [Congruent Numbers and Elliptic Curves]. For any $n \in \mathbb{Q}_+$, there is a bijection of sets:

$$\{a,b,c \in \mathbb{Q} | a^2+b^2=c^2, \frac{ab}{2}=n\} \longleftrightarrow \{x,y \in \mathbb{Q} | ny^2 = x^3 - x, y \neq 0\}$$

given by

$$(a,b,c) \mapsto a = (-\frac{b}{a+c}, \frac{2}{a+c}), \quad (x,y) \mapsto (\frac{1-x^2}{y}, \frac{-2x}{y}, \frac{1+x^2}{y}).$$

And it can be shown that the elliptic curve $E^{(n)}: ny^2 = x^3 - x$ satisfies

$$E^{(n)}(\mathbb{Q})_{\text{tor}} = \{O, (0,0), (1,0), (-1,0)\}\text{?}.$$

So n is a congruence number iff $\text{rank}(E^{(n)}/\mathbb{Q}) \geq 1$. ⌟

Thm. (15.3.3.4) [Tunnell]. Let $n \in \mathbb{Z}_+$ be square-free, and $a = \begin{cases} 1 & ,2 \nmid n \\ 2 & ,2|n \end{cases}$. Then if n is a congruent number, then

$$\#\{x,y,z \in \mathbb{Z} | \frac{n}{a} = 2ax^2 + y^2 + 8z^2, 2|z\} = \#\{x,y,z \in \mathbb{Z} | \frac{n}{a} = 2ax^2 + y^2 + 8z^2, 2 \nmid z\}$$

And the converse is also true if we assume the rank part of B-S.D. conjecture for the elliptic curve $E^{(n)}/\mathbb{Q}: y^n = x^3 - n^2 x$. ⌟

Proof: □

Cor. (15.3.3.5) [Fibonacci1220/Fermat1640].

- 1, 2, 3 are not a congruent number.
- 5, 6, 7 are congruent numbers.

⌟

Proof: 1: We give a direct proof: If 1 is a congruent number, then by(15.3.3.1), there exists $r, s \in \mathbb{Z}_+$ s.t. $\gcd(r,s) = 1$, $r \not\equiv s (\text{mod } 2)$, and $rs(r-s)(r+s)$ is a square.

Then $r, s, r+s, r-s$ are pairwise coprime, so there exists $x, y, u, v \in \mathbb{Z}_+$ s.t.

$$r = x^2, \quad s = y^2, \quad r+s = u^2, \quad r-s = v^2,$$

and □

Conj. (15.3.3.6) [Congruence Number Problem]. Any $n \in \mathbb{Z}_+$ s.t. $n \equiv 5,6,7 (\text{mod } 8)$ is a congruence number. ⌟

Proof: □

Remark (15.3.3.7). For $n \in \mathbb{Z}_+$ square-free, the L-function of $E^{(n)}$ has root number

$$\varepsilon(n) = \begin{cases} 1 & ,n \equiv 1,2,3 (\text{mod } 8) \\ -1 & ,n \equiv 5,6,7 (\text{mod } 8) \end{cases}, \quad N(n) = \begin{cases} 32n^2 & ,2 \nmid n \\ 16n^2 & ,2|n \end{cases}.$$

In particular, the parity conjecture of B-S.D implies the congruence number problem(15.3.3.6). ⌟

Proof: □

Conj. (15.3.3.8).

$$\lim_{X \to \infty} \frac{\#\{n \in \mathbb{Z}_+ | n \equiv 1,2,3 (\text{mod } 8) \ \& \ n \text{ is congruent}\} \cap [1,X]}{\#\{n \in \mathbb{Z}_+ | n \equiv 1,2,3 (\text{mod } 8)\} \cap [1,X]} = 0.$$

⌟

4 Integral Points

Simple Cases

Thm. (15.3.4.1) [Pell's Equations]. A **Pell's equation** is a Diophantine equation of the form

$$\{x, y \in \mathbb{Z}_+ | x^2 - dy^2 = N\}$$

where $d \in \mathbb{Z}_+ \setminus (\mathbb{Z}_+)^2$ and $N \in \mathbb{Z}^\times$.

- For $N = 1$, there exists a solution (x_0, y_0) s.t. every solution (x, y) satisfies $(x + \sqrt{d}y) = (x_0 + \sqrt{d}y_0)^k$ for some $k \in \mathbb{Z}_+$. Such a (x_0, y_0) is called a **fundamental solution**.
- In general, if (x_0, y_0) is any solution to the equation for $x^2 - dy^2 = 1$, then every solution (x, y) for $x^2 - dy^2 = N$ satisfies $(x + \sqrt{d}y) = (x' + \sqrt{d}y')(x_0 + \sqrt{d}y_0)^k$ for some $k \in \mathbb{N}$, where $x', y' \in \mathbb{Z}$, and

$$(x')^2 - d(y')^2 = N, \quad |x'| \le \frac{\sqrt{|N|}(\sqrt{u_0} + \sqrt{u_0}^{-1})}{2}, \quad |y'| \le \frac{\sqrt{|N|}(\sqrt{u_0} + \sqrt{u_0}^{-1})}{2\sqrt{|d|}}, \quad u_0 = x_0 + \sqrt{d}y_0.$$

Moreover, if $N > 0$, we even can restrict to $|y'| \le \frac{\sqrt{|N|}(\sqrt{u_0} - \sqrt{u_0}^{-1})}{2\sqrt{|d|}}$ And if $N < 0$, then $y' > 0$. ⌟

Proof: 1: If $N = 1$, then the solutions of this equations are a subgroup of group of units in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. It follows from unit theorem that the group of units in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is isomorphic to $\{\pm 1\} \times \mathbb{Z}$. So because we are restricted to the case that $x, y \in \mathbb{Z}_+$, it follows that the group of solutions is isomorphic to $\mathbb{Z}_+$, and it in fact generated by a single minimal solution (x_0, y_0).

2: We use the regulator map

$$\mathrm{Reg} : \mathbb{Q}(\sqrt{d})^\times \to \mathbb{R}^2 : u \mapsto (\log u, \log \sigma(u)),$$

where σ is the non-trivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Then $\mathrm{Reg}(u_0) = \log(u_0)(1, -1)$, which is linearly independent to $(1, 1)$. Thus for any solution (x, y), there exists $c_1, c_2 \in \mathbb{R}$ s.t.

$$L(x + \sqrt{d}y) = c_1(1, 1) + c_2 L(u_0).$$

In particular, $c_1 = \frac{\log |x + \sqrt{d}y| + \log |x - \sqrt{d}y|}{2} = \frac{\log |N|}{2}$. And we can find $k \in \mathbb{Z}$ s.t. $c_2 = k + \delta$ with $|\delta| \le 1/2$. Therefore if $x' + \sqrt{d}y' = (x + \sqrt{d}y)(x_0 - \sqrt{d}y_0)^{-k}$, then

$$\max(\log |x' + \sqrt{d}y'|, \log |x' - \sqrt{d}y'|) \le \log \sqrt{|N| u_0}.$$

From which we can get the desired bound on x', y'. Finally, notice the hypothesis $x, y \in \mathbb{Z}_+$ implies that we can assume $k \ge 0$. □

Diophantine Sequences

Def. (15.3.4.2) [Diophantine Sequences]. For $m \in \mathbb{Z}_+$, a sequence of positive integers $a_1 \le a_2 \le \ldots \le a_m \in \mathbb{Z}_+$ is called a **Diophantine sequence** of length m if for any $1 \le i < j \le m$,

$$a_i a_j + 1 \in (\mathbb{Z}_+)^2.$$

⌟

Conj. (15.3.4.3). Every Diophantine sequence of length 3 can be extended to a Diophantine quadruple: If (a,b,c) is a Diophantine triple,

$$ab+1=r^2, \quad ac+1=s^2, \quad bc+1=t^2, \quad a,b,c,r,s,t\in\mathbb{Z}_+,$$

then (a,b,c,d) is a Diophantine quadruple where $d=a+b+c+2abc\pm 2rst$.

Then it is conjectured that these are the only two ways of extension. ⌟

Proof: For example,

$$(at\pm rs)^2-1=a^2(bc+1)+(ac+1)(ab+1)\pm 2arst-1=a(a+b+c+2abc\pm 2rst).$$

For the conjecture,? □

Thm. (15.3.4.4) [Baker-Davenport/Kedlaya/Dujella-Pethö].

- If $\{1,3,c\}$ is a Diophantine triple, then there exists $k\in\mathbb{Z}_+$ s.t.

$$c=c_k=\frac{1}{6}[(2+\sqrt{3})(7+4\sqrt{3})^k+(2-\sqrt{3})(7-4\sqrt{3})^k-4].$$

  Notice $c_0=0, c_1=8, c_2=120$.
- $(1,3,c,d)$ is a Diophantine quadruple iff $\{c,d\}=\{c_k,c_{k+1}\}$ for some $k\in\mathbb{Z}_+$.

⌟

Proof: 1:

2: Given item1, it suffices to show that if $k\in\mathbb{Z}_+$, the set of equations

$$\{d,x,y,z\in\mathbb{Z}_+|d+1=x^2, \quad 3d+1=y^2, \quad c_kd+1=z^2\}$$

has only solutions $d\in\{c_{k-1},c_{k+1}\}$.

It's equivalent to solve the Pell'e equation set:

$$\{z^2-c_kx^2=1-c_k, \quad 3z^2-c_ky^2=3-c_k\}.$$

We first prove for $k=1$:

Lemma (15.3.4.5) [The $k=1$ case, Baker-Davenport]. $(1,3,8,d)$ is a Diophantine sequence iff $d=120$. ⌟

Proof: If $(1,3,8,n)$ is a Diophantine sequence, then $n=x^2-1$ for some $x\in\mathbb{Z}_+$. Then there exists $y,z\in\mathbb{Z}_+$ s.t.

$$\{3x^2-2=y^2, \quad 8x^2-7=z^2\}.$$

Thus it suffices to show that such a set of equations has solutions in $\mathbb{Z}_+$ iff $x\in\{1,11\}$.

First, by(15.3.4.1), we can show that positive integral solutions to $y^2-3x^2=-2$ are all of the form

$$y+\sqrt{3}x=(1+\sqrt{3})(2+\sqrt{3})^m, \quad m\in\mathbb{N},$$

thus

$$x=\frac{1+\sqrt{3}}{2\sqrt{3}}(2+\sqrt{3})^m-\frac{1-\sqrt{3}}{2\sqrt{3}}(2-\sqrt{3})^m.$$

If $m=0, x=1$, and if $m=2$, $x=11$.

Similarly, positive integral solutions to $z^2 - 8x^2 = -7$ are all of the form

$$z + \sqrt{8}x = (1+\sqrt{8})(3+\sqrt{8})^n, \quad n \in \mathbb{N}$$

or

$$z + \sqrt{8}x = (5+2\sqrt{8})(3+\sqrt{8})^n = (-1+\sqrt{8})(3+\sqrt{8})^{n+1}, \quad n \in \mathbb{N},$$

thus

$$x = \frac{1+\sqrt{8}}{2\sqrt{8}}(3+\sqrt{8})^n - \frac{1-\sqrt{8}}{2\sqrt{8}}(3-\sqrt{8})^n$$

or

$$x = \frac{-1+\sqrt{8}}{2\sqrt{8}}(3+\sqrt{8})^n - \frac{-1-\sqrt{8}}{2\sqrt{8}}(3-\sqrt{8})^n.$$

Let $P = \frac{1+\sqrt{3}}{2\sqrt{3}}(2+\sqrt{3})^m, m \geq 3$ and $Q = \frac{1+\sqrt{8}}{2\sqrt{8}}(3+\sqrt{8})^n$ or $Q = \frac{-1+\sqrt{8}}{2\sqrt{8}}(3+\sqrt{8})^n$, then we want a solution to

$$P + \frac{2}{3P} = Q + \frac{7}{8Q}.$$

For any such solution, $P > 80$, and

$$P - Q > \frac{2}{3P} - \frac{2}{3Q} = \frac{2(P-Q)}{PQ},$$

so $P > Q$. And also $Q > P - \frac{7}{8Q} > P - \frac{7}{8}$, so

$$P - Q = \frac{7}{8Q} - \frac{2}{3P} < \frac{7}{8(P-\frac{7}{8})} - \frac{2}{3P} < \frac{1}{4P}.$$

Thus

$$0 < \log\frac{P}{Q} < -\log(1 - \frac{1}{4P^2}) < \frac{1}{4P^2} + \frac{1}{16P^4} < 0.26P^{-2},$$

which means that

$$0 < m\log(2+\sqrt{3}) - n\log(3+\sqrt{8}) + \log\frac{(1+\sqrt{3})\sqrt{8}}{(\pm 1+\sqrt{8})\sqrt{3}} < 0.26P^{-2} < \frac{0.11}{(2+\sqrt{3})^{2m}}.$$

Then it follows from Baker's theory(14.7.1.11) that $m < 10^{40}$.
Finally, using(15.2.4.7) twice, it can be shown that no such $m \geq 3$ exists(Cf. [B-D69]). □

After this, assume k is the smallest natural number s.t. the assertion is wrong. Then $k \geq 2$ because $k = 1$ is true by the above lemma(15.3.4.5). Fix $c = c_k \geq 120$. The hypothesis implies that there exists $s, t \in \mathbb{Z}_+$ s.t. $c + 1 = s^2, 3c + 1 = t^2$. So Neither c nor $3c$ is a square. Then it follows from(15.3.4.1) that there exists $z', x' \in \mathbb{Z}, m \in \mathbb{N}, z'', y'' \in \mathbb{Z}, n \in \mathbb{N}$ s.t.

$$z + x\sqrt{c} = (z' + x'\sqrt{c})(s+\sqrt{c})^m, \quad z\sqrt{3} + y\sqrt{c} = (z''\sqrt{3} + y''\sqrt{c})(t + \sqrt{3c})^n,$$

and

$$|z'| \leq \sqrt{c-1}\frac{\sqrt{s+\sqrt{c}} + \sqrt{s+\sqrt{c}}}{2}^{-1} < \sqrt{c}\frac{\sqrt{2s+3}}{2} < \frac{c}{4},$$

$$|z''| \le \sqrt{3(c-3)} \frac{\sqrt{t+\sqrt{3c}} + \sqrt{t+\sqrt{3c}}}{6}^{-1} < \sqrt{t^2-10} \frac{\sqrt{2t+3}}{6} < \frac{c}{6}.$$

If we define sequences

$$\{v_p| : v_0 = z', v_1 = sz' + cx', v_{p+2} = 2sv_{p+1} - v_p\},$$

$$\{w_q| : w_0 = z'', w_1 = tz'' + cx'', w_{q+2} = 2tw_{q+1} - w_q\},$$

then $z = v_m = w_n$. Moreover, we can use induction to show that

$$v_{2p} \equiv z' + 2c(p^2 z' + psx')(\text{mod } c^2), \quad v_{2p+1} \equiv sz' + c[2p(p+1)sz' + (2p+1)x'](\text{mod } c^2), \quad p \in \mathbb{N}.$$

$$w_{2q} \equiv z'' + 2c(3q^2 z'' + qty'')(\text{mod } c^2), \quad w_{2q+1} \equiv tz'' + c[6q(q+1)tz'' + (2q+1)y''](\text{mod } c^2), \quad q \in \mathbb{N}.$$

Then we claim:

Lemma (15.3.4.6). Let $k \in \mathbb{Z}_{\ge 2}$ be the minimal number s.t. there exists $t \in \mathbb{Z}_+$ s.t. $(1, 3, c_k, c_t)$ is a Diophantine sequence, then with $c = c_k$,

- If $v_{2m} = w_{2n}$ has a solution, then $z' = z'' = \pm 1$.
- If $v_{2m+1} = w_{2n}$ has a solution, then $z'' = sz' = \pm s$.
- If $v_{2m} = w_{2n+1}$ has a solution, then $z' = tz'' = \pm t$.
- If $v_{2m+1} = w_{2n+1}$ has a solution, then $z'/t = z''/s = \pm 1$.

⌟

Proof: Cf.[D-P98]P294.? Use minimality of k. □

After this, it is easy to show that $v_{2m} = w_{2n+1}$ or $v_{2m+1} = w_{2n}$ has no solutions by parity reason(notice c is even). For the next two cases:

Lemma (15.3.4.7).

- If $v_{2m} = w_{2n}$, then

$$0 < 2m \log(s + \sqrt{c}) - 2n \log(t + \sqrt{3c}) + \log \frac{\sqrt{3}(\sqrt{c} \pm 1)}{\sqrt{c} \pm \sqrt{3}} < \frac{3}{2}(s + \sqrt{c})^{-4m}.$$

- If $v_{2m+1} = w_{2n+1}$, then

$$0 < (2m+1) \log(s + \sqrt{c}) - (2n+1) \log(t + \sqrt{3c}) + \log \frac{\sqrt{3}(2\sqrt{c} \pm t)}{2\sqrt{c} \pm s\sqrt{3}} < 22(s + \sqrt{c})^{-4m-2}.$$

In particular, in both cases, $m \ge n$. ⌟

Proof: Cf.[D-P98]P298.? The derivation is similar to the $k = 1$ case. □

Cor. (15.3.4.8).

- If $v_{2m} = w_{2n}$, and $m, n \neq 0$, then $n > 0.105\sqrt{c}$.
- If $v_{2m+1} = w_{2n+1}$, and $m, n \neq 0$, then $n > 0.156\sqrt[4]{c}$.

⌟

Proof: Cf.[D-P98]P300.? □

Then it follows from(15.3.4.7) and Baker's theory(14.7.1.11) that if $v_{2m} = w_{2n}$, then

$$\frac{3}{2}m \log c < 3.822 \cdot 10^{15} \cdot 0.33 \log c \cdot 0.38 \log c \cdot 0.64 \log c \cdot \log(2m),$$

thus

$$\frac{m}{\log(2m)} < 2.045 \cdot 10^{14} (\log c)^2.$$

Combining(15.3.4.8), we get

$$m < 2.045 \cdot 10^{14} \log(2m)[\log(91m^2)]^2,$$

which implies $m < 9 \cdot 10^{19}$ and so $c < 8 \cdot 10^{41}$ and $k \leq 36$.

Similarly, if $v_{2m+1} = w_{2n+1}$, then

$$2m \log c < 3.822 \cdot 10^{15} \cdot 0.33 \log c \cdot 0.38 \log c \cdot 0.73 \log c \cdot \log(2m+1),$$

thus

$$\frac{m}{\log(2m+1)} < 1.75 \cdot 10^{14} (\log c)^2.$$

Combining(15.3.4.8), we get

$$m < 1.75 \cdot 10^{14} \log(2m+1)[\log(1689m^4)]^2,$$

which implies $m < 4 \cdot 10^{20}$ and so $c < 5 \cdot 10^{85}$ and $k \leq 75$.

So to complete the proof, it suffices to show that:

Lemma (15.3.4.9).

- For $k \leq 36$, the equation $v_{2m} = w_{2n}$ with $0 \leq n \leq m < 9 \cdot 10^{19}$ has only one solution $m = n = 0$.
- For $k \leq 75$, the equation $v_{2m+1} = w_{2n+1}$ with $0 \leq n \leq m < 4 \cdot 10^{20}$ has only one solution $m = n = 0$(in which case $z = 2c \pm st$, corresponding to $d = c_{k\pm 1}$, in view of(15.3.4.3)). ⌟

Proof: Use(15.2.4.7) twice, wich $M = 9 \cdot 10^{19}$ and $M = 9$. Cf.[D-P98]P303. □
□

Thm. (15.3.4.10) [Bo-Alain-Volker]. There are no Diophantine sequences of length 5. ⌟

Proof: Cf.[There is no Diophantine quintuple. (English summary) Trans. Amer. Math. Soc. 371 (2019), no. 9, 6665–6709.] □

Waring's Problem

Def. (15.3.4.11) [Waring's Problem]. For $k \geq 1$, let $g(k) \in \mathbb{Z}_+$ be the smallest number s.t. every positive integer is a sum of at most $g(k)$ positive k-th powers. ⌟

Prop. (15.3.4.12). Situation as in(15.3.4.11), $g(k) \geq \lfloor 2^k \rfloor + \lfloor (\frac{3}{2})^k \rfloor - 2$. ⌟

Proof: This is because the number $\lfloor (\frac{3}{2})^k \rfloor 2^k - 1$ requires $\lfloor (\frac{3}{2})^k \rfloor - 1$ powers 2^k and $2^k - 1$ powers 1^k. □

Prop. (15.3.4.13) [Dickson-Niven-Pillai-Rubugunday]. Situation as in(15.3.4.11),

$$g(k) = \begin{cases} 2^k + \lfloor (\frac{3}{2})^k \rfloor - 2, & \lceil (\frac{3}{2})^k \rceil - (\frac{3}{2})^k \geq (\frac{3}{4})^k \\ ?, & \text{otherwise} \end{cases}.$$

In particular, $g(1) = 1, g(2) = 4, g(3) = 9, g(4) = 19$. ⌟

Proof: ? □

Conj. (15.3.4.14) [Mahler]. Situation as in(15.3.4.11), $g(k) = 2^k + \lfloor (\frac{3}{2})^k \rfloor - 2$ any k. ⌟

Proof: □

Thm& Conj.Cor. (15.3.4.15). By(15.2.5.11), this is true for k sufficiently large. But it is not known for how large k this is true, eventually due to the ineffectiveness of the proof of Roth's theorem(15.2.3.7). ⌟

Siegel's Theorem

References are [C-Z02] and [Sie35].

Thm. (15.3.4.16) [Siegel]. If $F \in$ `NField` and $C/F \subset \mathbb{A}^n_F$ is an affine curve with normalization C_{sm}, and let $\overline{C}$ be the completion of C_{sm}. Suppose $g(\overline{C}) > 0$ or $\#\widetilde{C} \backslash C_{\mathrm{sm}} \geq 3$, then for any $\Sigma^\infty_F \subset_{\mathrm{fin}} S \subset \Sigma_F$, $\#C(\mathcal{O}_{F,S}) < \infty$. ⌟

Proof: Firstly, it suffices to prove for C smooth: As the normalization is finite and birational(6.4.2.7), by omitting f.m. points, we may assume that all rational points of C lift to rational points of C. Moreover, if $\Gamma(C_{\mathrm{sm}}) = \Gamma(C)[f_1, \ldots, f_r]$, where f_i are integral over C_{sm}. We can enlarge S s.t. C has an integral model over $\mathcal{O}_{F,S}$, and each f_i is integral over $\Gamma(C/\mathcal{O}_{F,S})$. Then each $\mathcal{O}_{F,S}$-points of C lifts to C_{sm}, and the assertion reduces to C_{sm}.

For $g(\overline{C}) \geq 2$, this is a special case of Faltings' Theorem(15.14.8.2).

For $g = 1$, the assertion follows from(15.11.7.2).

For $g = 0$, then $\#\widetilde{C} \setminus C_{\mathrm{sm}} \geq 3$(in fact, any other cases can be reduced to the case $\#\widetilde{C} \setminus C_{\mathrm{sm}} \geq 3$, Cf.[B-G06]P184.) Then ?

□

abc-Conjecture

Conj. (15.3.4.17) [Strong *abc*-Conjecture, Masser-Oesterlé1985]. Given $F \in$ `NField`, for any $\varepsilon > 0$, there is a constant C_ε that for any $a, b, c \in \mathcal{O}_F$ that $a + b = c$,

$$H_F([a, b, c]) \leq C_\varepsilon |\operatorname{Nm}_{K/\mathbb{Q}}(\prod_{\mathfrak{p}|abc} \mathfrak{p})|^{1+\varepsilon}.$$

⌟

Proof: □

5 Ternary Diophantine Equations

Def. (15.3.5.1) [Ternary Diophantine Equations]. A **ternary diophantine equation** is a Diophantine equation of the form

$$\{x, y, z \in \mathbb{Z} | Ax^p + By^q = Cz^r\}$$

where $A, B, C \in \mathbb{Z}^\times$. A **non-trivial solution** is a solution that $xyz \neq 0$. A **primitive solution** is a solution s.t. $\gcd(x, y, z) = 1$. ⌟

Prop. (15.3.5.2) [Pythagorean Triples]. A triple $(x, y, z) \in \mathbb{Z}^3$ s.t. $\gcd(x, y, z) = 1$ and $x^2 + y^2 = z^2$ is called a **Pythagorean triple**. Then for any $a > b \in \mathbb{Z}_+$ s.t. $\gcd(a, b) = 1$ and $a \not\equiv b \pmod 2$,

$$(x, y, z) = (a^2 - b^2, 2ab, a^2 + b^2)$$

is a Pythagorean triple. Conversely, any Pythagorean triple is of this form(after possibly switching x and y). ⌟

Proof: It is easy to verify that $(a^2 - b^2, 2ab, a^2 + b^2)$ is a Pythagorean triple. Conversely, for a Pythagorean triple (x, y, z), we may assume $y \neq 2$, and $y^2 = (z-x)(z+x)$. Notice $\gcd(z-x, z+x)|2$, but $2 \nmid y$, so $\gcd(z - x, z + x) = 1$. Thus there exists $r, s \in \mathbb{Z}_+$ s.t.

$$z + x = r^2, z - x = s^2.$$

Then $r \equiv s \pmod 2$. Denote $a = \frac{r+s}{2}, b = \frac{r-s}{2} \in \mathbb{Z}$, then $z = \frac{r^2+s^2}{2} = a^2 + b^2, x = \frac{r^2-s^2}{2} = 2ab$, and $y = rs = a^2 - b^2$. □

Def. (15.3.5.3) [Frey's Curve]. Let $a, b, c \in \mathbb{Z}$ satisfy $a^p + b^p = c^p, p \geq 3 \in \mathbf{P}, abc \neq 0$, the **Frey curve** for a, b, c is the elliptic curve $E_{a^p,b^p,c^p} \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ define by the Weierstrass equation

$$W_{a^p,b^p,c^p} : y^2 = x(x + a^p)(x - b^p).$$

Then it satisfies:

- $\mathfrak{D}_{W_{a^p,b^p,c^p}} = 16a^{2p}b^{2p}(a^p + b^p)^2 = 16(abc)^{2p}$.
- $\Delta^{\min}_{E_{a^p,b^p,c^p}/\mathbb{Q}}$ satisfies $\Delta^{\min}_{a^p,b^p,c^p} \geq \frac{|abc|^{2p}}{2^8}$ by(15.11.4.25).

⌟

Prop. (15.3.5.4) [Galois Representation of Frey's Curve]. Let $\rho_{a^p,b^p,c^p} : \mathrm{Gal}_\mathbb{Q} \to \mathrm{GL}(2, \mathbb{F}_p)$ be the mod p Galois representation of $\mathrm{Gal}_\mathbb{Q}$ corresponding to the Frey's curve E_{a^p,b^p,c^p}(15.3.5.3), and let $\overline{\rho}_{a^p,b^p,c^p}$ be its reduction modulo p. Suppose that $a \equiv -1 \pmod 4$ and $2|b$, then

- $\overline{\rho}_{a^p,b^p,c^p}$ is absolutely irreducible.
- $\overline{\rho}_{a^p,b^p,c^p}$ is odd.
- $\overline{\rho}_{a^p,b^p,c^p}$ is unramified outside $2p$, flat at p, and semistable at 2**?**.

⌟

Proof: **?** Cf.[Serre, Galois representations arising from Modular Forms]Section4.1.. □

Remark (15.3.5.5). One suspects that such a Galois representation doesn't even exist. ⌟

Thm. (15.3.5.6) [Fermat's Last Theorem, Ribet/Wiles-Taylor]. If $p \geq 5 \in \mathbf{P}$, then there are no integral solution to the equation $a^p + b^p = c^p$. ⌟

Proof: If there exists an integral solution s.t. $abc \neq 0$, consider the Frey's curve E_{a^p,b^p,c^p}(15.3.5.3), then by(15.3.5.4), $\overline{\rho}_{a^p,b^p,c^p}$ is absolutely irreducible, odd and unramified outside $2p$, and flat at p.

Then it follows from modularity conjecture(19.4.2.6) that ρ_{a^p,b^p,c^p} is attached to some newform $f \in S_2(\Gamma_0(2p))$. Then it follows from Ribet's theorem(20.9.1.7) that $\overline{\rho}_{a^p,b^p,c^p} = \overline{\rho}_{g,p}$ for some newform $g \in S_2(\Gamma_0(2))$. But there is no cuspidal form of level $\Gamma_0(2)$ and weight 2 because $X_0(2) = \mathbb{P}^1$, and $H^0(\mathbb{P}^1, \Omega^1_{\mathbb{P}^1}) = 0$, contradiction. □

Remark (15.3.5.7) [Szpiro's Conjecture and Fermat's Last Theorem]. The Szpiro's conjecture(15.7.12.17) implies Fermat's last theorem for sufficiently large n(depending on the effectiveness of Szpiro's conjecture). ⌟

Proof: Let $a, b, c \in \mathbb{Z}$ satisfy $a^n + b^n = c^n, n \geq 2, abc \neq 0$, the conductor $N_{a,b,c}$ of the Frey's curve(15.3.5.3) $E_{a,b,c}$ satisfies $N_{a,b,c} \leq 2^8(abc)$ by(15.11.4.25). Szpiro's conjecture implies

$$\frac{|abc|^{2n}}{2^8} \leq |\Delta^{\min}_{a,b,c}| \leq \kappa_1 N_E^7 \leq 2^{56}\kappa_1|abc|^7,$$

so $|abc|^{2n-7} \leq 2^{64}\kappa$. As $|abc| \geq 2$, this gives an upper bound for n. □

Prop. (15.3.5.8) [Fermat's Equation in Function Case]. If $n \geq 2$, then any non-trivial solutions to the equation in $\mathbb{C}[T]$ of

$$X^n + Y^n = Z^n$$

are of the form $n = 2, X = (a^2 - b^2)/2, Y = ab, Z = (a^2 + b^2)/2$, where $a, b, c \in \mathbb{C}[T]$. ⌟

Proof: The $n = 2$ case is easy. If $n > 2$, we show there are no non-trivial solutions: Differentiate it to get:

$$X^{n-1}X' + Y^{n-1}Y' = Z^{n-1}Z',$$

And cancelling X^{n-1}, we get

$$Y^{n-1}(X'Y - Y'X) = Z^{n-1}(X'Z - Z'X).$$

Now $X'Z - Z'X \neq 0$ because X, Z are not linearly equivalent, and Y, Z is coprime, so $Y^{n-1} | X'Z - Z'X$. But then if we assume $\dim Y \geq \dim X$, then $(n-1)\dim Y \leq 2\dim Y - 1$, which implies $n \leq 2$, contradiction. □

Prop. (15.3.5.9) [Darmon].

- For $n \in \mathbb{Z}_{\geq 3}$, the equation $\{x, y, z \in \mathbb{Z} | x^n + y^n = 2z^n\}$ has no non-trivial primitive solution.
- For $n \in \mathbb{Z}_{\geq 4}$, the equation $\{x, y, z \in \mathbb{Z} | x^n + y^n = z^2\}$ has no non-trivial primitive solution.
- For $n \in \mathbb{Z}_{\geq 3}$, the equation $\{x, y, z \in \mathbb{Z} | x^n + y^n = z^3\}$ has no non-trivial primitive solution.

⌟

Proof:

2: The case $n = 4$ is proved by Fermat. The case $n = 5, 6, 9$ is proved by [Poonen, Some diophantine equations of the form]. Thus it suffices to prove the case $n = p \in \mathbf{P}_{\geq 7}$. If $2|ab$, assume $2|a$, and $c \equiv 1 (\mathrm{mod}\ 4)$. And if $2 \nmid ab$, by replacing c with $-c$ if necessary, we can assume $a \equiv -1 (\mathrm{mod}\ 4)$. Then consider the Frey curve $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ given by the Weierstrass equation

The case $n = 4$ is proved by Lucas [Theory of Numbers, Dickson]P630. The case $n = 5$ is proved by [Poonen, Some diophantine equation of the form]. □

Prop. (15.3.5.10) [Darmon]. For $p \in \mathbf{P}_{\geq 11}$, the ternary Diophantine equation

$$\{x, y, z \in \mathbb{Z} | x^4 - y^4 = z^p\}$$

has no non-trivial primitive solution s.t. $z \in 2\mathbb{Z}$. And it has no non-trivial primitive solution if $p \equiv 1 (\mathrm{mod}\ 4)$. ⌟

Proof: Let (a, b, c) be a solution of this equation. If c is odd, we can assume a is odd and b is even(otherwise change c to $-c$). Then $a - b, a + b, a^2 + b^2$ are all p-th powers up to powers of 2. Consider the Frey curve $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ given by the Weierstrass equation

$$W : y^2 = x(x + (a + b)^2)(x - (a - b)^2) = x^3 + 4abx^2 - (a^2 - b^2)^2 x.$$

Then

$$j(E) = 2^6 \frac{(a^2 + 3b^2)^3 (3a^2 + b^2)^3}{c^{2p}(a^2 - b^2)^3}, \mathfrak{D} = 2^6 c^{2p} (a^2 - b^2)^2.$$

Then the conductor N_E of E can be calculated by Tate's algorithm**?**.

$$\mathrm{ord}_p(N_E) = \begin{cases} 1 & , p | c \\ 0 & , p \neq 2, p \nmid c \\ 5 & , p = 2, 2 \nmid c \end{cases}.$$

By a result of Mazur**?**, $\overline{\rho}_{E,2}$ is irreducible, and by [Serre, Sur les repr´esentations modulaires de degre 2 de Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$], ρ is unramified outside $2p$, and is finite at p. □

6 Unlikely Intersections

Def. (15.3.6.1) [Unlikely Intersections]. Let $S \in \mathcal{V}\mathrm{ar}^{\mathrm{sm}}/k$, and X, Y be irreducible subvarieties of S. Then an **atypical component** of $X \cap Y$ is a connected component $T \subset X \cap Y$ s.t. $\dim T > \dim X + \dim Y - \dim S$. ⌟

Conj. (15.3.6.2) [Zilber Conjecture on Intersecting with Tori]. Let $g \in \mathbb{Z}_+, S = \mathbb{G}_{m,\mathbb{C}}^g$. For any irreducible subvariety $X \subset S$, denote $X^{\mathrm{atyp}} \subset X$ to be the union of atypical components of $X \cap T$ where $T \subset S$ is an algebraic group. Then X^{atyp} is Zariski-closed. Equivalently, if X is not contained in a proper subvariety of S, then $X^{\mathrm{atyp}} \subset X$ is not Zariski dense in X. ⌟

Proof: □

Remark (15.3.6.3). Zilber's conjecture over $\overline{\mathbb{Q}}$ is equivalent to Zilber's conjecture over $\mathbb{C}$.**?**

⌟

Pila's Work

References are [P-W06].

Def. (15.3.6.4) [Algebraic and Transcendental Parts]. For $n \in \mathbb{Z}_+, X \subset \mathbb{R}^n$, the **algebraic part of** X is defined to be the union of all semi-algebraic subset of $\mathbb{R}^n$ contained in X, denoted by X^{alg}. And the **transcendental part** of X is defined to be $X^{\mathrm{trans}} = X \setminus X^{\mathrm{alg}}$. ⌟

Prop. (15.3.6.5)[Bombieri-Pila]. Let $f \in C([0,1])$ be a non-algebraic real-analytic function, then for any $\varepsilon \in \mathbb{R}_+$, there exists $C(f,\varepsilon) \in \mathbb{R}_+$ s.t.

$$\#\{x \in \Gamma(f) \cap \mathbb{Q}^2 | H(x) \leq H\} \leq C(f,\varepsilon)H^\varepsilon.$$

⌟

Proof: Cf.[P-W06]**?** □

Thm. (15.3.6.6)[Pila-Wilkie]. Let $X \subset \mathbb{R}^n$ be o-minimal definable, then for any $\varepsilon \in \mathbb{R}_+$, there exists $C(X,\varepsilon) \in \mathbb{R}_+$ s.t.

$$\#\{x \in X \cap \mathbb{Q}^2 | H(x) \leq H\} \leq C(X,\varepsilon)H^\varepsilon.$$

⌟

15.4 Arithmetic of Algebraic Groups

Main references are [Algebraic Groups and Number Theory], [Mil17b].

Notation (15.4.0.1).
- Use notations from Group Schemes I: Structure Theory.
- Use notations from p-adic Analysis.

⌟

1 over p-adic Number Fields

Notation (15.4.1.1).
- Let $(K, \mathcal{O}_K, k) \in p$-`NField`.

⌟

Prop. (15.4.1.2). If $G \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}} / \mathcal{O}_F$, then $G(\mathcal{O}_F)$ is compact. ⌟

Prop. (15.4.1.3). If G is a reductive group over K, then $\mathcal{G}(\mathcal{O}_K)$ is a maximal compact subgroup of $G(K)$. ⌟

Proof:

Prop. (15.4.1.4) [Reductive Groups are Unimodular]. If G/K is a reductive group, then $G(K)$ is unimodular. ⌟

Proof: □

□

Cor. (15.4.1.5). $GL(n, \mathcal{O}_F)$ is a maximal compact subgroup of $GL(n, F)$, and any compact subgroup of $GL(n, F)$ is conjugate to $GL(n, \mathcal{O}_F)$. ⌟

Proof: $GL(n, \mathcal{O}_F)$ is compact by(15.4.1.2).

For maximality, for any compact subgroup Γ, consider the standard representation of $\mathrm{GL}(n)$, it suffices to find an $\mathcal{O}_L$-lattice that is stable under Γ-action. Notice $\rho(\Gamma) \cap GL(n, \mathcal{O}_{L'})$ is open in $\rho(\Gamma)$, thus is of finite index, so $\Gamma(\mathcal{O}_L^n)$ is a lattice that is stable under Γ(14.2.3.34). □

Prop. (15.4.1.6). $SL(n, \mathbb{Q}_p)$ has two maximal subgroups

$$SL(n, \mathbb{Z}_p), \quad \begin{bmatrix} p & \\ & 1 \end{bmatrix}^{-1} SL(n, \mathbb{Z}_p) \begin{bmatrix} p & \\ & 1 \end{bmatrix}$$

up to conjugacy. ⌟

Proof: □

2 over Global Fields

Def. (15.4.2.1) [Groups of Non-Compact Types]. Let $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp} / \mathbb{Q}$ be semisimple, then G is said to be a **group of compact type** if $G(\mathbb{R})$ is compact, and said to be a group of non-compact type if it doesn't contain a non-trivial normal subgroup of compact type. ⌟

Prop. (15.4.2.2) [Real Approximation]. If $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp} / \mathbb{Q}$ satisfies each connected components of G contains a rational point, then $G(\mathbb{Q})$ is dense in $G(\mathbb{R})$. ⌟

Proof: Cf.[Mil17]P54. □

Congruence Subgroups

Def. (15.4.2.3) [Congruence Subgroups]. Let $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/\mathbb{Q}$ with an embedding $G \to \mathrm{GL}(n)_{\mathbb{Q}}$, for $N \in \mathbb{Z}_+$, define $\Gamma(N) = G(\mathbb{Q}) \cap \{g \in \mathrm{GL}(n;\mathbb{Z}) | g \equiv \mathbb{1} (\mathrm{mod}\ \ GL(n;N))\}$, and a **congruence subgroup** of $G(\mathbb{Q})$ is any subgroup of $G(\mathbb{Q})$ that contains some $\Gamma(N)$ as a finite index subgroup.

The notion is compatible with that defined in(15.4.3.13). In particular, the set of congruence subgroups of G doesn't depend on the embedding**?**. ⌟

Prop. (15.4.2.4) [Congruence Subgroup Problem]. Let G be a reductive group over $\mathbb{Q}$,

- If G is split simply connected other than SL(2), then every arithmetic subgroup of G is a congruence subgroup.
- If $G = \mathrm{SL}(2)$ or non-simply connected, there are many arithmetic subgroups of G that is not congruence subgroups.

⌟

Proof: Cf.[MATSUMOTO 1969. Sur les sous-groupes arithmétiques des groupes semi-simples de ´ploye´s. Ann. Sci. Ecole Norm. Sup. (4) 2:1 – 62.].[SURY, B. 2003. The congruence subgroup problem, volume 24 of Texts and Readings in Mathematics. Hindustan Book Agency, New Delhi.] □

Prop. (15.4.2.5). The image of a congruence subgroup may not be a congruence subgroup. ⌟

Proof:

□

Prop. (15.4.2.6) [Minkowski]. The congruence subgroup $1 + pGL(n;\mathbb{Z})$ is torsion-free for $p \in \mathbf{P} \setminus \{2\}$. ⌟

Proof: Cf.[P-R94]P232. □

3 over Adeles

Notation (15.4.3.1).

- In this subsection, let $F \in$ `GField` and $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/F$.

⌟

Def. (15.4.3.2) [Adele Groups]. Let $G \subset \mathrm{GL}(V) \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/F$, where $V \in \mathcal{V}\mathrm{ect}_F$, $G(\mathbf{A}_F)$ is called the **group of Adele points of** G. Let Λ be a $\mathcal{O}_F$-lattice of V, for any place $v \in \Sigma_F^{\mathrm{fin}}$, let K_v be the stabilizer of $\Lambda_v = \Lambda \otimes_{\mathcal{O}_F} \mathcal{O}_v$ in $G(F_v)$, then $\mathcal{K}_v$ are compact open subgroups of $G(F_v)$. Define the **adelic group of** G

$$G(A_F) = \prod_v{}' (G(F_v), \mathcal{K}_v),$$

which is a locally compact topological group. These K_v are called **hyperspecial compact subgroups**, and they are maximal subgroups of $G(\mathcal{K}_v)$ for a.e. v if G is reductive(15.4.1.3). We can modify the remaining v s.t. $\mathcal{K}_v$ are special maximal compact subgroups**?**, and denote

$$\mathcal{K} = \mathcal{K}^f \mathcal{K}_\infty, \quad \mathcal{K}^f = \prod_{v \in \Sigma_F^{\mathrm{fin}}} \mathcal{K}_v, \quad \mathcal{K}_\infty = \prod_{v \in \Sigma_F^{\infty}} \mathcal{K}_v.$$

⌟

Proof: To show $G(\mathbf{A}_F)$ is independent of Λ, notice $|G(\mathbf{A}_F)|$ is clearly invariant, and if Λ' is another lattice, then $d^{-1}\Lambda \subset \lambda' \subset d\Lambda$ for some $d \in \mathbb{Z}_+$, so $\mathcal{K}_v$ are the same for $v \nmid d$.

$\mathcal{K}_v$ are compact open subgroups of $G(F_v)$ because they are the intersection of $GL(\Lambda_v) \cong GL(n, \mathcal{O}_v)$ with $G(F_v)$. To show they are maximal, for any other compact subgroup $\mathcal{K}'$ of $G(F_v)$, as $\mathcal{K}_v \cap \mathcal{K}$ is open, $\mathcal{K}'/K' \cap \mathcal{K}_v$ is a finite set, thus **?** □

Cor. (15.4.3.3). $G(\mathbf{A}_F) = G(\mathbf{A}_{F,S}) \times G(\mathbf{A}_F^S)$. ⌟

Prop. (15.4.3.4). For a closed embedding of algebraic groups $G \subset G' \in \mathcal{A}lg\mathcal{G}rp/F$, the inclusion $G(\mathbf{A}_F) \subset G'(\mathbf{A}_F)$ is a closed embedding. But for open immersions, the induced inclusion may not be immersions. For example, the embedding $\mathbb{G}_m \subset \mathbb{A}^1$ doesn't induce immersion $\mathbf{I}_F \subset \mathbf{A}_F$. ⌟

Proof: **?** □

Example (15.4.3.5) [GL(n)]. Fix the following compact subgroup of $GL(n, A)$:

$$\mathcal{K} = \prod \mathcal{K}_v, \quad \mathcal{K}_v = \begin{cases} O(n) & v \text{ real} \\ U(n) & v \text{ complex} \\ GL(n, \mathcal{O}_v) & v \text{ non-Archimedean} \end{cases}.$$

then $\mathcal{K}$ is the maximal compact subgroup of $GL(n, \mathbf{A}_F)$ in the sense that any compact subgroup can conjugate into K.

$\mathfrak{gl}_{n,\infty} = \prod_{v \in S_\infty} \mathfrak{gl}(n, F_v)$, then we can define $(\mathfrak{gl}_{n,\infty}, \mathcal{K}_\infty)$-modules. ⌟

Prop. (15.4.3.6). $GL(F)$ is discrete in $GL(A_F)$. ⌟

Proof: □

Prop. (15.4.3.7) [Fundamental Domain]. $GL(F)\backslash GL(\mathbf{A}_F)$ has a fundamental domain which can be covered by a sufficiently large **Siegel sets** $\mathfrak{S}_{c,d}$. ⌟

Proof: □

Prop. (15.4.3.8). $GL(F)\backslash GL(A_F)$ has finite volume if G is semisimple, and it is compact if G is anisotropic. ⌟

Proof: □

Def. (15.4.3.9) [Strong Approximation Property]. Let S be a finite set of places containing Σ_F^∞, a group G is said to satisfy the **strong approximation** for S if it satisfies the following equivalent conditions:

- The image of $G(F)$ is dense in $G(\mathbf{A}^S)$,
- $G(F)G(\mathbf{A}_S)$ is dense in $G(\mathbf{A})$.
- For any compact open subgroup $U^S \subset G(\mathbf{A}^S)$, $G(A) = G(F)G(A_S)U^S$.

In particular,

$$\Gamma\backslash G(\mathbf{A}_S) \cong G(F)\backslash G(\mathbf{A})/U^S.$$

where Γ is the image of $G(F) \cap (G(\mathbf{A}_S) \times U^S)$ in $G(\mathbf{A}_S)$. ⌟

Thm. (15.4.3.10) [Strong Approximation]. Assume G is a simply-connected semisimple group(9.3.2.1) and $G(A_S)$ is non-compact for some finite subset $\Sigma_F^\infty \subset S \subset \Sigma_F$, then G satisfies strong approximation for S. ⌟

Proof: Cf.[Algebraic Groups and Number Theory, P427]. □

Remark (15.4.3.11). This is not true for non-semisimple or non-simply connected: for $\mathbb{G}_m$, $\mathbb{Q}^\times$ is not dense in $\mathbb{A}_{\mathbb{Q},f}^\times$.

For PGL(2), the determinant of $PGL(2,\mathbb{Q})$ is $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ and the determinant of $PGL(2,\mathbb{A}_{\mathbb{Q},f})$ is $\mathbb{A}_{\mathbb{Q},f}^\times/(\mathbb{A}_{\mathbb{Q},f}^\times)^2$, which is not dense. ⌟

Cor. (15.4.3.12) [Strong Approximation for SL(n)]. Let $F\in$ `NField`, then

- $\mathrm{SL}(n)_F$ satisfies strong approximation for Σ_F^∞.
- Let K_0 be an open compact subgroup of $GL(n,\mathbf{A}^f)$, then
$$GL(n,F)GL(n,A_\infty)K_0T_1(A)=GL(n,A).$$
- Let K_0 be an open compact subgroup of $GL(n,\mathbf{A}^f)$ that the image of K_0 under the determinant map is $\prod_{v\in\Sigma_F^{\mathrm{fin}}}\mathcal{O}_v^*$, then
$$\det: GL(n,F)GL(n,\mathbf{A}_\infty)\backslash GL(n,\mathbf{A}_F)/K_0\to F^\times\,\mathbf{I}_{F,\infty}\backslash I_F/\prod_{v\in\Sigma_F^{\mathrm{fin}}}\mathcal{O}_v^*=\mathrm{Cl}_1(F)$$
is an isomorphism.

⌟

Proof: 1 is a direct consequence of(15.4.3.10).

2 is a direct consequence of 1.

3: det is clearly surjective. To show it is injective, if $\det(a)=\det(b)\in\mathrm{Cl}_1(F)$, then $\det(a)=\det(g_1g_\infty bk_0)$ where $g_1\in GL(n,F),g_\infty\in GL(n,A_{F,\infty}),k_0\in GL(n,A_F^f)$ by hypothesis. Then $g_1g_\infty bk_0a^{-1}\in SL(n,\mathbf{A}_F)$, and by item1 it is of the form $h_1h_\infty k_0$ where $h_1\in SL(n,F),h_\infty\in SL(n,A_{F,\infty}),k_1\in a(K_0\cap SL(n,\mathbf{A}_F^f))a^{-1}$. Then the assertion follows. □

Prop. (15.4.3.13) [Passage From Archimedean to Adele via Congruence Subgroups]. If $F\in$ `GField`, $U_\Gamma\subset G(\mathbf{A}_F^f)$ a compact open subgroup and Γ the image of $G(F)\cap(G(A_\infty)\times U_\Gamma)$ in $G(A_\infty)$, called a **congruence subgroup** of G. If G satisfies strong approximation for $S=\Sigma_F^\infty$(15.4.3.9), then
$$\Gamma\backslash G(A_\infty)\cong G(F)\backslash G(A)/U_\Gamma.$$

In general, for any open compact subgroup $U\subset G(A_f)$,
$$\#G(F)\backslash G(A)/G(A_\infty)U<\infty.$$

Thus if $\{g_i\}\subset G(A_f)$ is a set of double coset representatives,
$$G(F)\backslash G(A)/U=\coprod_i\Gamma_i\backslash G(A_\infty)$$
where Γ_i is the image of $(g_iUg_i^{-1}\times G(A_\infty))\cap G(F)$ in $G(A_\infty)$. Thus the passage from Archimedean to adele is not seriously affected by the lack of strong approximation. ⌟

Proof: The double coset is finite because for any $(g_v)\in G(A_F^f)$, by strong approximation for $\mathbb{G}_a$, we can choose a $g\in G(F)$ s.t. $g^{-1}g_v\in K_v$ for any $v\in\Sigma_F^{\mathrm{fin}}$, then the image is finite as U is compact open and $\prod_v K_v$ is compact. □

4 Integral Models

Groups over $\mathbb{Z}$

References are [Groups over $\mathbb{Z}$, Gross].

15.5 Arithmetic Subgroups

Main references are [Mor15] and [V. Platonov and A. Rapinchuk: Algebraic Groups and Number Theory.]

1 Arithmetic Subgroups

Def. (15.5.1.1) [Arithmetic Subgroups]. For $G \in \mathcal{L}\mathrm{in}\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/\mathbb{Q}$, an **arithmetic subgroup** $\Gamma \leq G(\mathbb{Q})$ is a subgroup that is commensurable with $G(\mathbb{Q}) \cap GL(n, \mathbb{Z})$ for some embedding $G \hookrightarrow \mathrm{GL}(n)_{\mathbb{Q}}$. This notion is independent of the embedding chosen.

If $G \subset \mathrm{GL}(V)$ and $L \subset V$ be a lattice, then the arithmetic subgroup $G(\mathbb{Q}) \cap GL(n, \mathbb{Z})$ is also denoted by $G(\mathbb{Z}; L)$, called the **group of units of** G. If no confusion is make, it is also denoted by $G(\mathbb{Z})$. ⌟

Proof: Cf.[?]P171. □

Lemma (15.5.1.2) [Invariance of Arithmetic Subgroups]. For $\varphi : G \to G' \in \mathcal{L}\mathrm{in}\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/\mathbb{Q}$, the kernel of an arithmetic subgroup is an arithmetic subgroup. ⌟

Proof: □

Cor. (15.5.1.3). If $G = H \ltimes N \subset \mathrm{GL}(V) \in \mathcal{L}\mathrm{in}\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/\mathbb{Q}$, then $H(\mathbb{Z}) \ltimes N(\mathbb{Z}) \subset G(\mathbb{Z})$ has finite index. ⌟

Proof: Let $\mathrm{pr} : G \to H$ be the projection, then $H(\mathbb{Z}) \ltimes N(\mathbb{Z}) = \mathrm{pr}^{-1}(H(\mathbb{Z}))$. □

Prop. (15.5.1.4). If $\varphi : G \to G' \in \mathcal{L}\mathrm{in}\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/\mathbb{Q}$ is surjective, then φ maps an arithmetic subgroup to an arithmetic subgroup. ⌟

Proof: ? □

Prop. (15.5.1.5). There exists arithmetic subgroups not of the form $G(\mathbb{Z}; L)$. ⌟

Proof: ? By the proof of(15.5.1.2), any $G^L_{\mathbb{Z}}$ must contain some congruence subgroup $G_{\mathbb{Z}}(d)$, but there are examples of subgroups of finite index of $SL(2, \mathbb{Z})$ not of this form, Cf.[?]Chap9.5. □

Prop. (15.5.1.6). Let $G \in \mathcal{L}\mathrm{in}\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/\mathbb{Q}$ and Γ be an arithmetic subgroup, then for any f.d. representation $\rho \in \mathrm{Rep}^{\mathrm{fd}}_{\mathbb{Q}}(G)$, there exists a Γ-invariant lattice. ⌟

Proof: Cf.[?]P173. □

Reduction Theory

Prop. (15.5.1.7). Let $G \in \mathcal{L}\mathrm{in}\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/\mathbb{Q}$ and Γ be an arithmetic subgroup, then Γ is finitely presented. ⌟

Proof: ? □

Prop. (15.5.1.8). Let $G \in \mathcal{L}\mathrm{in}\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/\mathbb{Q}$, then there exists only f.m. conjugacy classes of finite subgroups of $G_{\mathbb{Z}}$. ⌟

Proof: ? □

Thm. (15.5.1.9) [Borel Density Theorem]. Let $G \in \mathcal{L}\mathrm{in}\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/\mathbb{Q}$ be semisimple of non-compact type, then any arithmetic subgroup Γ is Zariski-dense in G. ⌟

Proof: Cf.[?]P205.? □

Compactness of $G(\mathbb{R})/G(\mathbb{Z})$

Prop. (15.5.1.10). Let $S \in \mathcal{L}in\mathcal{A}lg\mathcal{G}rp/\mathbb{Q}$ be a torus, then the following are equivalent:

- S is $\mathbb{Q}$-anisotropic.
- $S(\mathbb{R})/S(\mathbb{Z})$ is compact.

⌟

Proof: Cf.[?]P205.? □

Prop. (15.5.1.11). Let $G \in \mathcal{L}in\mathcal{A}lg\mathcal{G}rp/\mathbb{Q}$, then the following conditions are equivalent:

- $G(\mathbb{R})/G(\mathbb{Z})$ is compact.
- The reductive part of G^0 is anisotropic over $\mathbb{Q}$.

⌟

Proof: Cf.[?]P210.? □

Prop. (15.5.1.12) [Mahler's Criterion]. A subset $\Omega \subset GL(n;\mathbb{R})$ is compact modulo $GL(n;\mathbb{Z})$ iff it satisfies:

- $\{\det(g)|g \in \Omega\}$ is bounded.
- $[\Omega.(\mathbb{Z}^n \setminus \{0\})] \cap U = \varnothing$ for some nbhd U of $0 \in \mathbb{R}^n$.

⌟

Proof: Cf.[?]P211.? □

Finiteness of the Volume of $G(\mathbb{R})/G(\mathbb{Z})$

Prop. (15.5.1.13). For $G \in \mathcal{L}in\mathcal{A}lg\mathcal{G}rp/\mathbb{Q}$, $G(\mathbb{R})/G(\mathbb{Z})$ has finite volume iff G^0 doesn't have non-trivial characters defined over $\mathbb{Q}$. ⌟

Proof: Cf.[?]P213. □

Prop. (15.5.1.14). If $G \in \mathcal{L}in\mathcal{A}lg\mathcal{G}rp/\mathbb{Q}$ is semisimple, and Γ is an arithmetic subgroup, then $G(\mathbb{R})/\Gamma$ has finite volume. ⌟

Proof: Cf.[?]P220. □

Finite Arithmetic Groups

Conj. (15.5.1.15). If $G \subset \mathrm{GL}(n)_{\mathbb{Q}} \in \mathcal{A}lg\mathcal{G}rp/\mathbb{Q}$ is of compact-type, then for any totally real extension $F/\mathbb{Q}$, $G(\mathcal{O}_F) = G(\mathbb{Z})$. ⌟

Proof: □

Remark (15.5.1.16). By(15.5.1.17), it suffices to prove this conjecture for $\mathrm{O}(V)$ for any inner space $V/\mathbb{Q}$. ⌟

Prop. (15.5.1.17). If $G \subset \mathrm{GL}(n) \in \mathcal{A}lg\mathcal{G}rp/\mathbb{Q}$ satisfies $G(\mathbb{R})$ is compact and Zariski dense in G, then G preserves a quadratic definite quadratic form f. ⌟

Proof: Cf.[?]P230. □

Prop. (15.5.1.18) [Bartels-Kitaoka]. Let $F/\mathbb{Q}$ be a totally real nilpotent Galois extension, and $\Gamma \leq \mathrm{GL}(n;\mathcal{O})$ is a finite $\mathrm{Gal}(F/\mathbb{Q})$-invariant subgroup, then $\Gamma \subset \mathrm{GL}(n;\mathbb{Z})$. ⌟

Proof: Cf.[**?**]P234. □

Prop. (15.5.1.19). Let $V/\mathbb{Q}$ be an inner space and $A = (a_{ij}) \in GL(n;\mathbb{Z})$ be an integral Gram matrix for V. If $a_{ii} \leq 4\lambda$ for any i, where λ is the smallest eigenvalue of A, then for any totally real extension $F/\mathbb{Q}$, $\mathrm{O}(V;\mathcal{O}_F) = \mathrm{O}(V;\mathbb{Z})$. ⌟

Proof: Cf.[**?**]P236. □

2 Arithmetic Subgroup of Lie Groups

Def. (15.5.2.1) [Arithmetic Subgroups]. Let H be a connected real Lie group, then an **arithmetic subgroup** $\Gamma \subset H$ is a subgroup s.t. there exists an algebraic group $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/\mathbb{Q}$, a surjective homomorphism $G(\mathbb{R})^0 \to H$ with compact kernel, and $\Gamma_0 \subset G(\mathbb{Q})$ an arithmetic subgroup(15.5.1.1) s.t. $\Gamma_0 \cap G(\mathbb{R})^0$ is mapped to Γ. ⌟

Prop. (15.5.2.2). Let H be a semisimple real Lie group that admits a faithful f.d. representation, then every arithmetic subgroup of H is discrete of finite covolume, and contains a torsion-free subgroup of finite index. ⌟

Proof: Cf.[Mil17b]P34. □

Prop. (15.5.2.3). In any connected real Lie group there are only countably many arithmetic subgroups up to conjugacy. ⌟

Proof: Cf.[Mor15]5.1.20. □

Thm. (15.5.2.4) [Margulis]. Every discrete subgroup of finite volume in a non-compact simple real Lie group H is arithmetic unless H is isogenous to $SO(1,n)$ or $SU(1,n)$.

Note that $SL(2,\mathbb{R})$ is isogenous to $SO(1,2)$, so the theorem doesn't apply to it. ⌟

Proof: Cf.[Mor15]5.2.**?** □

15.6 Geometry of Numbers

References are [Cassels, Geometry of Numbers] and [Venkatesh's notes].

1 Minkowski Theory

Cf.[B-G06].

Thm. (15.6.1.1) [Minkowski's Lattice Point Theorem]. Let $V \in \mathcal{V}\mathrm{ect}_{\mathbb{R}}^n$ equipped with a Haar measure $\mathrm{d}x$ and $\Gamma \subset V$ be a complete lattice. Suppose $X \subset V$ is a centrally symmetric and convex measurable subset of V s.t.

$$\mu(X) > 2^n \operatorname{Vol}(\Gamma),$$

then $\# X \cap \Gamma > 1$. ⌟

Proof: Cf.[Neukirch]P27. □

Def. (15.6.1.2) [Minkowski Spaces]. For $F \in \mathtt{NField}$, $\mathbb{F}_{\mathbb{C}} \cong \prod_{\sigma: F \to \mathbb{C}} \mathbb{C}$, and $\mathrm{Gal}_{\mathbb{R}}$ acts on $\mathbb{F}_{\mathbb{C}}$ via permuting the coordinates. Then define

$$\mathbb{F}_{\mathbb{R}} = (\mathbb{F}_{\mathbb{C}})^{\mathrm{Gal}_{\mathbb{R}}}.$$

And it is equipped with a symmetric inner space structure via restriction from $\mathbb{F}_{\mathbb{C}} \cap \prod_{\sigma: F \to \mathbb{C}} \mathbb{C}$. Such a space $F_{\mathbb{R}}$ is called the **Minkowski space attached to** F. ⌟

Prop. (15.6.1.3) [Embedding in Minkowski Spaces]. For $F \in \mathtt{NField}$, there is a natural map $j : \mathbb{F} \subset \mathbb{F}_{\mathbb{R}}$, and if $\mathfrak{a} \neq 0 \in \mathrm{Ideal}(\mathcal{O}_F)$, then $j(\mathfrak{a})$ is a complete lattice in $F_{\mathbb{R}}$ with

$$\operatorname{Vol}(j(\mathfrak{a})) = \sqrt{|d_F|}||\mathfrak{a}||.$$

⌟

Proof: Cf.[Neukirch]P31. □

Prop. (15.6.1.4). Let $F \in \mathtt{NField}$ and $\mathfrak{a} \neq 0 \in \mathrm{Ideal}(\mathcal{O}_F)$. Let $c_\tau \in \mathbb{R}_+$ for each $\tau \in \operatorname{Hom}(F, \mathbb{C})$, s.t. $c_\tau = c_{\overline{\tau}}$, and

$$\prod_\tau c_\tau > (\frac{2}{\pi})^s \sqrt{|d_F|}||\mathfrak{a}||,$$

then there exists $a \in \mathfrak{a}^\times$ s.t.

$$|\tau(a)| < c_\tau, \quad \forall \tau \in \operatorname{Hom}(F, \mathbb{C}).$$

⌟

Proof: Cf.[Neukirch]P32. □

Prop. (15.6.1.5) [Minkowski's Second Theorem]. Let $F \in \mathtt{NField}$, $\deg(F) = d$, V a f.d. F-vector space of dimension n, and Λ a lattice in V. For any $v|\infty$, let S_v be a non-empty open convex symmetric bounded subset S_v of V_v. For $\lambda > 0 \in \mathbb{R}$, denote $\lambda S = \prod_{v|\infty} \lambda S_v \times \prod_{v\nmid\infty} \lambda \Lambda_v$. For $n \geq 1$, denote the ***n*-th succesive minimum** of S to be

$$\lambda_n = \inf\{t > 0 | tS \text{ contains } n \text{ linearly independent vectors of } \Lambda \text{ over } K\}.$$

Then
$$(\prod_{i=1}^{n}\lambda_i)\,\mathrm{Vol}(S)^{1/d}\leq 2^N,$$
where the volume is calculated w.r.t. the Adele measure given by(14.4.5.5).

Moreover, if S_v are totally symmetric, then
$$\frac{2^{dn}\pi^{sn}}{(n!)^r((2n)!)^s}N(d_{K/\mathbb{Q}})^{n/2}\leq(\prod_i\lambda_i)^d\mathrm{Vol}(S).$$

⌟

Proof: Cf.[B-G06]P611. □

15.7 Arithmetic of Abelian Varieties

Main references are [Sta], [Abelian Varieties notes Conrad], [Mil08], [B-G06], [Abelian Variety van der Geer], [BLR90]. See [Bhatt's notes] for everything done in the relative setting. A history of Abelian varieties can be found in [Mil08]P125.

1 Basics

Def. (15.7.1.1) [Abelian Schemes]. For $S \in \mathcal{S}\mathrm{ch}$, an **Abelian scheme** over S is a proper smooth group variety $A \in \mathcal{V}\mathrm{ar}/S$(6.11.5.1). Denote $\mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/S$ the subcategory of $\mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/S$ consisting of Abelian schemes over S.

Being an Abelian scheme is stable under base change of fields, by(6.11.1.3). ⌟

Prop. (15.7.1.2). For $S \in \mathcal{S}\mathrm{ch}$ and $X \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/S$, any global tangent vector on a group variety is left invariant. ⌟

Proof: Because $\Gamma(X, \mathcal{O}_X) = k$(6.11.1.12), so by(9.1.4.35), $\Gamma(X, \mathcal{O}_X \otimes T_{X,e}) = T_{X,e}$ are all generated by left invariant vectors(left and right translation commutes). □

Thm. (15.7.1.3) [Abelian Varieties are Projective, Weil]. Abelian varieties are projective, by(9.1.4.8) and(6.4.5.3). ⌟

Thm. (15.7.1.4)[Rigidity]. Let $S \in \mathcal{S}\mathrm{ch}$ and $f : X \to Y \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/S$ be a morphism from an Abelian varieties to a group variety, then it is a group homomorphism followed by a translation $t_{f(e_X)}$. ⌟

Proof: Set $y = i_Y(f(e_X))$ and consider $h = t_y \circ f$, then $h(e_X) = e_Y$, and consider the morphism:

$$g : X \times X \to Y : (x, x') \mapsto h(xx')(h(x)h(x'))^{-1}.$$

then $g(e_X, X) = g(X, e_X) = e_Y$, so the rigidity lemma(6.11.1.20) shows g is constant with value e_Y. Thus $h \circ m_X = m_Y \circ (h \times h)$, thus h is a group homomorphism. □

Cor. (15.7.1.5) [Abelian Varieties are Commutative]. For $S \in \mathcal{S}\mathrm{ch}$,

- If $X \in \mathcal{V}\mathrm{ar}/S$, then the Abelian variety structure on X is determined by e_X.
- If $X \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/S$, the group law on X is commutative, justifying the name.

⌟

Remark (15.7.1.6). The completeness of X is essential for the proof. In fact, there are many non-commutative group varieties, like $\mathrm{GL}(n)$.

From now, use the additive notation for Abelian varieties. ⌟

Proof: 1: If there are two Abelian variety structures $(m, i), (n, j)$, then consider $X \times X \to X \to X : (x, y) \mapsto m(x, y)(n(x, y)^{-1})$, then it is constant on $e_X \times X$ and $X \times e_X$, thus it is constant, so $m = n$. And $i = j$ is also clear by the associativity.

2: The inverse i is a group homomorphism by(15.7.1.4), thus it is commutative. □

Prop. (15.7.1.7) [Rigidity of Morphism from Smooth Varieties]. If $k \in$ `Field` and $X \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/k$, then any rational map from a smooth k-variety Y extends to a morphism $Y \to X$. ⌟

Proof: By(6.4.5.15), a rational map is defined on a set whose complement has codimension ≥ 2, but then(9.1.1.20) shows it must be defined on all of X. □

Prop. (15.7.1.8). For $S \in \mathcal{S}\mathrm{ch}$ and $X, Y \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/S$. If $f : X \to Y$ is a homomorphism over S s.t. for any arithmetic point $s \in S$, $f_s : X_s \to Y_s$ has finite kernel, then f is surjective, thus is an isogeny. ⌟

Proof: ? □

Cor. (15.7.1.9) [Quotient by Finite Subgroups]. Quotients of an Abelian variety A are also an Abelian varieties. ⌟

Proof: It is a group variety of dimension 1 with a rational point by(9.1.5.29). And it is complete by(6.4.5.3). □

Remark (15.7.1.10). WARNING: it is not true that the quotient of an Abelian variety by any finite group of automorphisms is an Abelian variety, as the quotient of an elliptic curve by the hyperelliptic involution(i.e. -1) is just $\mathbb{P}^1$. ⌟

Cor. (15.7.1.11)[Even Functions]. For $k \in \mathtt{Field}$ and $E \in \mathcal{E}\mathrm{ll}/k$, then $f \in R(E)$ is even iff $f \in K(x)$. ⌟

Proof: Write $f(x, y) = g(x) + h(x)y$, then the condition says $(2y + a_1x + a_3)h(x) = 0$ for any $(x, y) \in E(\overline{K})$. Thus $h(x) = 0$, otherwise E is degenerate, which is not possible. □

Pseudo-Abelian Varieties

Def. (15.7.1.12) [Pseudo-Abelian varieties]. A **pseudo-Abelian variety** over a field k is a group variety with no non-trivial affine normal group subvarieties. ⌟

Prop. (15.7.1.13). Abelian varieties are pseudo-Abelian varieties. ⌟

Proof: Every normal group subvariety is closed thus complete, hence if it is affine, it equals e. □

Prop. (15.7.1.14). Being a pseudo-Abelian variety is stable under separable base change of fields. ⌟

Proof: Cf.[Mil17]P149. □

Prop. (15.7.1.15). Let G be a group variety over k, then there exists a unique affine normal group subvariety N s.t. G/N is a pseudo-Abelian variety. And this N is stable under base change. ⌟

Proof: This follows from(9.1.4.34) and(9.1.5.30)(9.1.5.29). □

Prop. (15.7.1.16) [Barsotti-Chevalley]. Let k be perfect, then any pseudo-Abelian variety over k is complete hence is an Abelian variety. ⌟

Proof: Cf.[Mil17]P154. □

Cor. (15.7.1.17). If G is a group variety over a perfect field k, then unique affine normal group subvariety N s.t. G/N is an Abelian variety, by(15.7.1.15). ⌟

Thm. (15.7.1.18)[Algebraic Groups are Extensions of Abelian Varieties]. Let G be a connected algebraic group over a field k, then there is a connected affine normal algebraic subgroup N(not necessarily smooth) s.t. G/N is is an Abelian variety. ⌟

Proof: Cf.[Mil17]P155. □

Cor. (15.7.1.19). Every pseudo-Abelian variety G is commutative. ⌟

Proof: As G is smooth and connected, so is $[G,G]$(9.1.4.27), so it is a group variety(9.1.4.34). Let N be given by(15.7.1.18), then because G/N is an Abelian variety, $[G,G]\subset N$. Thus $[G,G]$ is affine, which implies $[G,G]=e$. □

Prop. (15.7.1.20) [Totaro(2013)]. Any pseudo-Abelian variety is an extension of a connected unipotent group variety U by an Abelian variety A in a unique way. ⌟

Proof:

□

Line Bundles

Remark (15.7.1.21). As Abelian varieties are regular, $\mathrm{Cl}(X)\cong\mathrm{Pic}(X)$, by(6.5.3.15). ⌟

Prop. (15.7.1.22) [Theorem of the Cube]. If X is an Abelian variety, and L is a line bundle over X, then

$$\Theta(L)=\mathrm{pr}_{123}^*(L)\otimes\mathrm{pr}_{12}^*(L^{-1})\otimes\mathrm{pr}_{13}^*(L^{-1})\otimes\mathrm{pr}_{23}^*(L^{-1})\otimes\mathrm{pr}_1^*(L)\otimes\mathrm{pr}_2^*(L)\otimes\mathrm{pr}_3^*(L)$$

is trivial. ⌟

Proof: This is trivial on $0\times X\times X, X\times 0\times X, X\times X\times 0$, so it is trivial, by(6.11.1.23). □

Cor. (15.7.1.23). There is a form of morphisms from a scheme to X, just by considering $(f,g,h): Y\times Y\times Y\to X\times X\times X$, i.e.

$$(f+g+h)^*L\otimes(f+g)^*L^{-1}\otimes(f+h)^*L^{-1}\otimes(g+h)^*L^{-1}\otimes f^*L\otimes g^*L\otimes h^*L$$

is trivial. ⌟

Cor. (15.7.1.24) [Theorem of the Square]. Let A be an Abelian variety that $\mathcal{L}$ is a line bundle, then for any $x,y\in A$,

$$t_{x+y}^*L\otimes L\cong t_x^*L\otimes t_y^*L\in\mathrm{Pic}(A_{k(x)k(y)}).$$

Notice this isomorphism is defined under the field generated by the residue fields of x and y. ⌟

Proof: Apply the theorem of the cube(15.7.1.23) for $f=\mathrm{id}_X$ and g,h the function with constant value x,y. □

Cor. (15.7.1.25). For a line bundle L on an Abelian variety X, then the map $\varphi_L: X\to\mathrm{Pic}(X): x\mapsto[t_x^*L\otimes L^{-1}]$ is a homomorphism. ⌟

Cor. (15.7.1.26). For any $\mathcal{L}\in\mathrm{Pic}(A)$,

$$[n]^*L\cong L^{n(n+1)/2}\otimes[-1]^*L^{n(n-1)/2}.$$

⌟

Proof: Use(15.7.1.23) in case $f=[n],g=[1],h=[-1]$, then we have:

$$n^*L^2\otimes(n+1)^*L^{-1}\otimes(n-1)^*L^{-1}\cong(L\otimes[-1]^*L)^{-1}.$$

So we can use induction. □

Def. (15.7.1.27) [Even Line Bundle]. Consider the involution $[-1]$ of X and its action on the line bundles, then a **even/odd line bundle** is defined to be a line bundle L that $[-1]^*\mathcal{L} \cong \mathcal{L}$(resp. $\mathcal{L}^{-1}$). ⌟

Prop. (15.7.1.28). On an Abelian variety, there is an even very ample line bundle. ⌟

Proof: Abelian variety is projective by(15.7.1.3), thus there is a very ample line bundle L, and $[-1]^*L$ is also very ample, so $L \otimes [-1]^*L$ is even and very ample, by(6.5.4.23). □

Prop. (15.7.1.29). For $F \in \mathtt{NField}, A \in \mathcal{A}b\,\mathcal{V}ar\,/F$ and $c \in \mathrm{Pic}(A)$, there are an odd line bundle c^- and an even line bundle c^+ that $c = c_- + c_+$. ⌟

Proof: Consider $2c = (c+[-1]^*(c))+(c-[-1]^*(c))$. $c-[-1]^*(c)$ is odd thus is in $\mathrm{Pic}^0(X)$ by(15.7.4.9), thus by(15.7.6.14), there is a $c^* \in \mathrm{Pic}^0(X)$ that $2c^* = c - [-1]^*(c)$. Then $c = (c - c^*) + c^*$ satisfies the requirement. □

Lemma (15.7.1.30). Let $S \in \mathcal{S}\mathrm{ch}, A \in \mathcal{A}b\,\mathcal{V}ar\,/S$ and $\mathrm{pr}_i : A \times A \to A$ be the projections and m be the multiplication, then the following are equivalent:

- $m^*(c) \cong \mathrm{pr}_1^*(c) + \mathrm{pr}_2^*(c)$.
- $\tau_a^*(c) \cong c$ for $a \in A$.

And if these are satisfied, c is even. ⌟

Proof: The equivalence is a consequence of the formula $(m^*(c) - \mathrm{pr}_1^*(c) - \mathrm{pr}_2^*(c))|_{A\times\{a\}} = \tau_a^*(c) - c$ and the see-saw principle(6.11.1.22). the last assertion is a consequence of the first equation pulled back via the morphism

$$A \to A \times A : a \mapsto (a, -a).$$

□

Prop. (15.7.1.31) [Projective Embeddings]. No Abelian varieties of dimension g can be embedded into $\mathbb{P}^{2g-1}$. No Abelian variety except for elliptic curves and Abelian surfaces of degree 10 in $\mathbb{P}^4$ can be embedded into $\mathbb{P}^{2g}$. ⌟

Proof: Cf.[Van de Geer P26], where algebraic topologies are used. □

2 Formal Groups

Def. (15.7.2.1) [Formal Group Law of Abelian Varieties]. Given $k \in \mathtt{Field}, A \in \mathcal{A}b\,\mathcal{V}ar\,/k$, the group structure on A induces a homomorphism $\mathcal{O}_{A,e} \to (\mathcal{O}_{A,e} \times \mathcal{O}_{A,e})_{e\times e}$, whose completion is a formal group law of dimension n. ⌟

3 over Alg.Closed Fields

Notation (15.7.3.1).

- Let $k \in \mathtt{Field}, k = \overline{k}$.

⌟

Prop. (15.7.3.2). There is a closed pt 0 in X that corresponds to 0 in the group $X(k)$, if we denote Ω_0 the cotangent space at 0, it is the stalk of the differential $\Omega_{X/k}$ at 0(6.5.5.6). ⌟

Def. (15.7.3.3) [Fields of Moduli]. Let k be a field, the **field of moduli** of an Abelian variety A over $\overline{k}$ is the fixed field of $\{\sigma \in \mathrm{Gal}(\overline{k}/k) | A^\sigma \cong A\}$. ⌟

Def. (15.7.3.4) [Fields of Definition]. Let k be a field, the **field of moduli** of an Abelian variety A over $\overline{k}$ is the minimal field $\overline{k} \supset k' \supset k$ s.t. A is defined over k'. ⌟

Remark (15.7.3.5). Generally, the field of definition is bigger than the field of moduli. ⌟

Prop. (15.7.3.6). For any Abelian variety A over a field $k = \overline{k}$ of dimension g, $\dim_k H^1(A, \mathcal{O}_A) \leq g$. In fact, equality holds by(15.7.4.16). ⌟

Proof: This follows from Borel's classification of Hopf-algebras(3.11.3.14). Cf.[Van de Geer P94] or [Conrad Notes, P45].**?** □

Prop. (15.7.3.7). Let $k \in \mathtt{Field}, k = \overline{k}$, $A \in \mathcal{A}b\,\mathcal{V}ar\,/k$, and $X \subset A$ is an integral subvariety. Suppose $\{a \in A(k) | a + X = X\} = 0$, then for m large, the map

$$\alpha_m : X^m \to A^{m-1} : (x_1, \ldots, x_m) \mapsto (x_1 - x_2, x_2 - x_3, \ldots, x_{m-1} - x_m)$$

is quasi-finite with generic degree 1. ⌟

Proof: Cf.[Equidistribution of Small points, Shouwu]P163.**?** □

p**-Divisible Groups**

Prop. (15.7.3.8). For $k \in \mathtt{Field}, \operatorname{char} k = p, A \in \mathcal{A}b\,\mathcal{V}ar\,/k, \ell \in \mathbf{P} \setminus \{p\}$, $A(k^{\text{sep}})$ is an Abelian group and $A[\ell^n] \cong (\mathbb{Z}/(\ell^n))^{2g}$ and $A[p^n] \cong (\mathbb{Z}/(p^n))^r$ for some $r \geq 1$. ⌟

Prop. (15.7.3.9). There is an isomorphism

$$\mathrm{H}^m_{\text{ét}}(\Lambda_{k^{\text{sep}}}, \mathbb{Q}_\ell) \cong \bigwedge^m_{\mathbb{Q}_\ell} (V_\ell(A))^*.$$

⌟

Proof: Cf.[Grothendieck Monodromy theorem]. □

4 Dual Abelian Varieties

Def. (15.7.4.1) [Dual Abelian Varieties]. For $S \in \mathcal{S}\mathrm{ch}$ and $A \in \mathcal{A}b\,\mathcal{V}ar\,/S$, the **dual Abelian variety** $A^\vee$ is defined to be its Picard scheme $\underline{\mathrm{Pic}}^0_{A/S} \in \mathcal{S}\mathrm{ch}^{\text{sep,loc.pf}}\,/S$(9.7.2.22), which represents $\widetilde{\underline{\mathrm{Pic}}}^0_{A/S}$(i.e. line bundles with a rigidification(9.7.2.5)). We will see it is an Abelian variety(i.e. smooth) in(15.7.4.16).

By definition, there is a universal line bundle $p_A \in \mathrm{Pic}(A \times A^\vee)$ with a rigidification along e. ⌟

Def. (15.7.4.2) [Symmetric Homomorphisms]. For $S \in \mathcal{S}\mathrm{ch}$ and $X \in \mathcal{A}b\,\mathcal{V}ar\,/S$, a homomorphism $\alpha : X \to X^\vee$ over S is called a **symmetric homomorphism** if $\alpha^\vee = \alpha$. ⌟

Prop. (15.7.4.3) [$A \to A^\vee$ **Induced by Line Bundles**]. Let $S \in \mathcal{S}\mathrm{ch}$ and $A \in \mathcal{A}b\,\mathcal{V}ar\,/S$. For any $\mathcal{L} \in \underline{\mathrm{Pic}}_{A/S}(S)$(line bundles with a rigidification(9.7.2.1)), there is a **Mumford line bundle** on $A \times A$ given by

$$\Lambda(\mathcal{L}) = m^*\mathcal{L} - \mathrm{pr}_1^*\mathcal{L} - \mathrm{pr}_2^*\mathcal{L},$$

where $m : A \times A \to A$ is the product. It is in $\mathrm{Pic}^0(A)$ because $u : \Lambda(c)|_{e \times A} \cong \mathcal{O}_S$ and $\Lambda(\mathcal{L})|_{A \times a} = \tau_a^* c - c$. Then by definition, this line bundle corresponds to a morphism $\lambda_{\mathcal{L}} : A \to A^\vee$ over S, and by(9.7.2.34) $\lambda_c(a) = \tau_a^* c - c \in A^\vee(k(a))$. This is also a homomorphism of Abelian schemes, by(15.7.1.4), as $\varphi_c(e) = e$.

It is clear that $\mathcal{L} \mapsto \lambda_{\mathcal{L}}$ is a group homomorphism $\mathrm{Pic}_{A/S}(S) \mapsto \mathrm{Hom}_S(A, A^\vee)$. Also, denote $K(\mathcal{L}) = \ker(\lambda_{\mathcal{L}})$. ⌟

Cor. (15.7.4.4). $\lambda_{\mathcal{L}}$ is symmetric. ⌟

Proof: This is because $\Lambda(\mathcal{L})$ is symmetric. □

Cor. (15.7.4.5). For $x \in A(k)$, $\lambda_{\tau_x^*\mathcal{L}} = \lambda_{\mathcal{L}}$. ⌟

Proof: This follows from see-saw lemma, by observing that stalks of the line bundles in(15.7.4.3) are $\tau_{a+x}^*\mathcal{L} - \tau_x^*\mathcal{L}$ and $\tau_a^*\mathcal{L} - \mathcal{L}$ resp.. □

Cor. (15.7.4.6). $(\mathrm{id}_A, \varphi_{\mathcal{L}})^* p_A = \mathcal{L} \otimes [-1]^*\mathcal{L}$. ⌟

Proof:

$$(\mathrm{id}_A, \varphi_{\mathcal{L}})^* p_A = \Delta_A^*(\mathrm{id} \times \lambda_{\mathcal{L}})^* p_A = \Delta_A^*(m^*\mathcal{L} - \mathrm{pr}_1^*\mathcal{L} - \mathrm{pr}_2^*\mathcal{L}) = [2]^*\mathcal{L} \otimes \mathcal{L}^{-2} \cong \mathcal{L} \otimes [-1]^*\mathcal{L}(15.7.1.26).$$

□

Prop. (15.7.4.7) [Poincaré Class is Even]. The Poincaré class $p_A \in \mathrm{Pic}(A \times A^\vee)$ is even. ⌟

Proof: Let $b \in A^\vee$, then

$$([-1]^*(p))|_{A\times\{b\}} = [-1]^*(p|_{A\times\{-b\}}) = [-1]^*(-b) = b.$$

and

$$([-1]^*(p))|_{\{0\}\times A^\vee} = [-1]^*(p|_{\{0\}\times\widehat{A}}) = 0.$$

Thus $[-1]^*p \cong p$ by(9.7.2.34) and the see-saw principle(6.11.1.22). □

Lemma (15.7.4.8). If $b \in \mathrm{Pic}(A)$ and $\lambda_b = 0$, then for any ample $c \in \mathrm{Pic}(A)$, there is some $a \in A(K)$ that $b = \tau_a^*(c) - c$. ⌟

Proof: [Mumford, P77]. □

Thm. (15.7.4.9) [Characterizing $A^\vee$]. For $\mathcal{L} \in \mathrm{Pic}(A)$, $[-1]^*(\mathcal{L}) \otimes \mathcal{L}^{-1} \in \mathrm{Pic}^0(A)$, and the following are equivalent:

1. $\mathcal{L} \in \mathrm{Pic}^0(A)$.
2. $\lambda_{\mathcal{L}} = 0$.
3. For every ample line bundle $c \in \mathrm{Pic}(A)$, there is an $a \in A$ that $\mathcal{L} \cong \tau_a^*(c) - c$.
4. There is an ample line bundle $c \in \mathrm{Pic}(A)$ and an $a \in A$ s.t. $\mathcal{L} \cong \tau_a^*(c) - c$.
5. $\mathcal{L}$ is odd.
6. For any scheme X, the map $\mathrm{Mor}(X, A) \to \mathrm{Pic}(X) : \varphi \mapsto \varphi^*(c)$ is a group homomorphism.

⌟

Proof: $2\to 3$ is lemma(15.7.4.8). $4\to 1$ is by(15.7.4.3). $3\to 4$ is trivial.

$1\to 2$: $\mathcal{L}\in\mathrm{Pic}^0(A)$ corresponds to a section $[\mathcal{L}]:k\to\underline{\mathrm{Pic}}^0_A$. Let

$$\Lambda(p_A)=(m\times\mathrm{id}_{\underline{\mathrm{Pic}}^0(A)})^*(p_A)-(\mathrm{pr}_1\times\mathrm{id}_{\underline{\mathrm{Pic}}^0(A)})^*(p_A)-(\mathrm{pr}_2\times\mathrm{id}_{\underline{\mathrm{Pic}}^0(A)})^*(p_A),$$

then it corresponds to a map $\Lambda:A\times\underline{\mathrm{Pic}}^0_A\to\underline{\mathrm{Pic}}^0_A$ s.t.

$$\lambda_{\mathcal{L}}=\Lambda\circ(i_1\times[\mathcal{L}]):A\to\underline{\mathrm{Pic}}^0_A.$$

But $\Lambda(A\times\{0\})=0$, so by rigidity lemma(6.11.1.20) it factors through the projection pr_1. Thus $\lambda_{\mathcal{L}}=0$.

$6\to 5$ is trivial, and 6 is clearly equivalent to the assertion when $X=A$, and it is equivalent to 2 by(15.7.1.30).

We next prove $[-1]^*(c)-c\in\mathrm{Pic}^0(A)$: because $[-1]\tau_a=\tau_{-a}[-1]$, we have

$$\tau_a^*([-1]^*(c))-[-1]^*(c)=[-1](\tau_{-a}^*(c)-c).$$

since $\tau_{-a}^*(c)-c\in\mathrm{Pic}^0(X)$ by(15.7.4.3), the equation is equal to $c-\tau_{-a}^*(c)$ by implication$1\to 2\to 6$. and this further equals $\tau_a^*(c)-c$ by the theorem of square(15.7.1.24). Then

$$\tau_a^*([-1]^*(c)-c)-([-1]^*(c)-c)=0.$$

Hence $[-1]^*(c)-c\in\mathrm{Pic}^0(A)$ by the implication $2\to 3\to 4\to 1$.

$5\to 1$: Let c be an odd element, then $-2c=[-1]^*(c)-c\in\mathrm{Pic}^0(A)$ by what just proved, we have $c\in\mathrm{Pic}^0(A)$, then φ_c has image in the kernel of $[2]$ on $\widehat{A}$, by the implication $1\to 2$, thus it has trivial image, by(15.7.6.14). □

Cor. (15.7.4.10). $\mathcal{L}\mapsto\lambda_{\mathcal{L}}$ induces an injection

$$\mathrm{NS}(A_{\overline{k}})=\mathrm{Pic}(A_{\overline{k}})/\mathrm{Pic}^0(A_{\overline{k}})\hookrightarrow\mathrm{Hom}(A_{\overline{k}},A^\vee_{\overline{k}}).$$

⌟

Cor. (15.7.4.11) [Abelian Varieties are Finite Torsion-Free]. For $k\in\mathtt{Field}$ and $A\in\mathcal{A}b\mathcal{V}ar/k$, $\mathrm{NS}(A_{\overline{k}})$ is a finite free $\mathbb{Z}$-module. (Although this is true for any complete variety**?**). ⌟

Proof: This follows from(15.7.4.10) and(15.7.6.8). □

Cor. (15.7.4.12). Let $S\in\mathcal{S}\mathrm{ch}$ and $A\in\mathcal{A}b\mathcal{V}ar/S$. If b is a section of $\underline{\mathrm{Pic}}^0_{A/S}\to S$, and $\mathcal{L}=b^*(p_A)\in\mathrm{Pic}(A)$, then $\lambda_A=0$. ⌟

Proof: □

Cor. (15.7.4.13). For $\mathcal{L}\in\mathrm{Pic}(A)$ and $n\in\mathbb{Z}$, $\lambda_{[n]\mathcal{L}}=n^2\lambda_{\mathcal{L}}$. ⌟

Proof: By(15.7.1.26), it suffices to prove for $n=-1$. And this follows from(15.7.4.9) and the fact $[-1]^*\mathcal{L}\otimes\mathcal{L}^{-1}\in\mathrm{Pic}^0(A)$. □

Prop. (15.7.4.14). Let $k\in\mathtt{Field}$, $A\in\mathcal{A}b\mathcal{V}ar/k$. For $\lambda\in\mathrm{Hom}(A,A^\vee)$, consider $\mathcal{M}=(\mathrm{id},\lambda)^*p_A$, then $\lambda_{\mathcal{M}}=\lambda+\lambda^\vee$. In particular, if λ is symmetric, then $\varphi_{\mathcal{M}}=2\lambda$. ⌟

Proof: [Geer]P159. □

Prop. (15.7.4.15) [Ample Implies Non-Degenerate]. $\mathcal{L} \in \mathrm{Pic}(A)$ is ample iff it is non-degenerate and $H^0(A, \mathcal{L}) \neq 0$.

In particular, an effective line bundle on A is ample iff it is non-degenerate. ⌟

Proof: Cf.[Diophantine Geometry, P253] or [Conrad notes].**?** □

Cor. (15.7.4.16) [Dual Abelian Variety]. Let $k \in \mathtt{Field}$ and $A \in \mathcal{A}b\mathcal{V}ar/k$, then

$$A^\vee = \underline{\mathrm{Pic}}^0_{X/S} = \underline{\mathrm{Pic}}^0_{X/S,\mathrm{red}} = \underline{\mathrm{Pic}}^\tau_{X/S}$$

is also an Abelian variety, and $\dim A = \dim A^\vee = \dim_k H^1(A, \mathcal{O}_A)$. ⌟

Proof: Take an ample line bundle $\mathcal{L}$ on A, then $\varphi_L : A \to A^\vee$ has finite kernel, thus $\dim \widehat{A} \geq \dim A$, but by(15.7.3.6) and(9.7.2.24), $\dim_k H^1(A, \mathcal{O}_A) = T_e(A^\vee) \leq \dim A$, thus it is regular by(5.3.5.17).

$\underline{\mathrm{Pic}}^\tau_{X/S} = \underline{\mathrm{Pic}}^0_{X/S}$ because we can pass to the $k = \overline{k}$, and use the fact Abelian varieties are torsion-free(15.7.4.11). □

Lemma (15.7.4.17). For $k \in \mathtt{Field}$ and $A \in \mathcal{A}b\mathcal{V}ar/k$, $\mathcal{L} \in \mathrm{Pic}(A)$, consider the double Picard map(9.7.2.37) $\kappa_A : A \to A^{\vee\vee}$, then $\lambda_{\mathcal{L}} = \lambda_{\mathcal{L}}^\vee \circ \kappa_A : A \to A^\vee$. ⌟

Proof: Cf.[van Der Geer, P100]. □

Prop. (15.7.4.18) [Double Duality Theorem]. For $k \in \mathtt{Field}$ and $A \in \mathcal{A}b\mathcal{V}ar/k$, the double Picard map(9.7.2.37) $A \to A^{\vee\vee}$ is an isomorphism. ⌟

Proof: Cf.[van Der Geer, P101].**?** □

Prop. (15.7.4.19) [Dual Abelian Schemes]. If $S \in \mathcal{S}ch$ and $A \in \mathcal{A}b\mathcal{V}ar/S$, then

- $\underline{\mathrm{Pic}}^0_{A/S} = \mathrm{Pic}^\tau_{A/S}$ is a projective Abelian scheme over S, called the **dual Abelian scheme** of A/S.
- the double Picard map(9.7.2.37) $A \to A^{\vee\vee}$ is an isomorphism.

⌟

Proof: By reducing to the fiber, these reduces to the case that S is a field, and this case follows from(15.7.4.16) and(15.7.4.18). □

Def. (15.7.4.20) [Non-Degenerate Line Bundles]. For $S \in \mathcal{S}ch$ and $A \in \mathcal{A}b\mathcal{V}ar/S$, a **non-degenerate line bundle** is a rigidified line bundle $\mathcal{L} \in \underline{\mathrm{Pic}}_{A/S}(S)$ s.t. $K(\mathcal{L}) = \ker \varphi_{\mathcal{L}}$ is a finite flat group scheme, i.e. $\varphi_{\mathcal{L}}$ is an isogeny. ⌟

5 Cohomology on Abelian Varieties

Thm. (15.7.5.1) [Cohomology of the Poincaré Class]. For $k \in \mathtt{Field}$ and $A \in \mathcal{A}b\mathcal{V}ar^g/k$, Let $\mathrm{pr}_2 : A \times A^\vee \to A^\vee$ be the projection, then

$$R^n \mathrm{pr}_{2*} p_A = e_*(k)^{\delta_{n,g}}, \quad H^n(A \times A^\vee, p_A) = k^{\delta_{n,g}}.$$

⌟

Proof: Cf.[Conrad, P62] or [Geer, P126]**?**. □

Thm. (15.7.5.2) [Cohomology of Line Bundles]. Let $k \in \mathtt{Field}$ and $A \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}^g/k$, $\mathcal{F} \in \mathfrak{Coh}(A)$, then

1. $\chi(\mathcal{F}) = \deg(\mathrm{ch}_g(\mathcal{F}))$.
2. If $\mathcal{L} \in \mathrm{Pic}(A)$, then $\chi(\mathcal{L}) = \deg(c_1(\mathcal{L})^g)/g!$. In particular, $\chi(\mathcal{L}^m) = m^g\chi(\mathcal{L})$.
3. $\deg(\lambda_{\mathcal{L}}) = \chi(\mathcal{L})^2$. In particular, $\deg(\lambda_{\mathcal{L}})$ is a square. Notice if $\mathcal{L}$ is degenerate, then $\deg(\lambda_{\mathcal{L}}) = 0$.
4. If $\mathcal{L} \in \mathrm{Pic}(A)$ is a non-degenerate line bundle, then there is a unique integer $0 \leq i \leq g$ s.t. $H^i(X, \mathcal{L}) \neq 0$. Such an i is called the **index of** $\mathcal{L}$. And $\mathrm{ind}(\mathcal{L}^{-1}) + \mathrm{ind}(\mathcal{L}) = g$. Notice $\mathrm{ind}(\mathcal{L}) = 0$ is equivalent to it is effective or equivalent to it being ample(15.7.4.15).
5. Moreover, if $k = \mathbb{C}$, and $A = \mathrm{Lie}(A)/\Lambda$, $\mathcal{L} \in \mathrm{Pic}(A)$, then $c_1(\mathcal{L})$ corresponds to a Hermitian form H**?**, and $\mathrm{ind}(\mathcal{L})$ is just the number of negative eigenvalues of H.

⌟

Proof: 1, 2: Because $\mathcal{T}_{A/k}$ is trivial, the Todd class $\mathrm{Todd}(\mathcal{T}_{A/k}) = 1$, so the assertions follows from Hirzebruch-Riemann-Roch(8.1.10.3).

3. 4. For the last assertion, Cf.[Van de Geer, P131]**?**

$$\dim_k H^n(X \times X, \Lambda(\mathcal{L})) = \deg(\lambda_{\mathcal{L}})\delta_{n,g},$$

$$H^n(X\times X, \Lambda(\mathcal{L})) \cong H^n(X\times X, m^*\mathcal{L}\otimes \mathrm{pr}_1^*\mathcal{L}^{-1}) \cong H^n(X\times X, \mathrm{pr}_1^*\mathcal{L}\otimes \mathrm{pr}_2^*\mathcal{L}^{-1}) \cong \bigoplus_{p+q=n} H^p(X,\mathcal{L})\otimes H^q(X,\mathcal{L}^{-1}).$$

So item4 follows from the two equations above.

5:**?** □

Cor. (15.7.5.3). Let $k \in \mathtt{Field}$ and $f : X \to Y \in \mathrm{Isog}_k$, then $\chi(f^*\mathcal{L}) = \deg(f)\chi(\mathcal{L})$. ⌟

Proof: We may base change to $k = \overline{k}$. By the proposition and the fact $c_1(f^*(\mathcal{L})^g) = f^*(c_1(\mathcal{L})^g)$, it suffices to show that $\deg(f^*([P])) = \deg(f)$ for any point $P \in Y(k)$, which is trivial. □

Prop. (15.7.5.4) [Properties of Indices]. For $k \in \mathtt{Field}$ and $A \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/k$, then

- The index is a locally constant function in algebraic families of non-degenerate line bundles. In particular, if $\mathcal{L} \in \mathrm{Pic}(A)$ is non-degenerate and $\mathcal{L}' \in \mathrm{Pic}^0(A)$, $\mathrm{ind}(\mathcal{L}) = \mathrm{ind}(\mathcal{L} \otimes \mathcal{L}')$.
- If $f : B \to A \in \mathrm{Isog}_k$, and $\mathcal{L} \in \mathrm{Pic}(A)$ a non-degenerate line bundle, then $\mathrm{ind}(\mathcal{L}) = \mathrm{ind}(f^*\mathcal{L})$.
- If $\mathcal{L}$ is non-degenerate, then for $m \in \mathbb{Z}_+$, $\mathcal{L}^{\otimes m}$ is non-degenerate too, and $\mathrm{ind}(\mathcal{L}^{\otimes m}) = \mathrm{ind}(\mathcal{L})$.
- If $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_1 \otimes \mathcal{L}_2 \in \mathrm{Pic}(A)$ are all non-degenerate, then $\mathrm{ind}(\mathcal{L}_1 \otimes \mathcal{L}_2) \leq \mathrm{ind}(\mathcal{L}_1) + \mathrm{ind}(\mathcal{L}_2)$.
- If $\mathcal{L}, \mathcal{L}' \in \mathrm{Pic}(X)$ and $\mathcal{L}, \mathcal{L} \otimes \mathcal{L}'$ are both non-degenerate, then $\mathrm{ind}(\mathcal{L} \otimes \mathcal{L}') \leq \mathrm{ind}(\mathcal{L})$.

⌟

Proof: Cf.[Geer, P134].**?** □

Prop. (15.7.5.5). Let $k \in \mathtt{Field}$ and $A \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/k$. Suppose $\mathcal{L}, \mathcal{H} \in \mathrm{Pic}(A)$ and $\mathcal{L}, \mathcal{L} \otimes \mathcal{H}$ are both non-degenerate, and that $\mathrm{ind}(\mathcal{L}) \neq \mathrm{ind}(\mathcal{L} \otimes \mathcal{H})$, then the polynomial $P(t) = \deg((c_1(\mathcal{L}) + tc_1(\mathcal{H}))^g)$ has a root $t \in [0, 1]$. ⌟

Proof: Cf.[Geer, P136]**?** □

Cor. (15.7.5.6). Let $k \in \mathtt{Field}$ and $A \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/k$. Then for any $\mathcal{L} \in \mathrm{Pic}(A)$ non-degenerate and $m \in \mathbb{Z}_+$, $\mathrm{ind}(\mathcal{L}^m) = \mathrm{ind}(\mathcal{L})$. ⌟

Proof: ? □

Thm. (15.7.5.7) [Kempf-Mumford-Ramanujam]. Let $\mathcal{L}$ be a line bundle on an Abelian variety A, and fix an ample line bundle H on A, let Φ be the Hilbert polynomial of $\mathcal{L}$ w.r.t. H, then

- The multiplicity of 0 in Φ equals $\dim K(\mathcal{L})$.
- If $\mathcal{L}$ is non-degenerate, then all roots of Φ in $\mathbb{C}$ are real, and the number of positive roots equals $\operatorname{ind}(\mathcal{L})$.

⌟

Proof: Cf.[Van de Geer, P139,140]. □

Prop. (15.7.5.8). For any ample line bundle $\mathcal{L}$ on A, $\mathcal{L}^{\otimes m}$ is basepoint-free for $m \geq 2$ and very ample for $m \geq 3$. ⌟

Proof:

□

Prop. (15.7.5.9). Let $S \in \mathcal{S}\mathrm{ch}$ is connected and $X \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/S$. If $\mathcal{L} \in \operatorname{Pic}(X)$ is non-degenerate, and there exists an arithmetic point $s \in S$ s.t. L_s is ample on X_s, then $\mathcal{L}$ is relatively ample on X/S. ⌟

Proof: □

6 Isogenies and Tate Modules

Isogenies

Prop. (15.7.6.1) [Isogenies of Abelian Varieties]. Let $k \in \mathtt{Field}$ and $f : X \to Y \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/k$, the following are equivalent:

- f is an isogeny.
- f is surjective and $\dim X = \dim Y$.
- $\ker f$ is a finite group scheme and $\dim X = \dim Y$.
- f is finite.

The set of isogenies from X to Y is denoted by $\operatorname{Isog}(X, Y)$. $\operatorname{Isog}(X, X) \cup \{0\}$ is denoted by $\operatorname{Isog}(X)$. ⌟

Proof: This follows from the theory of algebraic groups. □

Prop. (15.7.6.2) [Separable Isogenies]. Let $f : X \to Y$ be an isogeny of Abelian varieties over k, then

- For any $Q \in Y(\overline{k})$, $\#f^{-1}(Q)(\overline{k}) = \deg_s(f)$, and for any $P \in X$, $e_P(f) = \deg_i(f)$.
- The map: $X[f] \to \operatorname{Gal}(K(X_{\overline{k}})/\varphi^*(K(Y_{\overline{k}}))) : P \mapsto \tau_P^*$ is an isomorphism of groups.
- f is unramified iff it is étale iff it is separable, and in this case, $K(X_{\overline{k}})/K(Y_{\overline{k}})$ is an Abelian Galois extension of degree $\deg(f)$.

⌟

Proof: 1: By(6.11.3.4), this holds for Q in a dense open subset of Y, thus by homogeneity, it holds for all Q. The second assertion follows from the fact after shrining f is finite locally free of rank $\deg(f)$ by using homogeneity on X.

2: This is clearly a group homomorphism. By Galois theory, it suffices to show it is injective, which is clear.

3: This follows from(15.7.6.1) and generic unramifiedness(6.6.5.9). □

Prop. (15.7.6.3) [Isogenous is an Equivalence Relation]. If $k \in \texttt{Field}, X, Y \in \mathcal{A}b\mathcal{V}ar/k$ and $f \in \operatorname{Isog}(X,Y)$, $d = \deg(f)$, then there exists $g \in \operatorname{Isog}(Y,X)$ s.t. $g \circ f = [d]_X, f \circ g = [d]_Y$.

In particular, we can write $X \sim Y$ to denote that X, Y are isogenous. This is an equivalence relation. ⌟

Proof: As $\ker(f)$ is a finite group scheme of rank d, $[d]\ker(f) = 0$, so $[d]$ factors through f via $g : Y \to X$, so $g \circ f = [d]_X$. Then also $[d]_Y \circ f = f \circ [d]_X = f \circ (g \circ f) = (f \circ g) \circ f$, thus $[d]_Y = f \circ g$ as f is a quotient map. □

Prop. (15.7.6.4) [Dual Isogenies]. Let $A, A' \in \mathcal{A}b\mathcal{V}ar/k$ and $\varphi \in \operatorname{Hom}(A, A')$, then we get a dual homomorphism $\widehat{\varphi} \in \operatorname{Hom}((A')^\vee, A^\vee)$. Then:

- $\widehat{\widehat{\varphi}} = \varphi$.
- $\deg(\widehat{\varphi}) = \deg(\varphi)$.
- $\widehat{\varphi + \psi} = \varphi^\vee + \widehat{\psi}$.
- $([m]_E)^\vee = [m]_{E^\vee}$.

⌟

Proof: 1: This is formal.

2: [Conrad, P66].?

3: This is clear from the modular description of $\widehat{A}$.

4: This follows from 3. □

<u>$\operatorname{Hom}(X,Y)$</u>

Def. (15.7.6.5) [Simple Abelian Varieties]. A **simple Abelian variety** is an Abelian variety that has no non-trivial Abelian subvarieties. ⌟

Thm. (15.7.6.6) [Poincaré's Complete Reducibility Theorem]. Let B be an Abelian subvariety of A, then there exists an Abelian subvariety C of A that the addition gives an isogeny

$$B \times C \to A.$$

⌟

Proof: Choose an ample line bundle c on A, let $\iota : B \to A$ be the inclusion and $\widehat{\iota} : \widehat{A} \to \widehat{B}$ the dual map, then

$$(\widehat{\iota} \circ \lambda_c)|_B = \lambda_{\iota^*(c)}.$$

Since $\iota^*(c)$ is also ample, $\varphi_{\iota^*(c)}$ is an isogeny, thus has finite kernel. Let $C = \ker(\iota \circ \varphi_c)$, then we have $C \cap B$ is finite, whence $B \times C \to A$ has finite kernel. The dimension theorem(9.1.4.36) applied to $\iota \circ \varphi_c$ shows

$$\dim C + \dim B^\vee = \dim A^\vee.$$

and this together with(15.7.4.16) shows $B \times C \to A$ is a surjection, because A is irreducible. Thus it is an isogeny. □

Cor. (15.7.6.7). For $k \in \texttt{Field}, A \in \mathcal{A}b\mathcal{V}ar/k$, there are simple Abelian subvarieties $B_1, \ldots, B_n$ of A that the inclusions give an isogeny

$$B_1 \times \ldots \times B_n \to A.$$

⌟

Prop. (15.7.6.8) [Hom(A, A') is Torsion-Free and F.g.]. Let k be a field and $A, A' \in \mathcal{A}b\mathcal{V}ar/k$, then $\mathrm{Hom}(A_1, A_2)$ w.r.t. the addition is a f.g. torsion-free Abelian group of rank at most $4g^2$. ⌟

Proof: Assume $[m]\circ\varphi = 0$, then $\varphi\circ[m] = 0$, and use the fact $[m]$ is surjective(15.7.6.14). The last assertion follows from(15.13.2.3). □

Def. (15.7.6.9) [Quasi-Isogenies]. For $A, A' \in \mathcal{A}b\mathcal{V}ar/k$, $\mathrm{Hom}(A, A')_{\mathbb{Q}} = \mathrm{Hom}(A, A') \otimes \mathbb{Q}$ is called the set of **quasi-isogenies** from A to A'.

Define the category Isog/k to be the category consisting of Abelian varieties over k with morphisms $\mathrm{Mor}(A, A') = \mathrm{Hom}(A, A')_{\mathbb{Q}}$. Notice $f : A \to A' \in \mathcal{A}b\mathcal{V}ar/k$ is an isogeny iff f is an isomorphism in Isog/k, by(6.4.4.20).

Thus by(15.7.6.7), Isog/k is a semisimple $\mathbb{Q}$-linear Abelian category. ⌟

Prop. (15.7.6.10). For $A, A' \in \mathcal{A}b\mathcal{V}ar/k$, if $A \sim A'$, then $\mathrm{End}_{\mathbb{Q}}(A) = \mathrm{End}_{\mathbb{Q}}(A')$. Moreover, $\mathrm{End}_{\mathbb{Q}}(A)$ is a semisimple $\mathbb{Q}$-algebra, and it is simple iff A is simple. ⌟

Proof: These follow from(15.7.6.7). □

Def. (15.7.6.11) [Abelian Varieties of GL(2)-Type]. $A \in \mathcal{A}b\mathcal{V}ar/\mathbb{Q}$ is called an **Abelian variety of GL(2)-type** if A is simple and $\mathrm{End}(A)_{\mathbb{Q}}$ contains some $E \in \mathtt{NField}$ with $[E : \mathbb{Q}] = \dim A$. ⌟

Thm. (15.7.6.12). $A \in \mathcal{A}b\mathcal{V}ar/\mathbb{Q}$ is of GL(2)-type iff it is a simple quotient of $J_1(N)/\mathbb{Q}$. ⌟

Proof: Cf.[Ribet, Abelian Varieties over $\mathbb{Q}$ and Modular Forms]. And [Serre's Modularity Conjecture 1]P502.? □

Tate Modules

Prop. (15.7.6.13). For $S \in \mathrm{N}\mathcal{S}\mathrm{ch}$, $A \in \mathcal{A}b\mathcal{V}ar^g/S, n \in \mathbb{Z}_+$ and n is invertible on S, then $A[n]$ is a finite locally free S-group scheme of order n^{2g}. ⌟

Proof: ? □

Prop. (15.7.6.14) [Multiplication Map, Weil]. Let $k \in \mathtt{Field}$, $A \in \mathcal{A}b\mathcal{V}ar/k$, and $n \in \mathbb{Z}\cap k^\times$, then $[n] : A \to A$ is finite faithfully flat of degree $n^{2\dim A}$. In particular it is an isogeny(15.7.6.1), and

- If $n \in \mathbb{Z}\setminus(\mathrm{char}\, k)$, then $[n]$ is finite étale and $|A[n]| \cong (\mathbb{Z}/n\mathbb{Z})^{2\dim A}$.
- If $n = 0 \in k$, then $[n]$ is not separable.
- If $\mathrm{char}\, k = p \in \mathbf{P}$, then $|A(p)| \cong (\mathbb{Z}/p\mathbb{Z})^r \times \alpha_p^{2g-2r} \times \mu_p^r$ for some $0 \le r \le g$. In particular, $A[p^e] = (\mathbb{Z}/(p^e))^r$ for any $e \ge 0$. This r is called the **p-rank** of A. It is invariant under isogenies.

⌟

Proof: 1, 2: Let $Z = \ker([n])$, then it is proper. By(15.7.1.26), choose an ample line bundle $\mathcal{L} = \mathcal{L}(D) \in \mathrm{Pic}(A)$, then $\mathcal{O}_Z = \mathcal{L}_Z^{n(n+1)/2} \otimes [-1]^*\mathcal{L}_Z^{n(n-1)/2}$. As $\mathcal{L}_Z$ and $[-1]^*\mathcal{L}_Z$ are both ample, $\mathcal{O}_Z$ is ample. Now(6.4.4.20) shows Z is finite. Thus by dimension equation, $[n]$ is finite and faithfully flat.

The action of $[n]$ on the tangent space at the origin is given by multiplying by n by(9.2.2.1), thus it is unramified at the origin iff $n \in \mathbb{Z}\cap k^*$ by(6.6.5.12), and also on any other closed points by homogeneity. Thus if $n \in \mathbb{Z}\cap k^*$, $[n]$ is finite étale, and otherwise $[n]$ is not separable, by(6.6.5.12), as it is not generically unramified.

To calculate $A[n]$ in the étale case, notice $[n]^*D = n^2D$, and the intersection number formula

$$n^{2g}(D \cdot D \cdot \ldots \cdot D) = ([n]^*D \cdot [n]^*D \cdot \ldots \cdot [n]^*D) = \deg([n])(D \cdot D \cdot \ldots \cdot D)$$

where the intersection is g-fold, thus $(D \cdot D \cdot \ldots \cdot D)$ equals the degree of the projection embedding of X via $\mathcal{L}(D)$ thus positive, so we get $\deg([n]) = n^{2g} = \#A[n]$ as $[n]$ is finite étale. To see the structure of $A[n]$, notice this is true for any $m|n$.

3: **?** Cf.[Conrad]. The last assertion follows from the fact the fact $[p]$ is surjective and the structure theory of Abelian groups. □

Def. (15.7.6.15) [Tate Modules]. Let $k \in \texttt{Field}, A \in \mathcal{A}b\mathcal{V}ar/k$. For $\ell \in \mathbf{P}\backslash \operatorname{char} k$, define $T_\ell(A) = \varprojlim_{n\geq 0} A[\ell^n]$, called the **Tate module** of A. Then it is naturally a $\mathbb{Z}_\ell$-module and isomorphic to $\mathbb{Z}_\ell^{2g}$ by(15.7.6.14).

Also define $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. There are Gal_k actions on them, as $[\ell^n]$ is étale and Gal_k preserves $A[\ell^n]$ because O is Gal_k-invariant.

For $\ell = \operatorname{char} k = p > 0$, we can also define $T_p(A)$, which is isomorphic to $\mathbb{Z}_p^r$ for some $0 \leq r \leq g$ by(15.7.6.14), but there is not Galois action on it. ⌟

Def. (15.7.6.16) [Adelic Tate Modules]. Situation as in(15.7.6.15), if $\operatorname{char} k = 0$, define the **Adelic Tate module** to be

$$T_f(A) = \prod_{\ell\in\mathbf{P}} T_\ell(A), \quad V_f(A) = \prod_{\ell\in\mathbf{P}}{}' (V_\ell(A), T_\ell(A)).$$

⌟

Prop. (15.7.6.17) [Étale Cohomology and Tate Modules]. Let $k = k^s$ and $A \in \mathcal{A}b\mathcal{V}ar^g/k$, and $\ell \in \mathbf{P}\backslash \operatorname{char} k$, then

- There are canonical isomorphisms $\mathrm{H}^1_{\text{ét}}(A, \mathbb{Z}_\ell) \cong \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), \mathbb{Z}_\ell) \cong T_\ell(A)(1)$. Thus $\mathrm{H}^1_{\text{ét}}(A, \mathbb{Z}_\ell) \cong \mathbb{Z}_\ell^{2g}$ by(15.7.6.14).
- The cup product define isomorphisms $\wedge^r H^1_{\text{ét}}(A, \mathbb{Z}_\ell) \cong H^r(A, \mathbb{Z}_\ell)$ for any $r > 0$.

⌟

Proof: Cf.[Mil08]P55. **?** □

Cor. (15.7.6.18). There is a natural Gal_k-invariant pairing $\wedge^r T_\ell(A) \times \mathrm{H}^r_{\text{ét}}(A, \mathbb{Z}_\ell) \to \mathbb{Z}_\ell$. ⌟

Prop. (15.7.6.19). Let $k \in \texttt{Field}, A \in \mathcal{A}b\mathcal{V}ar/k$ and $\ell \in \mathbf{P} \setminus \{\operatorname{char} k\}$, then for the representation $\rho_\ell : \mathrm{End}(A)_\mathbb{Q} \to \mathrm{End}(V_\ell)$ and any $f \in \mathrm{End}(A)_\mathbb{Q}$,

$$\deg(f) = \det(\rho_\ell(f)).$$

In particular, $\deg([n] - f) = \det(n - \rho_\ell(f))$ for any $n \in \mathbb{Z}$. ⌟

Proof: **?** □

Prop. (15.7.6.20) [Semisimplicity]. Let $F \in \texttt{GField}, \ell \in \mathbf{P}\backslash \operatorname{char} F, A \in \mathcal{A}b\mathcal{V}ar/F$, then the action of Gal_F on $V_\ell(A)$ is semisimple. ⌟

Proof:

□

7 Polarizations and Weil Pairings

Polarizations and Rosati Involutions

Def. (15.7.7.1) [Polarizations]. For $S \in \mathcal{S}\mathrm{ch}$ and $X \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}\,/S$, a **polarization** of X/S is a symmetric isogeny $\lambda : X \to X^\vee$ s.t. étale locally, λ is of the form $\lambda_{\mathcal{L}}$ for relatively ample rigidified line bundles $\mathcal{L}$.

A **principal polarization** of an Abelian variety is a polarization of degree 1.

The category of Abelian varieties over k of dimension g together with a polarization of degree d is denoted by $\mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}^{g,\mathrm{polar}=d}\,/k$. ⌟

Prop. (15.7.7.2) [Zarhin's Trick]. For any $k \in \texttt{Field}$ and $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}\,/k$, $(A \times A^\vee)^4$ is canonically principally polarized. ⌟

Proof: Cf.[Mil08]P60. □

Thm. (15.7.7.3) [Finitely Many Polarizations]. Let $k \in \texttt{Field}$ and $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}\,/k$, then for any $d \in \mathbb{Z}_+$, there are only f.m. isomorphism classes of polarizations on A of degree d. ⌟

Proof: Cf.[Mil08]P63. □

Def. (15.7.7.4) [Rosati Involutions]. For $k \in \texttt{Field}, A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}\,/k$ and $\lambda : A \to A^\vee$ a polarization, then the inverse $\lambda^{-1} \in \mathrm{Hom}(A^\vee, A)_{\mathbb{Q}}$ is definable by(15.7.6.3). Then the **Rosati involution** corresponding to λ is defined to be the map

$$\mathrm{End}(A)_{\mathbb{Q}} \to \mathrm{End}(A)_{\mathbb{Q}} : \alpha \mapsto \lambda^{-1} \circ \alpha^\vee \circ \lambda.$$

Then it is an involution. ⌟

Prop. (15.7.7.5) [Rosati Involutions are Positive]. For $k \in \texttt{Field}$ and $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}\,/k$, the bilinear form

$$(\alpha, \beta) \mapsto \mathrm{tr}(\alpha \circ \beta^\dagger) : \mathrm{End}(A)_{\mathbb{Q}}^2 \to \mathbb{Q}$$

is positive definite. ⌟

Proof: □

Prop. (15.7.7.6). Let $k \in \texttt{Field}$ and $(A, \lambda) \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}\,/k$, then

- $\#\,\mathrm{Aut}((A, \lambda)) < \infty$.
- for any $n \geq 3$, any automorphism of (A, λ) acting trivially on $A[n]$ is the identity.

⌟

Proof: Cf.[Milne, P62]**?** □

Weil Pairings

Thm. (15.7.7.7)[Weil Pairings]. Let $S \in \mathcal{S}\mathrm{ch}$ and $X, Y \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}\,/S$, then for any isogeny $\alpha : X \to Y$, there is a perfect pairing

$$e_\alpha : \ker(\alpha) \times \ker(\alpha^\vee) \to \mathbb{G}_m.$$

⌟

Proof: Cf.[Mumford, P143]**?**. □

Def. (15.7.7.8) [Induced Pairings]. For $k \in \texttt{Field}, A \in \mathcal{A}b\mathcal{V}ar$, if e_m is any Weil pairing, and $\lambda : A \to A^\vee \in \mathrm{Isog}/k$, denote

$$e_m^\lambda = e_m \circ (\mathrm{id} \times \lambda) : A[m] \times A[m] \to \mu_m(1).$$

⌟

Def. (15.7.7.9). Let $k \in \texttt{Field}, \ell \in \mathbf{P}$ and $\mathrm{char}\, k \neq 2, \ell$. Then for $A \in \mathcal{A}b\mathcal{V}ar/k$, $\lambda \in \mathrm{Hom}(A, A^\vee)$ is ⌟

Prop. (15.7.7.10) [Weil Pairing for Elliptic Curves]. Let $E \in \mathcal{E}\mathrm{ll}/k$, then for any $m \in \mathbb{Z} \cap k^*$, there is a non-degenerate pairing

$$e_m : E[m] \times E[m] \to \mu_m$$

that is alternating, non-degenerate and Gal_k-invariant.

Moreover, $e_{mm'}(S,T) = e_m([m']S,T)$ for $S \in E[mm']$ and $S \in T[m]$. In particular, for $\ell \in \mathbf{P} \backslash \mathrm{char}\, k$, we can define a Weil pairing on the Tate module

$$e : T_\ell(E) \times T_\ell(E) \to \mu_{\ell^\infty}.$$

⌟

Proof: Let $T \in E[m]$, then by(15.11.1.22), there exists some $f \in \overline{K}(E)^*$ s.t. $\mathrm{div}(f) = m[E] - m[O]$. Let $T' \in E[m^2]$ s.t. $mT' = T$, then there exists a function $g \in \overline{K}(E)^*$ s.t.

$$\mathrm{div}(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} ([T' + R] - [R]).$$

Notice $f \circ [m]$ and g^m have the same divisor, so we may assume $f \circ [m] = g^m$. Then for any $S \in E[m]$ and $X \in E$, $g(S+X)^m = f(mX) = g(X)^m$, so $E \to \mathbb{P}^1 : g(X+S)/g(X)$ is constant and has value in μ_m, denote it by $e(T,S)$.

For bilinearity, Cf.[Sil16]P94**?**.

For alternating, Cf.[Sil16]P94**?**.

For non-degeneracy, if $e_m(S,T) = 1$ for any $T \in E[m]$, then g is $E[m]$-invariant, which implies $g = h \circ [m]$ for some $h \in \overline{K}(E)^*$ by(15.7.6.2) and the fact $[m]$ is separable. Then $(h \circ [m])^m = f \circ [m]$, so $f = h^m$, and $\mathrm{div}(h) = [T] - [O]$, so $T = O$.

Galois invariance is clear.

The last assertion follows by taking $g' = g \circ [m']$ and $f' = f^{m'}$. □

Cor. (15.7.7.11) [Primitive Pairing]. Let $E \in \mathcal{E}\mathrm{ll}/k$, then for any $m \in \mathbb{Z} \cap k^*$, $\mu_m \subset K(E[m])$, and there exists some $S, T \in E[m]$ s.t. $e_m(S,T)$ is a primitive m-th roots of unity. ⌟

Proof: If the subgroup generated by all $e_m(S,T)$ is μ_d, then $e_m([d]S,T) = 1$ for any $S,T \in E[m]$, so $[d]S = 0$ by non-degeneracy, so $d = m$ because $\#E[m] = (\mathbb{Z}/(m))^2$. Then the Gal_k-invariance of e shows $\mu_m \subset K(E[m])$. □

Prop. (15.7.7.12) [Duality with Isogenies]. Let $k \in \texttt{Field}$ and $\varphi : E_1 \to E_2 \in \mathrm{Isog}_k^1$, $m \in \mathbb{Z} \in k^*$, then for $S \in E_1[m], T \in E_2[m]$,

$$e_m(S, \varphi^\vee(T)) = e_m(\varphi(S), T).$$

In particular, for $S \in T_\ell(E_1)$ and $T \in T_\ell(E_2)$, $e(S, \varphi^\vee(T)) = e(\varphi(S), T)$. ⌟

Proof: Cf.[Sil16]P97**?**. □

Prop. (15.7.7.13). Let $E \in \mathcal{E}\text{ll}/k$ and $\varphi \in \operatorname{End}(E), \varphi \in \operatorname{End}(E)$, $\ell \in \mathbf{P} \setminus \operatorname{char} k$, then $\det(\varphi_\ell) = \deg(\varphi), \operatorname{tr}(\varphi_\ell) = 1 + \deg(\varphi) - \deg(1-\varphi)$. ⌟

Proof: For any $v, v' \in T_\ell(E)$, use the Weil pairing:

$$e(v,v')^{\deg(\varphi)} = e([\deg(\varphi)]v, v') = e(\varphi_\ell v, \varphi_\ell v') = e(v,v')^{\det(\varphi_\ell)},$$

thus $\deg(\varphi) = \det(\varphi_\ell)$. The latter equality follows from the identity $\operatorname{tr}(A) = 1 + \det(A) - \det(1-A)$ for any $A \in M_2(R)$. □

8 Over Archimedean Local Fields

Prop. (15.7.8.1) [Complex Abelian Varieties and Complex Tori]. By(12.9.5.9) and GAGA(12.8.7.17), $\mathcal{A}\text{b}\mathcal{V}\text{ar}/\mathbb{C}$ is the same as the category of complex tori V/Λ with a Riemann form $\omega : \wedge^2\Lambda \to \mathbb{Z}$(12.9.5.9).

Such a complex tori V/Λ is called a **polarizable integral Hodge structure**. ⌟

Def. (15.7.8.2) [Types of Polarizations]. Given a complex tori $X = V/\Lambda$ of dimension d with a Riemann form ω, there exists a basis of Λ and $d_1|d_2|\dots|d_n \in \mathbb{Z}_+$ s.t. the matrix ω w.r.t. this basis is

$$\begin{bmatrix} & D \\ -D & \end{bmatrix}, \quad D = \operatorname{diag}(d_1,\dots,d_n),$$

then X is said to have type D. ⌟

Prop. (15.7.8.3) [Abelian Varieties with Polarizations]. For $n \in \mathbb{Z}_+$ and $d_1|d_2|\dots|d_n \in \mathbb{Z}_+$, the set of polarized Abelian varieties over $\mathbb{C}$ of type $D = \operatorname{diag}(d_1,\dots,d_n)$ with a symplectic basis is in bijection with the set of $\operatorname{GL}(n,\mathbb{C})$ orbits of isomorphisms of real vector spaces $\Pi_\mathbb{R} : U_D \otimes \mathbb{R} \to \mathbb{C}^g$ s.t. for any $x, y \in V$,

$$(\Pi_\mathbb{R}^{-1}\,\mathrm{i}\,x, \Pi_\mathbb{R}^{-1}\,\mathrm{i}\,y)_D = (\Pi_\mathbb{R}^{-1}x, \Pi_\mathbb{R}^{-1}y)_D,$$

and the symmetric form

$$(x,y) \mapsto (\Pi_\mathbb{R}^{-1}\,\mathrm{i}\,x, \Pi_\mathbb{R}^{-1}y)_D$$

is positive definite.

And it is moreover canonical in bijection to the Siegel upper half space $\mathcal{H}_n$(12.13.6.6). ⌟

Proof: For any $X = V/U \in \mathcal{A}\text{b}\mathcal{V}\text{ar}^n/\mathbb{C}$ with a Riemann form ω of type D and a basis $\{u_1,\dots,u_n,v_1,\dots,v_n\}$ of U s.t. the matrix of ω is $\begin{bmatrix} & D \\ -D & \end{bmatrix}$. Then by choosing any complex basis $e_1,\dots,e_n$ of V, we get an isomorphism $U \otimes \mathbb{R} \cong \mathbb{C}^g$, and we can represent $\{u_i\}$ in the basis $\{e_i\}$ s.t.

$$(e_1,\dots,e_n,\mathrm{i}\,e_1,\dots,\mathrm{i}\,e_n) = \Pi_\mathbb{R}(u_1,\dots,u_n,v_1,\dots,v_n), \quad \Pi_\mathbb{R} = \begin{bmatrix} \Pi_{11} & \Pi_{12} \\ \Pi_{21} & \Pi_{22} \end{bmatrix} \in \operatorname{Mat}(2n,\mathbb{R}).$$

Then

$$(e_1,\dots,e_n)(\Pi_{11} + \mathrm{i}\,\Pi_{21}, \Pi_{21} + \mathrm{i}\,\Pi_{22})(u_1,\dots,u_{2n}),$$

and $\Pi = (\Pi_{11} + \mathrm{i}\,\Pi_{21}, \Pi_{21} + \mathrm{i}\,\Pi_{22})$ as in(12.9.5.11). Then the first assertion follows from(12.9.5.9). Notice the $\mathrm{GL}(n,\mathbb{C})$-orbit relation comes from the arbitrariness of the choice of basis $e_1,\dots,e_n$.

For the second assertion, notice that in each $\mathrm{GL}(n,\mathbb{C})$-orbit, there is a canonical choice of basis $\{e_1,\dots,e_n\}$ s.t. $e_i = \frac{1}{d_i}v_i$. Then in this basis,

$$\Pi_{\mathbb{R}} = \begin{bmatrix} \Pi_{11} & D \\ \Pi_{21} & 0 \end{bmatrix}, \quad \Pi = (\Pi_{11} + \mathrm{i}\,\Pi_{12}, D).$$

So if $Z = \Pi_{11} + \mathrm{i}\,\Pi_{12}$, the Riemann relations(12.9.5.11) are just equivalent to

$$\{Z^t = Z, \quad \mathrm{Im}(Z) \in \mathrm{Pos}(n,\mathbb{C})\}.$$

□

Cor. (15.7.8.4). For $n \in \mathbb{Z}_+$ and $d_1|d_2|\dots|d_n \in \mathbb{Z}_+$, the set of polarized Abelian varieties over $\mathbb{C}$ of type $D = \mathrm{diag}(d_1,\dots,d_n)$ with a symplectic basis is in bijection with the set of homomorphisms of real algebraic groups $h_1 : S_1 \to \mathrm{Sp}_{\mathbb{R}}(U_D)$ satisfying

- The complexification $h_{1,\mathbb{C}} : \mathbb{C}^\times \to \mathrm{Sp}_{\mathbb{R}}(U_D \otimes \mathbb{C})$ has weights ± 1 with multiplicities n.
- the symmetric form $(x,y) \mapsto (h_1(\mathrm{i})x, y)_D$ is positive definite.

⌟

Cor. (15.7.8.5) [Classifying Abelian Varieties with Polarizations]. It follows from(15.7.8.3) that for $n \in \mathbb{Z}_+$ and $d_1|d_2|\dots|d_n \in \mathbb{Z}_+$, the set of isomorphisms of Abelian varieties over $\mathbb{C}$ of type $D = \mathrm{diag}(d_1,\dots,d_n)$ with a symplectic basis is bijection with the set

$$\mathrm{Sp}_D(\mathbb{Z})\backslash\mathscr{H}_n.$$

⌟

Prop. (15.7.8.6) [Dual Riemann Forms]. If $X = V/\Lambda$ is a complex torus with a Riemann form ω, then the dual complex torus(12.9.5.8) $X^\vee$ also has a Riemann form defined as follows: any $f \in V^*$ corresponds to an element v_f s.t. $f(u) = \omega(u, v_f)$. Thus we can define $\omega'(f,g) = \omega(v_f, v_g)$. And there is an isogeny(i.e. surjective isomorphism with finite kernel)

$$A \to A^\vee : \overline{a} \mapsto [x \mapsto \omega(x,a)]$$

which is compatible with the Riemann forms. ⌟

Prop. (15.7.8.7) [Rosati Involutions are Positive]. Let $X = V/\Lambda \in \mathcal{A}b\,\mathcal{V}ar/\mathbb{C}$, then for any $\alpha \in \mathrm{End}_{\mathbb{Q}}(X)$, there exists $\alpha' \in \mathrm{End}_{\mathbb{Q}}(X)$ s.t.

$$\omega(\alpha x, y) = \omega(x, \alpha' y).$$

And this determines an involution on $\mathrm{End}_{\mathbb{Q}}(X)$, called the **Rosati involution**. Notice this is compatible with that defined in(15.7.7.4), by using(15.7.8.6).

Then this is a positive involution on $\mathrm{End}_{\mathbb{Q}}(X)$. ⌟

Proof: Notice the form $\omega_J : (x,y) \mapsto \omega(x, Jy)$ is symmetric and positive, and

$$\omega_J(\alpha x, y) = \omega(\alpha x, Jy) = \omega(x, \alpha' Jy) = \omega(x, J\alpha' y) = \omega_J(x, \alpha' y).$$

So this involution is positive by(15.8.2.19). □

Thm. (15.7.8.8) [Frobenius-Lefschetz-Poincaré-Riemann-Weierstrass]. The functor $A \mapsto H_1(A,\mathbb{Z})$ defines an equivalence from $\mathcal{A}b\,\mathcal{V}ar/\mathbb{C}$ to the category of polarizable integral Hodge structures of type $\{(-1,0),(0,-1)\}$. ⌟

Proof: ? □

Elliptic Curve Case

Prop. (15.7.8.9) [Complex Tori as Elliptic Curves]. Let Λ be a complete real lattice of $\mathbb{C}$, then we can make $\mathbb{C}/\Lambda$ into a Riemannian surface as the quotient space of $\mathbb{C}$. Then it is positive by**??**t is a smooth curve of genus 1 with the origin as the rational point, which means it is an elliptic curve. ⌟

Prop. (15.7.8.10) [Elliptic Curve as Complex Tori]. For an elliptic curve $\mathbb{C}/\Lambda$ over $\mathbb{C}$, by(11.5.4.7), the Weierstrass functions(11.5.4.5) $\mathfrak{P}, \mathfrak{P}'$ are just the rational functions in(15.11.1.7), so the map

$$z \mapsto [\mathfrak{P}(z), \mathfrak{P}'(z), 1]$$

is biholomorphic from $\mathbb{C}/\Lambda$ to the elliptic curve defined by the equation $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ that $g_2^3 - 27g_3^2 \neq 0$. And it also preserves the group structure. ⌟

Proof: To show that the homomorphism preserves group structure, notice that if z_1, z_2, z_3 maps to three points that is colinear, then they satisfy a equation

$$f(z) = a\mathfrak{P}(z) + b\mathfrak{P}'(z) + c.$$

If $b \neq 0$, then this is a meromorphic function with three poles, thus three zeros, which is exactly z_1, z_2, z_3, so by(11.5.4.2), $z_1 + z_2 + z_3 \equiv 0 \mod \Lambda$. If $b = 0$, then $z_3 = 0$, which corresponds to the point $(1, 0, 0) \in \mathbb{P}^2$, then the same argument shows $z_1 + z_2 + 0 \equiv 0 \mod \Lambda$. □

Lemma (15.7.8.11) [Isogenies and Homogeneities]. If E_1, E_2 are elliptic curves in $\mathbb{P}^2$ corresponding to Λ_1, Λ_2 via(15.7.8.10) resp., then the natural map

$$\{\text{isogenies } E_1 \to E_2\} \to \{\text{non-constant holomorphic maps } \varphi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2, \varphi(0) = 0\}$$

is a bijection. ⌟

Proof: By(12.9.5.2), it suffices to show for any lattices Λ_1, Λ_2 and $\alpha \in \mathbb{C}^*$ that $\alpha\Lambda_1 \subset \Lambda_2$, the map

$$[\mathfrak{P}(z, \Lambda_1), \mathfrak{P}'(z, \Lambda_1), 1] \to [\mathfrak{P}(\alpha z, \Lambda_2), \mathfrak{P}'(\alpha z, \Lambda_2), 1]$$

is a morphism. For this, notice $\mathfrak{P}(\alpha z, \Lambda_2)$ is an elliptic function for Λ_1, thus by(11.5.4.7), it is a rational function of $\mathfrak{P}(z, \Lambda_1)$ and $\mathfrak{P}'(z, \Lambda_1)$. □

Lemma (15.7.8.12). Let $E/\mathbb{C}$ be an elliptic curve in $\mathbb{P}^2$ defined by a Weierstrass equation, then there exists a lattice $\Lambda \subset \mathbb{C}$, unique up to homothety, that the embedding given in(15.7.8.10) induces an isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$. ⌟

Proof: This is a consequence of(11.5.4.8) and(15.11.1.14). □

Prop. (15.7.8.13) [Elliptic Curves and Complex Tori]. The following categories are equivalent:

- $\mathrm{Isog}^1/\mathbb{C}$.
- Category of complex tori with morphisms homomorphisms preserving 0.
- Category of lattices in $\mathbb{C}$ with homotheties as morphisms.

⌟

Proof: This is a consequence of(15.7.8.10)(15.7.8.11) and(12.9.5.2). □

Cor. (15.7.8.14) [j-Functions Correspond]. In this correspondence, If $E \cong E_\tau = \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$, then E is given by the by Weierstrass equation

$$W : y^2 = x^4 - \frac{g_2(\Gamma)}{4}x - \frac{g_3(\Gamma)}{4}.$$

Then

$$\Delta(W) = \Delta(\tau), \quad j(E) = j(\tau).$$

⌟

Proof: Comparing the definitions and use the definitions of $E_4, E_6, G_4, G_4, g_2, g_3$(20.2.4.5)(11.5.4.7), we get

$$g_2 = 60G_4 = 120\zeta(4)E_4 = \frac{4}{3}\pi^4 E_4 (21.7.4.1),$$

$$g_3 = 140G_6 = 280\zeta(4)E_6 = \frac{8}{27}\pi^4 E_6 (21.7.4.1).$$

So by(15.11.1.6),

$$j(W) = j(\tau) = 1728\frac{E_4(\tau)^3}{E_4^3(\tau) - E_6^2(\tau)}.$$

And for Δ, because $\Delta(\tau) = (2\pi)^{12}E_4^3(\tau)/j(\tau)$ and $\Delta(W) = c_4^3/j(\tau)$(15.11.1.5), it suffices to show that $c_4 = (2\pi)^4 E_4$. But

$$c_4 = 48g_2 = (2\pi)^4 E_4.$$

□

Prop. (15.7.8.15). Let $E/\mathbb{C}$ be an elliptic curve and Λ a lattice in $\mathbb{C}$ that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, then

- there is a natural isomorphism $H_1(E(\mathbb{C}), \mathbb{Z}) \cong \Lambda : \gamma \mapsto \int_\gamma dz$.
- There is a natural isomorphism $H_1(E(\mathbb{C}), \mathbb{Z}/(m)) \cong E[m]$.

⌟

Proof: Cf.[Sil16]P176. □

Over $\mathbb{R}$

Prop. (15.7.8.16). Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{R}$, then there exists a unique τ in the set

$$\mathcal{C} = \{\mathrm{i}\, t | t \geq 1\} \cup \{e^{\mathrm{i}\,\theta} | \pi/3 \leq \pi/2\} \cup \{1/2 + \mathrm{i}\, t | t \geq \sqrt{3}/2\}.$$

s.t. $j(\tau) = j(E)$. And by(15.11.6.3), each $\tau \in \mathcal{C}$ corresponds to exactly two isomorphism classes of elliptic curves over $\mathbb{R}$. ⌟

Proof: Firstly these τ satisfies $j(\tau) \in \mathbb{R}$ because by the power expansions of $j(\tau)$(20.2.4.22), for $\tau = it$ or $1/2 + it$, $q \in \mathbb{R}$, thus $j(\tau) \in \mathbb{R}$. For $\tau = e^{i\theta}$, $\overline{j(e^{i\theta})} = j(-e^{-i\theta}) = j(e^{i\theta})$ as $j \in M_0(\Gamma(1))$.

Next it can be proven $j(i\infty) = +\infty$ and $j(1/2 + i\infty) = -\infty$, and j is injective on $\mathcal{C}$ by(20.2.4.22). Thus the assertion follows by continuity. □

Remark (15.7.8.17). Notice by action of $\alpha = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ on $\{e^{i\theta} | \pi/3 \leq \pi/2\}$, we can also replace $\mathcal{C}$ by

$$\mathcal{C}' = \{\mathrm{i}\, t | t \geq 1\} \cup \{1/2 + \mathrm{i}\, t | t > 1/2\}.$$

⌟

9 char $k > 0$ Case

Prop. (15.7.9.1) [Finiteness over Finite Fields]. If $k \in \texttt{Field}, \#k < \infty$, then for any $g \in \mathbb{Z}_+$, $\# \mathcal{A}b\,\mathcal{V}ar^g/k < \infty$. ⌟

Proof: Firstly we show for A principally polarized by an ample line bundle $\mathcal{L}$. Then $\chi(\mathcal{L}) = 1$ by(15.7.5.2), and $\mathcal{L}^{\otimes 3}$ is very ample by(15.7.5.8), so it embeds A as a variety of degree $3^g.g!$ in $\mathbb{P}3^g - 1$ by(15.7.5.2). Such a variety is determined by its Chow form, which is a homogenous polynomial of degree $3^g.g!.d$ in each of $g+1$ sets of 3^g variables**?**. And the number of such polynomials are finite.

The general case can be reduced to the principal polarized case by Zarhin's trick(15.7.7.2). □

Prop. (15.7.9.2). Let $p \in \mathbf{P}, q \in p^{\mathbb{Z}}$, and $(A, \lambda) \in \mathcal{A}b\,\mathcal{V}ar^{\text{polar}}/\mathbb{F}_q$ with Rosati involution $\dagger$, then

$$\text{Frob}_{q,A}^{\dagger} \circ \text{Frob}_{q,A} = [q].$$

⌟

Proof: Cf.[Mil08]P76.**?** □

Honda-Tate Theory

References are [Tat66] and [Hon68].

Prop. (15.7.9.3)[Weil Conjecture for Abelian Varieties]. For $p \in \mathbf{P}, r \in \mathbb{Z}_+, q = p^r, \ell \in \mathbf{P} \backslash \ell$, and $A \in \mathcal{A}b\,\mathcal{V}ar^g/\mathbb{F}_q$, let $\varphi_A = \varphi^r$ be the Frobenius of A, and let $P_\varphi(X)$ be the characteristic polynomial of the action of φ_A on $T_\ell(A)$, then

- $P_{A,\ell}(X) \in \mathbb{Z}[X]$, and is invariant of ℓ chosen. Thus we omit ℓ from now on.
- $P_A(X) = \prod_{i=1}^{2g}(X - \alpha_i)$, where $\alpha_i \in \mathbb{C}$ and $|\alpha_i| = q^{1/2}$.
- $\#A(\mathbb{F}_{q^m}) = \prod_{i=1}^{2g}(1 - \alpha_i^m)$.

In particular,

$$|\#A(\mathbb{F}_{q^m}) - q^{mg}| \leq 2gq^{m-\frac{1}{2}} + (4^g - 2g - 1)q^{m(g-1)}.$$

⌟

Proof: These follow from(15.7.6.17) and Weil conjecture(17.2.2.6)(21.2.3.5). □

Thm. (15.7.9.4)[Tate]. For $k \in \texttt{Field}^{\text{fin}}, \ell \in \mathbf{P} \setminus \{\text{char}\, k\}$ and $A \in \mathcal{A}b\,\mathcal{V}ar/k$, the homomorphism

$$\text{End}_k(A) \to \text{End}_{\varphi_A}(V_\ell(A))$$

is an isomorphism. ⌟

Proof: **?** □

Thm. (15.7.9.5)[Honda-Tate]. For $p \in \mathbf{P}, q \in p^{\mathbb{Z}_+}$ and $A \in \mathcal{A}b\,\mathcal{V}ar^g/\mathbb{F}_q$ simple, by(15.7.9.3), for any embedding $\mathbb{Q}(\varphi_A) \hookrightarrow \mathbb{C}$, $\iota(\alpha)$ is a Weil q-number(14.4.1.13), and we get a map of sets

$$A \mapsto [\varphi_A] : \{\text{simple Abelian varieties}/\mathbb{F}_q\}/(\sim \text{isogenies}) \to \text{Weil}(q^{1/2})/(\sim \text{conjugations}).$$

Then this is a bijection. ⌟

Proof: The injectivity follows from(15.13.2.5) and the irreducibility of the action of φ_A on $V_\ell(A)$**?**, and the surjectivity is proven by Honda**??**(or [Chai-Oort]). □

Cor. (15.7.9.6). For $k \in \texttt{Field}^{\text{fin}}, \ell \in \mathbf{P} \setminus \{\text{char}\, k\}$, two Abelian varieties $A, B \in \mathcal{A}b\mathcal{V}ar^g/k$ are isogenous iff $\det(\varphi_A|H^1(A_{\overline{k}}, \mathbb{Q}_\ell)) = \det(\varphi_B|H^1(B_{\overline{k}}, \mathbb{Q}_\ell))$. ⌟

Proof: **?** □

Thm. (15.7.9.7)[Description of $\mathrm{End}(A)_\mathbb{Q}$ in terms of φ_A]. For $p \in \mathbf{P}, q \in p^{\mathbb{Z}_+}$ and $A \in \mathcal{A}b\mathcal{V}ar^g/\mathbb{F}_q$ be simple, let $D = \mathrm{End}(A)_\mathbb{Q}, \varpi = \varphi_A \in D$, then

- D is a central division ring over $\mathbb{Q}(\varpi)$.
- For any $v \in \Sigma_{\mathbb{Q}(\varpi)}$, $\mathrm{inv}_v(D) = \frac{\mathrm{ord}_v(\varpi)}{\mathrm{ord}_v(q)}[\mathbb{Q}(\varpi)_v : \mathbb{Q}_p] \in \mathbb{Q}/\mathbb{Z}$. In particular, for $v \notin \Sigma^{p\infty}_{\mathbb{Q}(\varpi)}$, $\in_v (D) = 0$.
- $[D : \mathbb{Q}]_{\mathrm{red}} = 2 \dim A$.

⌟

Proof: Cf.[Tat66] or [Waterhouse and Milne, 1971].**?** □

10 Jacobians of Curves

Prop. (15.7.10.1)[Picard Schemes of Curves]. Let C be a smooth complete precurve over a field k of genus g with a rational point, then

- $\underline{\mathrm{Pic}}_{C/k}$ is representable by a disjoint union of smooth complete varieties $\underline{\mathrm{Pic}}^d_{C/k}, d \in \mathbb{Z}$ where $\underline{\mathrm{Pic}}^d_{C/k}$ corresponds to relative line bundles of degree d.
- $\underline{\mathrm{Pic}}^0_{C/k}$ is an Abelian variety over k.
- for $d \geq 0$, the Abel map $\mathrm{Div}^d_{C/k} \to \underline{\mathrm{Pic}}^d_{C/k}$ is surjective for $d \geq g$ and smooth for $d \geq 2g - 1$.
- The morphism $\mathrm{Div}^g_{C/k} \to \underline{\mathrm{Pic}}^g_{C/k}$ is birational.

⌟

Proof: Cf.[Sta]0BA0 or [Neron Models] or(15.7.10.2)**?**. item1 follows from(8.1.12.5) □

Prop. (15.7.10.2)[Picard Scheme of Relative Curves]. If X/S is locally projective, flat with fibers all curves, $m \in \mathbb{Z}$, let $\underline{\mathrm{Pic}}^m_{X/S}$ denote the subfunctor of $\underline{\mathrm{Pic}}_{X/S}$ representing invertible sheaves $\mathcal{L}$ with $\deg(\mathcal{L}) = m$, then

- $\underline{\mathrm{Pic}}^m_{X/S}$ are clopen subschemes of $\underline{\mathrm{Pic}}_{X/S}$ of f.t. and form a disjoint cover of it, and forming it commutes with base change.
- $\underline{\mathrm{Pic}}^{(0)}_{X/S} = \underline{\mathrm{Pic}}^0_{X/S} = \underline{\mathrm{Pic}}^\tau_{X/S}$, and each $\underline{\mathrm{Pic}}^m_{X/S}$ is a fppf-torsor under $\underline{\mathrm{Pic}}^0_{X/S}$.
- If X/S is projective and S is Noetherian, then each $\underline{\mathrm{Pic}}^m_{X/S}$ is quasi-projective over S.

⌟

Proof: Cf.[Kle05]P60.**?** □

Def. (15.7.10.3)[Jacobians of Curves]. For a smooth complete precurve over a field k, its **Jacobian variety** $\mathrm{Jac}(C)$ is just its Picard variety $\underline{\mathrm{Pic}}^0_{C/k}$(15.7.10.1). ⌟

Cor. (15.7.10.4). For a smooth complete precurve C over a field with a rational point, $x \in \mathrm{Pic}_{C/k}$ is in $\mathrm{Jac}(C)$ iff the corresponding line bundle x on $C_{k(x)}$ has degree 0, by(15.7.10.1). ⌟

Prop. (15.7.10.5). If C is a smooth complete curve of dimension g, then $\mathrm{Jac}(C)$ has dimension g, by(9.7.2.24) and(9.7.2.22). ⌟

Def. (15.7.10.6)[Symmetric Product]. Let C be a smooth curve, then the symmetric product $C^{(r)} = C^r/S_r$ is a smooth variety of dimension r by considering the symmetric functions. ⌟

Prop. (15.7.10.7) [Generic Riemann-Roch]. ⌟

Prop. (15.7.10.8) [Polarization of Jacobians]. ⌟

Prop. (15.7.10.9) [Push and Pull]. For a non-constant morphism $\varphi : C_1 \to C_2$ of pointed smooth curves over k, the push and pull induce maps

$$\varphi_* : \mathrm{Jac}(C_1) \to \mathrm{Jac}(C_2), \quad \varphi^* : \mathrm{Jac}(C_2) \to \mathrm{Jac}(C_1).$$

s.t. $\varphi_* \circ \varphi^* = [\deg(\varphi)]$. ⌟

Proof:

□

Prop. (15.7.10.10) [Abel-Jacobi]. Let X be a smooth curve over $\mathbb{C}$ with a rational point x_0, then $\mathrm{Jac}(C)$ is isomorphic to $\Omega^1_{\mathrm{hol}}(X)^\vee/H_1(X,\mathbb{Z})$ as complex manifolds via

$$\mathcal{L}(\sum_x n_x x) \mapsto \sum_x n_x \int_{x_0}^x .$$

⌟

Proof: □

Prop. (15.7.10.11). Let $k \in \mathtt{Field}$, C be a smooth complete curve over k, $P \in C(k)$, then for any $\ell \in \mathbf{P}$, the map $f_P : C \to \mathrm{Jac}(C)$ induce isomorphisms

$$H^1(\mathrm{Jac}(C), \mathcal{O}_{\mathrm{Jac}(C)}) \cong H^1(C, \mathcal{O}_C), \quad H^1(\mathrm{Jac}(C), \mathbb{Z}_\ell) \cong H^1(C, \mathbb{Z}_\ell).$$

⌟

Proof: Cf.[Mil08]P114. □

Prop. (15.7.10.12) [Surjection by Jacobians]. Let $k \in \mathtt{Field}$ and $A \in \mathcal{A}b\mathcal{V}ar/k$, there exists a smooth complete curve C over k and a surjection $\mathrm{Jac}(C) \to A$. ⌟

Proof: We only prove for $\#k = \infty$. For k finite, Cf.[Gabber, On space filling curves and Albanese varieties], [Poonen, Bjorn, Bertini theorems over finite fields. Ann. of Math].?

Since elliptic curves are their own Jacobians, we can assume that $\dim A > 1$. Choose a projective embedding $A \to \mathbb{P}^n_k$, then by Bertini and the fact $\#k = \infty$, there is a hyperplane cut $A \cap H$ that is also a smooth complete k-variety. By repeating $\dim A - 1$ dimes, we get a k-curve C on A. This curve gives a map $\mathrm{Jac}(C) \to A$ by(15.7.10.8) and double duality(15.7.4.18). The image is an Abelian subvariety of A. If it is not the whole of A, then by Poincaré 's reducibility theorem(15.7.6.6), there exists another Abelian subvariety $A_2 \subset A$ s.t. $\mathrm{Jac}(C) \times A_2 \to A$ is an isogeny. In particular, $\mathrm{Jac}(C) \cap A_2$ is finite.

Using the embedding $C \subset \mathrm{Jac}(C)$, C is regarded as a subscheme of $\mathrm{Jac}(C)$. Take $n \in \mathbb{Z} \cap k^*$ large, the composition $\mathrm{Jac}(C) \times A_2 \xrightarrow{(1,n)} \mathrm{Jac}(C) \times A_2 \to A$ is finite, and the inverse image of C projects to $[n]^{-1}(A_1 \cap A_2) \subset A_2$, which is finite and disconnected. So the inverse image of C is not connected, which contradicts the fact it is an ample divisor by(6.5.4.12) and(6.8.6.25). □

Conj. (15.7.10.13) [Resolution Conjecture]. Let $k \in \texttt{Field}, k = \overline{k}$, and $A \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/k$, we can find a surjective homomorphism $J_1 \to A$ where J_1 is a Jacobian of a curve by(15.7.10.12). Then the identity component of the kernel is also an Abelian variety. Then we can do the same process again.
is it possible to choose the Jacobians s.t. the process terminate after finite steps? ⌟

Proof: □

Thm. (15.7.10.14) [Tonelli]. Let $k \in \texttt{Field}$ and $k = \overline{k}$, and $(C, P), (C', P')$ be pointed complete smooth curves over k. Let $f : C \to \mathrm{Jac}(C)$ and $f' : C' \to \mathrm{Jac}(C')$ be the maps corresponding to P, P'. Then if $\beta : (\mathrm{Jac}(C), \lambda) \cong (\mathrm{Jac}(C'), \lambda')$ is an isomorphism of polarized Jacobians, then

- There exists an isomorphism $\alpha : C \to C'$ s.t. $f' \circ \alpha = \pm\beta \circ f + c$ for some $c \in \mathrm{Jac}(C')(k)$.
- If $g(C) \geq 2$ and C is non-hyperelliptic, then $\alpha, \pm 1, c$ are determined by β, P, P'. And if $g(C) \geq 2$, then ± 1 can be arbitrary, and α, c is determined by $\beta, \pm 1, P, P'$.

⌟

Proof: Cf.[Mil08]P120. □

Cor. (15.7.10.15).

- If $k \in \texttt{Field}, C, C'$ are complete smooth curves over k with rational points s.t. their polarized Jacobians are isomorphic, then C, C' are isomorphic over k.
- If $k \in \texttt{Field}$ is perfect, C, C' are complete smooth curves of genus≥ 2 over k, then if their polarized Jacobians are isomorphic, then C, C' are also isomorphic over k.

⌟

Proof: Let $\beta : (\mathrm{Jac}(C), \lambda) \cong (\mathrm{Jac}(C'), \lambda')$ is an isomorphism, for any $P \in C(\overline{k}), P' \in C'(\overline{k})$, there is a unique isomorphism $\alpha : C_{\overline{k}} \cong C'_{\overline{k}}$ s.t. $f^{P'} \circ \alpha = \pm\beta \circ f^P + c$, and if C is hyperelliptic, take $\pm = +$. Then if Q, Q' are different points, $f^P = f^Q + d$, $f^{Q'} = f^{P'} + e$ for some $d \in \mathrm{Jac}(C)(\overline{k}), e \in \mathrm{Jac}(C')(\overline{k})$. So α is invariant of the points P, P' chosen. In particular,

$$f^{\sigma(P')} \circ \alpha = \sigma(f^{P'}) \circ \alpha = \pm\beta \circ \sigma(f^P) + \sigma(c) = \pm\beta f^{\sigma(P)} + \sigma(c).$$

for any $\sigma \in \mathrm{Gal}_k$. So α is invariant under Gal_k, which means C, C' are isomorphic over k. □

Arithmetics

Prop. (15.7.10.16). If $F \in \texttt{GField}$ and C is a complete smooth curve over F with good reduction at a place P of F, then $\mathrm{Jac}(C)$ has good reduction at P. ⌟

Proof: The hypothesis implies C extends to a smooth proper curve $\mathcal{C}$ over $\operatorname{Spec} R_P$. Then the Picard scheme $\mathcal{J}$ of $\mathcal{C}/\operatorname{Spec} R_P$(15.7.10.2) has generic fiber $\mathrm{Jac}(C)$, which implies $\mathrm{Jac}(C)$ has good reduction at P. □

11 Néron Models

Main references are [Serre/Tate, Good Reduction of Abelian Varieties], [BLR90] and http://virtualmath1.stanford.edu/~conrad/mordellsem/Notes/L11.pdf.

Def. (15.7.11.1) [Néron Models]. Let (S, K) be a Dedekind scheme and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{sm,sep,ft}}/K$, then a **Néron model** for X is a smooth scheme $\mathcal{X} \in \mathcal{S}\mathrm{ch}^{\mathrm{sm,sep,ft}}/S$ representing the functor

$$\mathcal{S}\mathrm{ch}^{\mathrm{sm}}/S \to \mathcal{S}\mathrm{et} : \mathcal{Y} \mapsto \mathrm{Hom}_K(\mathcal{Y} \otimes_S K, X).$$

In particular, the natural map $\mathcal{X}(R) \to X(K)$ is a bijection. ⌟

Cor. (15.7.11.2) [Group Structures]. Let (S, K) be a Dedekind scheme and $X \in \mathcal{G}\mathrm{rp}^{\mathrm{sm,sep,ft}}/K$, then any Néron model for X is naturally equipped with a group structure extending that of X. ⌟

Proof: This follows from the universal properties. □

Prop. (15.7.11.3) [Étale Valuation Criterion for Group Schemes]. Let (R, K) be a DVR and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{sm,sep,ft}}/K$, then if $\mathcal{X}/R$ is a Néron model for X, then $\mathcal{X}$ satisfies valuation criterion for any R' that is the integral closure of R in an unramified field extension K'/K.

Conversely, if X is a group scheme over K, then the converse is also true: If $\mathcal{G}$ is a smooth R-group scheme of f.t., then $\mathcal{G}$ is a Néron model of its generic fiber iff the natural map $\mathcal{G}(R^{\mathrm{sH}}) \to \mathcal{G}(K^{\mathrm{sH}})$ is an isomorphism. ⌟

Proof: Cf.[BLR90]Prop. 7.1.1. □

Prop. (15.7.11.4) [Étale Base Change]. Let (R, K) be a Dedekind domain and ⌟

Proof: □

Prop. (15.7.11.5) [Unramified Base Change]. Let (R, K) be a DVR and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{sm,sep,ft}}/K$, K'/K an unramified field extension, R' the integral closure of R in K', then if $\mathcal{X}$ is a Néron model for X, then $\mathcal{X}_{R'}$ is a Néron-model for $X_{K'}$. ⌟

Proof: Because R'/R is smooth(by(6.6.4.6) and the definition of unramifiedness(14.2.2.4)), for any $\mathcal{Y}'/R'$ smooth,

$$\mathrm{Mor}_{R'}(\mathcal{Y}', \mathcal{X}_{R'}) = \mathrm{Mor}_R(\mathcal{Y}', \mathcal{X}) = \mathrm{Mor}_K(\mathcal{Y}'_K, X) = \mathrm{Mor}_{K'}(\mathcal{Y}'_{K'}, X_{K'}).$$

□

Prop. (15.7.11.6) [Étale Descent]. Let $(R, K) \subset (R', K') \subset (R^{\mathrm{sH}}, K^{\mathrm{sH}})$ be DVRs. If G is a smooth group scheme of f.t. over K s.t. $G_{K'}$ has a Néron model $\mathcal{G}'/R'$, then $\mathcal{G}'$ descends to a Néron model $\mathcal{G}/R$ of G. ⌟

Proof: Cf.[BLR90]Prop. 6.5.4. □

Cor. (15.7.11.7). Let $(R, K) \subset (R', K')$ be an unramified extension of DVRs, and $G \in \mathcal{G}\mathrm{rp}^{\mathrm{sm,ft}}/K$, then G has a Néron model iff $G_{K'}$ has a Néron model. ⌟

Proof: Cf.[BLR90]Prop. 6.5.4. □

Prop. (15.7.11.8) [Localness of Néron Property]. Let (S, K) be a Dedekind scheme and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{sm,sep,ft}}/K$.

- If (S_i) is an open cover of S, then X has a Néron model over S iff it has a Néron model over each S_i.
- $\mathcal{X} \in \mathcal{S}\mathrm{ch}^{\mathrm{ft,sep}}/S$ is a Néron model for X iff for each closed point $s \in S$, $\mathcal{X} \times_S \operatorname{Spec} \mathcal{O}_{S,s}$ is a Néron model for X over $\mathcal{O}_{S,s}$.

⌟

Proof: 1: One direction follows from(15.7.11.4), for the other, notice they can be glued by universal properties.

2: Cf.[BLR, Prop1.2.4]. If $\mathcal{X}/S$ is a Néron model, then for any closed point $s \in S$ and any $\varphi : \mathcal{Y}_{(s)} \in \mathcal{S}\mathrm{ch}^{\mathrm{sm}}/\mathcal{O}_{S,s}$ with a morphism $Y_{(s),K} \to X$, we need to show that it can be extended uniquely to a morphism over $\mathcal{O}_{S,s}$. We may assume that $Y_{(s)}$ is f.p., and then it extends to a scheme Y/S' on a nbhd S' of s. Then because X/S_i is a Néron model by item1, we can extend the φ over S', which restricts to a morphism over $\mathcal{O}_{S,s}$. The uniqueness is clear.

The converse is similar. Just notice that smoothness is a stalkwise properties(6.6.4.5). □

Prop. (15.7.11.9) [Extending Néron Models]. Let (S,K) be a Dedekind scheme and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{sm,sep,ft}}/K$, then X has a Néron model over S iff there exists an open dense subscheme $S' \subset S$ s.t. X has a Néron model over S, and for any $s \in S \setminus S'$, X has a Néron model over $\mathcal{O}_{S,s}$. ⌟

Proof: One direction is obvious**?**, for the other, for each $s_i \in S \setminus S'$, $\mathcal{X}_i/\mathcal{O}_{S,s_i}$ extends to smooth scheme on a nbhd S_i of s_i, and since $\mathcal{X}_i$ and $\mathcal{X}/S'$ has isomorphic generic fibers, we can assume that they are isomorphic on $S_i \cap S'$ after shrinking S_i. Then the glue together to a Néron model over $\mathcal{O}_{S,s}$. Then the assertion follows from(15.7.11.8). □

Cor. (15.7.11.10) [Néron Differentials]. Let (S,K) be a Dedekind scheme and $E \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/S$ with Néron model $\mathcal{A}/S$, then $\mathcal{K}_{\mathcal{E}/S}$ is free of rank 1. A generator of it is called a **Néron differential** of E. It is defined up to units on S. ⌟

Néron Models for Abelian Varieties

Prop. (15.7.11.11) [Néron Model for Abelian Varieties]. Let $K \in$ `Field` and A be any ring of integers in the field K, and $X \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/K$. Then there exists an open subset $Y = \operatorname{Spec} A_S \subset \operatorname{Spec} A$, and a scheme $\widetilde{X}$ projective over Y, and morphisms $\widetilde{m}: \widetilde{X} \times \widetilde{X} \to \widetilde{X}$ over Y and $\widetilde{e}: Y \to X$ that:

- The fiber of $\widetilde{X}$ over a generic point of Y with the morphisms $\widetilde{m}, \widetilde{e}$ are Abelian varieties isomorphic to X.
- $\widetilde{X}$ is a group scheme over Y, and its fiber over any closed point of Y with the morphisms $\widetilde{m}, \widetilde{e}$ are Abelian varieties.
- The mapping in item1 induces an isomorphism of groups $\widetilde{X}(Y) \cong X(K)$.

⌟

Proof: 1: Consider for any qc scheme over a field K, it is glued together from f.m. affine schemes, and these glueing involves f.m. polynomials and rational transition functions, and the coefficients of them are contained in a subring $A_S \subset K$ of f.t. over A. Thus this variety can be seen as a variety over A_S with the same equations, satisfying item1. The situation is similar for morphisms between qc schemes, in particular $\widetilde{m}$ and $\widetilde{e}$, thus constructing $\widetilde{X}$.

2: Cf.[Mumford, P265].**?**

3: Cf.[Mumford, P265].**?** □

Cor. (15.7.11.12). Let $x \in \widetilde{X}(Y)$, consider x as a closed subscheme of $\widetilde{X}$ and denote $n^{-1}(x)$ the closed subscheme in $\widetilde{X}$ the inverse image of x under the morphism $[n]_Y$. Then the natural projection $n^{-1}(x) \to Y$ is étale over all points $y \in Y$ that $\operatorname{char} k(y) \nmid n$. ⌟

Proof: [Mumford, P265].**?** □

Thm. (15.7.11.13) [Good Reduction of Abelian Varieties]. Let (S,K) be a Dedekind scheme, $A \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/K$ and $\mathcal{A} \in \mathcal{S}\mathrm{ch}/S$ is proper smooth with generic fiber A, then the group structure extends to $\mathcal{A}$, making it a Néron model of A. ⌟

Proof: Cf.[BLR90]P19 or [L11, Neron Model]P8.**?**

By(15.7.11.8), we may assume that S is local. □

Thm. (15.7.11.14) [Néron Model of Abelian Varieties]. Let (S, K) be a Dedekind scheme and $A \in \mathcal{A}b\mathcal{V}ar/K$, then A has a Néron model $\mathcal{A}/S$. Moreover, let $S' \subset S$ be the set of good points for A, then $\mathcal{A}_{S'} \in \mathcal{A}b\mathcal{V}ar/S'$. ⌟

Proof: We show that A extends to an Abelian scheme over a nbhd of each good point of S for A. This will suffice combining with(15.7.11.13)(15.7.11.18)(15.7.11.8) and(15.7.11.9).

By hypothesis, A extends to a smooth proper scheme $A_{(s)}$ over $\mathcal{O}_{S,s}$, and then we can extend it to a scheme of f.t. over a nbhd of s. By shrinking if necessary, we can assume it is smooth and proper, by(6.8.4.6). □

Prop. (15.7.11.15) [Strong Néron Extension Property]. Let (S, K) be a Dedekind domain, and $A \in \mathcal{A}b\mathcal{V}ar/K$ with a Néron model $\mathcal{A}/S$, then for any $\mathcal{Y} \in \mathcal{S}ch^{\mathrm{sm}}/S$ and a rational map $\varphi : \mathcal{Y}_K \to A$, there exists uniquely an S-morphism $\mathcal{Y} \to \mathcal{A}$ extending φ. ⌟

Proof: This follows from(15.7.1.7). □

Def. (15.7.11.16) [Relative Identity Components]. Let (S, K) be a Dedekind scheme and $A \in \mathcal{A}b\mathcal{V}ar/K$ with Néron differential $\mathcal{A}/S$, the **relative identity component** $\mathcal{A}_0$ of $\mathcal{A}$ is defined to be the open subgroup of $\mathcal{A}$ deleting all non-identity components of $\mathcal{A}_{\kappa(P)}$ for any closed point $P \in S$.

Then $\mathcal{A}_0$ is a subgroup scheme of $\mathcal{A}$**?**. ⌟

Proof of the Existence of Néron Models for Abelian Varieties

Cf.[BLR]Chap3-6.

Remark (15.7.11.17). In this subsubsection, let $(\mathcal{O}_K, K, k)$ be a DVR. ⌟

Prop. (15.7.11.18) [Local Néron Models for Abelian Varieties]. (15.7.11.14) is true when S is a DVR. ⌟

Def. (15.7.11.19) [Weak Néron Models]. For $X \in \mathcal{S}ch^{\mathrm{sm,sep,ft}}/K$, a **weak Néron model** for X is a family $(X_i) \in \mathcal{S}ch^{\mathrm{sm,sep,ft}}/R$ s.t. each K^{sH}-point of X extends to a R^{sH}-point of some X_i. ⌟

Thm. (15.7.11.20). For $X \in \mathcal{S}ch^{\mathrm{sm,sep,ft}}/K$, if $X(K^{\mathrm{sH}})$ is bounded in X, then there exists a weak Néron model for X. ⌟

Proof: Cf.[BLR90]P74. □

Prop. (15.7.11.21) [Weak Néron Property]. Let $X \in \mathcal{S}ch^{\mathrm{sm,sep,ft}}/K$ and (X_i) is a weak Néron model for X. If $Z \in \mathcal{S}ch^{\mathrm{sm}}/\mathcal{O}_K$ s.t. Z_k is irreducible, then any rational map $Z_k \to X_k$ extends to a rational map $Z \to X_i$ over R for some i. ⌟

Proof: Cf.[BLR90]P74. □

Properties of Néron Models

Prop. (15.7.11.22). If $(\mathcal{O}_K, K)$ is a DVR, then for $\mathcal{G} \in \mathcal{G}\mathrm{rp}^{\mathrm{sm,ft}}/\mathcal{O}_K$, the following are equivalent:

- $\mathcal{G}$ is a Néron model of its generic fiber.
- $\mathcal{G}(\mathcal{O}_K^{\mathrm{sH}}) \to \mathcal{G}(K^{\mathrm{sH}})$ is an isomorphism.
- $\mathcal{G}$ is separated and $\mathcal{G}(\mathcal{O}_K^{\mathrm{sH}}) \to \mathcal{G}(K^{\mathrm{sH}})$ is surjective.

⌟

Proof: $1 \to 2$ is trivial. $2 \to 3$ is valuation criterion. $2 \to 1$ follows from Weil's Extension Theorem and Weak Néron Property.

For $3 \to 2$:Cf.[BLR]7.1.1.? □

Prop. (15.7.11.23). If R has mixed characteristic $(0,p)$ and absolute ramification $e < p-1$, $0 \to A' \to A \to A'' \to 0 \in \mathcal{A}b\mathcal{V}\mathrm{ar}/K$ is an exact sequence, and A has good reduction, then the sequence of Néron models

$$0 \to \mathcal{A}' \to \mathcal{A} \to \mathcal{A}'' \to 0$$

is exact. ⌟

Proof: Cf.[BLR]Prop7.5.4. □

12 Reductions

Cf.[L13, Semistable Reductions for Abelian Varieties].

over DVRs

Prop. (15.7.12.1) [Reduction Types of Abelian Varieties]. Let $(\mathcal{O}_K, K, k)$ be a DVR and $A \in \mathcal{A}b\mathcal{V}\mathrm{ar}/K$ with a Néron model $\mathcal{A}/\mathcal{O}_K$(15.7.11.14), let $\widetilde{A}$ be the special fiber, then by(15.7.1.18), there exists a filtration of subgroups

$$\mathcal{A}_k \supset \mathcal{A}_k^0 \supset \mathcal{A}_k^1$$

where $\mathcal{A}_k^0$ is the identity component of $\mathcal{A}_k$, and $\mathcal{A}_k^1$ is affine commutative s.t. $\widetilde{A}^0/\widetilde{A}^1 \in \mathcal{A}b\mathcal{V}\mathrm{ar}/k$. Then A is said to have

- **good reduction** if $\mathcal{A}_k \in \mathcal{A}b\mathcal{V}\mathrm{ar}/k$. This is compatible with the definition as in(15.10.1.2) by(6.6.4.6).
- **semistable reduction** if $\widetilde{A}^1$ is a torus.
- **bad reduction** if $\widetilde{A}^1$ contains a copies of $\mathbb{A}^1$.

There are not other possibilities(?, Cf.[Milne]Chap 15). ⌟

Def. (15.7.12.2) [Tamagawa Numbers]. Let $(\mathcal{O}_K, K, k)$ be a DVR and $A \in \mathcal{A}b\mathcal{V}\mathrm{ar}/K$ with Néron model $\mathcal{A}/\mathcal{O}_K$, define the **component group of** A to be $\pi_0(\mathcal{A}_k)$, denoted by $\Phi(A)$. And $\#\Phi(A) < \infty$ is called the **Tamagawa number** of A.

Then $c(A)$ equals the number of geo.connected components of $\mathcal{A}_k$. And if k is finite, it also equals the connected components of $\mathcal{A}_k$ with a rational point. ⌟

Proof: Cf.[Liu Qing, 10.2.21(a)]. □

Def. (15.7.12.3) [Local Conductor]. Let $E \in \mathcal{E}\mathrm{ll}/F$, then the **conductor of** E is defined in [Sil99]P380.**?**

If $F = \mathbb{Q}$, then the conductor $N_E = \prod_{p \in \mathbf{P}} p^{f_p}$, where

$$f_p = \begin{cases} 0, & E \text{ has good reduction at } p \\ 1, & E \text{ has multiplicative reduction at } p \\ 2, & E \text{ has additive reduction at } p \ \& \ p \neq 2,3 \\ 2+\delta_p, & E \text{ has additive reduction at } p \ \& \ p = 2,3 \end{cases}$$

where $0 \le \delta_2 \le 6, 0 \le \delta_2 \le 3$. ⌟

Proof: □

Thm. (15.7.12.4) [Semistable Reduction Theorem]. Let (R, K, k) be a DVR, K'/K a finite extension, and R' the alg.closure of R in K. Let $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/K$, then:

- If A has stable or semistable reduction, then the reduction type of $A_{K'}$ is the same as that of E.
- If K'/K is unramified, then the reduction type of $A_{K'}$ is the same as that of E.
- There exists such a finite extension K'/K s.t. $A_{K'}$ is of stable or split semistable reduction type.

⌟

Proof: We only prove for elliptic curves.**?**

1: For these two cases, c_4 and Δ cannot be reduced anymore to another minimal Weierstrass equation by(15.11.4.5).

2: It suffices to consider the additive reduction case: **?** The short Weierstrass equation case is clear, for the general case, use Tate's algorithm.

3: Use the Legendre or Deuring form(15.11.1.17)(15.11.1.18) to analyze Δ and c_4. □

Thm. (15.7.12.5) [Néron-Ogg-Shafarevich Criterion]. Let (R, K, k) be a DVR and $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/K$, $\ell \in \mathbf{P} \setminus \operatorname{char} k$, then the following are equivalent:

- A has good reduction.
- The module $A[m](K^s)$ is unramified as a Gal_K-module, for all $m \in \mathbb{Z} \setminus \operatorname{char} k$.
- The Tate module $T_\ell(A)$ is unramified for all(some) primes $\ell \in \mathbf{P} \setminus \operatorname{char} k$.
- The module $A[m]$ is unramified for infinitely many $m \in \mathbb{Z} \setminus \operatorname{char} k$.

⌟

Proof: $2 \to 3 \to 4$ are obvious.

For the rest, Cf.`http://virtualmath1.stanford.edu/~conrad/mordellsem/Notes/L11.pdf`P20 or [Mil08]P141.**?**

$1 \to 2$: Let K' be the finite extension of K generated by $E[m]$, then (15.7.12.4) implies $E_{K'}$ has the same reduction type as E. Then by(15.11.4.19), $E[m] \to \widetilde{E}_{K'}(k')$ is an injection. So clearly I_v acts trivially on $E[m]$.

$4 \to 1$: Let $m \in \mathbb{Z} \setminus \operatorname{char} k$ s.t. $E[m]$ is unramified and $m > \#E(K^{\mathrm{ur}})/E_0(K^{\mathrm{ur}})$, where $\#E(K^{\mathrm{ur}})/E_0(K^{\mathrm{ur}}) < \infty$ by(15.11.4.15). Then because $E[m] \cong (\mathbb{Z}/(m))^2 \subset E(K^{\mathrm{ur}})$, $E_0(K^{\mathrm{ur}})$ contains some subgroup isomorphic to $(\mathbb{Z}/(\ell))^2$ for some $\ell \in \mathbf{P} \setminus \operatorname{char} k$, thus by(15.11.4.19), $\widetilde{E}_{\mathrm{sm}}(\overline{k})$ contains some subgroup isomorphic to $(\mathbb{Z}/(\ell))^2$. But by(15.11.1.16), this is possible only when $\widetilde{E}_{\mathrm{sm}} = \widetilde{E}$. Thus $E_{K^{\mathrm{ur}}}$ has good reduction, so E also has good reduction by(15.7.12.4). □

Cor. (15.7.12.6). If $0 \to A' \to A \to A'' \to 0$ are exact sequences of Abelian varieties over K and A has good reduction, then A', A'' also have good reductions. ⌟

Cor. (15.7.12.7) [Isogeny and Good Reductions]. Let (R, K, k) be a DVR and $A \to A' \in \mathcal{A}b\mathcal{V}ar/K$ is an isogeny, then A has good reduction iff A' does. ⌟

Proof: Use(15.7.12.5) and the fact if $\ell \in \mathbf{P}$ is prime to $\operatorname{char} k$ and $\deg \varphi$, then $\varphi_\ell : T_\ell(A) \to T_\ell(A')$ is an isomorphism of Gal_K-modules. □

Prop. (15.7.12.8). If $K \in p$-`LField`, $\ell \in \mathbf{P}\backslash p$ and $A \in \mathcal{A}b\mathcal{V}ar/K$ satisfies $\rho_{\ell,A}(\mathrm{Gal}_K)$ has finite image, then A has potential good reduction. ⌟

Proof: It follows from class field theory that the image of I_K is a quotient of $\mathcal{O}_K^*$, which contains a pro-p-group of finite index, and $\mathrm{End}(T_\ell(A))$ contains a pro-ℓ-group of finite index, so the image is finite. Then A has potential good reduction by(15.7.12.5). □

Thm. (15.7.12.9) [Néron-Ogg-Shafarevich Criterion for Elliptic Curves]. Let K be a CDVR, $\ell \in \mathbf{P}\backslash\{\operatorname{char} k\}$ and $A \in \mathcal{A}b\mathcal{V}ar/K$, then

- A has good reduction iff $T_\ell(A)$ is an unramified Gal_K-module.
- A has good or semistable reduction iff I_K acts unipotently on $T_\ell(A)$.
- A has potential good reduction iff $T_\ell(E)$ is potentially unramified, i.e. $\rho_{\ell,A}(I_K)$ is finite.

⌟

Proof: 1 follows from(15.7.12.5).

2: We only prove for $\dim A = 1$ case**?**: As I_K acts trivially on $\det(T_\ell(E))$ by(18.3.4.3), it acts unipotently on $T_\ell(E)$ iff it has a fixed vector. If it has a fixed vector, then $\widetilde{E}_{\mathrm{sm}}(\overline{k})$ contains a subgroup isomorphic to $\mathbb{Z}/(\ell)$, which is possible only if E has semistable or good reduction, by(15.11.1.16) and(15.7.12.4). The converse is proved the same way as that of(15.7.12.5).

3 follows from(3.2.6.11). □

Cor. (15.7.12.10). If K is a CDVR with residue characteristic p and $\varphi : E \to E'$ is an isogeny of degree p of elliptic curves over K, then E has good reduction of ordinary type/supersingular type iff E' does. ⌟

Proof: By(15.7.12.7) we can assume both E, E' have good reductions, then their minimal Weierstrass equations are their Néron models, thus by definition φ extends to a map $\widetilde{\varphi} : \widetilde{E} \to \widetilde{E}'$. Let $\psi = \widehat{\varphi}$, then we also have $\widetilde{\psi} : \widetilde{E}' \to \widetilde{E}$ s.t. $\widetilde{\psi} \circ \widetilde{\varphi} = [p]_{\widetilde{E}}$, and $\widetilde{\varphi} \circ \widetilde{\psi} = [p]_{\widetilde{E}'}$. Thus $[p]_{\widetilde{E}'} \circ \widetilde{\varphi} = \widetilde{\varphi} \circ [p]_{\widetilde{E}}$, which implies $\deg_s([p]_{\widetilde{E}}) = \deg_s([p]_{\widetilde{E}'})$, thus we are done by(15.11.3.5). □

Prop. (15.7.12.11) [Isogeny and Semistability]. If $A, B \in \mathcal{A}b\mathcal{V}ar/k$ are isogenous, then A is semistable iff B is semistable. ⌟

Proof: **?** □

Good Reductions

Thm. (15.7.12.12) [Extending Abelian Variety Structures]. Let $S \in \mathcal{S}ch$ be Noetherian and connected, and $X \in \mathcal{S}m\mathcal{P}rpr/S$ with a section $e : S \to X$. If for some geometric point $s \in S$, $X_s \in \mathcal{A}b\mathcal{V}ar/\kappa(s)$ with unit point $e(s)$, then $X \in \mathcal{A}b\mathcal{V}ar/S$ with unit section e. ⌟

Proof: Cf.[Ngo, Shimura Varieties]P16. □

Prop. (15.7.12.13). Let $(\mathcal{O}_K, K, k)$ be a DVR, $A \in \mathcal{A}b\mathcal{V}ar/K$ with Néron model $\mathcal{A}/\mathcal{O}_K$, then the following are equivalent:

- $\mathcal{A}$ is an Abelian scheme.
- A has good reduction over $\mathcal{O}_K$.
- $\mathcal{A}_k^0$ is proper hence in $\mathcal{A}b\mathcal{V}ar/k$.

⌟

Proof: $1 \to 2, 2 \to 3$ is clear.

$3 \to 1$: By(6.11.5.3) $\mathcal{A}_0$(15.7.11.14) is an Abelian scheme, so $\mathcal{A}_0 = \mathcal{A}$ is the Néron model by(15.7.11.13). □

Prop. (15.7.12.14) [Exactness]. Let (R, K) be a DVR with mixed characteristic $(0, p)$ and ramification index $e < p - 1$. If $0 \to A' \to A \to A'' \to 0$ is an exact sequence in $\mathcal{A}b\mathcal{V}ar/K$, and A has good reduction, then so does A' and A'' by(15.7.12.5). Then the Néron models

$$0 \to \mathcal{A}' \to \mathcal{A} \to \mathcal{A}'' \to 0$$

for an exact sequence. ⌟

Proof: Cf.[BLR90]Prop7.5.4.. □

Prop. (15.7.12.15) [Extending Polarizations]. Let (R, K) be a DVR and $A \in \mathcal{A}b\mathcal{V}ar/K$ has good reduction over R, then any polarization $\lambda : \mathcal{A} \to \mathcal{A}^\vee$ extends to a polarization on $\mathcal{A}$. ⌟

Proof: See [Artin 1986, 4.4 in Arithmetic Geometry], and [Chai and Faltings 1990].**?** □

__over Dedekind Domains__

Def. (15.7.12.16) [Conductor]. For an elliptic curve E over a $F \in$ `GField`, the **conductor of** E is defined to be the integral ideal of F given by

$$N_{E/F} = \prod_{v \in \Sigma_F^0} \mathfrak{p}_v^{f_v}$$

where f_v is the local conductors(15.7.12.3). ⌟

Conj. (15.7.12.17) [Szpiro]. For any $\varepsilon > 0$, there exists $C_\varepsilon > 0$ s.t.

$$|N_{K/\mathbb{Q}}(\Delta_E)| \leq C_\varepsilon |N_{K/\mathbb{Q}}(N_E)|^{6+\varepsilon}$$

for any $E \in \mathcal{E}ll/\mathbb{Q}$, where N_E is the conductor of E. ⌟

Proof: □

Thm. (15.7.12.18) [No Everywhere Good Reduction over $\mathbb{Q}$]. There are no $A \in \mathcal{A}b\mathcal{V}ar/\mathbb{Q}$ with everywhere good reductions. There are 24 elliptic curves over $\mathbb{Q}$ with good reductions away form 2, and 784 elliptic curves over $\mathbb{Q}$ with good reduction away from 2, 3. ⌟

Proof: We only prove that there are no elliptic curves with everywhere good reductions.**?**

Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over $\mathbb{Q}$ with $a_i \in \mathbb{Z}$ and $\Delta = \pm 1$, then a_1 must be odd, otherwise $\Delta \equiv 5b_6^2 \equiv \pm 1 \mod 8$ is impossible. Thus $c_4 = b_2^2 - 24b_4 \equiv 1 \mod 8$. And $c_4^3 - c_6^2 = (\pm 12)^3$ shows that $c_4 \pm 12$ is a square or 3 times a square, which are both impossible by modulo 8.

For good reduction away from $2, 3$**?** □

Prop. (15.7.12.19). Let $F \in \texttt{NField}$ and $A, B \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/F$, and $S \subset \Sigma_F$ is a finite set of places of F containing Σ_F^∞ and all places s.t. A or B has bad reduction, then for any $\ell \in \mathbf{P}$ s.t. $S(\ell) \cap S = \varnothing$, there exists a finite set $T = T(S, \ell, g) \in \Sigma_\infty^0$ s.t. $T \cap (S \cup S(\ell)) = \varnothing$, and

$$P_\ell(\widetilde{A}_v, t) = P_\ell(\widetilde{B}_v, t) \Rightarrow A \sim B$$

⌟

Proof: Cf.[Mil08]P142. □

Semistable Reductions

Def. (15.7.12.20) [Semi-Abelian Schemes]. For $S \in \mathcal{S}\mathrm{ch}$, a **semi-Abelian scheme** S is a commutative smooth group variety s.t. each fiber is an extension of an Abelian scheme by a torus. ⌟

Prop. (15.7.12.21) [Reduction Theorem]. For any $F \in \texttt{NField}$, $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/F$, there exists a finite extension L/F s.t. A_L is semistable. ⌟

Proof: ? □

15.8 Complex Multiplication Theory

Main references are [Mil20b], [Lang, Complex Multiplication], [Abelian varieties with complex multiplication and modular functions, Shimura(1998)] and [The Fundamental Theorem of Complex Multiplication, Milne, 2007].

Notation (15.8.0.1).
- Use notations defined in Arithmetic of Abelian Varieties.

⌟

1 Introduction

Abelian varieties with complex multiplication correspond to special points on the moduli variety of abelian varieties, and their arithmetic is intimately related to that of the values of modular functions and modular forms at those points.

2 CM-Algebras and CM-Types

Def. (15.8.2.1) [CM-Fields]. A **CM-field** is a number field that is a totally imaginary quadratic extension of a totally real field. ⌟

Prop. (15.8.2.2) [Characterizing CM-Fields]. For $E \in \mathtt{NField}$, then E is a CM-field or totally real iff there exists exactly one $\mathtt{c}_E \in \mathrm{Aut}(E)$ s.t. for any $\rho \in \mathrm{Hom}(E, \mathbb{C}), \rho \circ \mathtt{c}_E = \mathtt{c} \circ \rho$. And it is CM iff $\mathtt{c}_E \neq \mathrm{id}_E$. ⌟

Proof: If $\rho \circ \mathtt{c}_E = \mathtt{c} \circ \rho$ for any $\rho \in \mathrm{Hom}(E, \mathbb{C})$, then $\rho \circ \mathtt{c}_E^2 = \rho$, so $\mathtt{c}_E^2 = \mathrm{id}$. if F is the fixed field of $\mathtt{c}_E$, then $[E : F] = 2$, and clearly F is totally real. Conversely, if E is a CM-field or totally real, then clearly there exists a unique such $\mathtt{c}_E$, which is the identity if E is totally real and the unique involution fixing the totally real subfield F.

In this case, if $\mathtt{c}_E \neq \mathrm{id}_E$, then $\rho(E) \subsetneq \mathbb{R}$ for any $\rho \in \mathrm{Hom}(E, \mathbb{C})$, thus E is totally imaginary. And if $\mathtt{c}_E = \mathrm{id}_E$, then E is also totally real. □

Cor. (15.8.2.3). A finite composite of CM-fields is a CM-field. In particular, the Galois closure of a CM-field is a CM-field.

And the composite of all CM-fields in $\mathbb{C}$ are the field $\mathbb{Q}^{\mathrm{cm}} \subset \overline{\mathbb{Q}}$ corresponding to the subgroup of $\mathrm{Gal}_{\mathbb{Q}}$ generated by all the elements $\{[\sigma, \mathtt{c}] | \sigma \in \mathrm{Gal}_{\mathbb{Q}}\}$, which is a normal subgroup. ⌟

Proof: The complex involutions on these CM-fields is compatible on their intersections, thus defines a complex involution on their composite. □

Cor. (15.8.2.4). Any CM-field E is of the form $E = F(\alpha)$, where F is totally real, $\alpha^2 \in F$, and $\rho(\alpha^2) \in \mathbb{R}_-$ for any homomorphism $\rho : F \to \mathbb{C}$. ⌟

Proof: If F is the totally real field contained in E and $\alpha \in E$ generates E over F, then by completing the square, we can assume $\alpha^2 \in F$. Then $\rho(\alpha^2) \in \mathbb{R}_-$ for any $\rho : F \to \mathbb{C}$, otherwise E is not totally imaginary. □

Def. (15.8.2.5) [CM-Algebras]. A **CM-algbera** is a finite product of CM-fields. ⌟

Def. (15.8.2.6) [CM-Types]. A **CM-type** for a CM-algebra E is a subset $\Phi \subset \mathrm{Hom}(E, \mathbb{C})$ s.t. $\mathrm{Hom}(E, \mathbb{C}) = \Phi \coprod \Phi^{\mathsf{c}_E}$.

A pair (E, Φ) where E is a CM-algebra and Φ is a CM-type on E is called a **CM-pair**.

More generally, if E is an étale algebra over $\mathbb{Q}$, then a **CM-type** on E is a subset $\Phi \subset \mathrm{Hom}(E, \mathbb{C})$ s.t. $\mathrm{Hom}(E, \mathbb{C}) = \sigma\Phi \coprod \mathsf{c} \circ \sigma\Phi$ for any $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. ⌟

Prop. (15.8.2.7). Let E be an étale algebra over $\mathbb{Q}$ and F the product of the largest totally real subfields of the factors of E, then choosing a CM-type is equivalent to choosing an extension ρ' to E of any homomorphism $\rho : F \to \mathbb{R}$. Thus a CM-pair (E, Φ) defines an isomorphism

$$E \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow[\cong]{\Phi} \prod_{\rho: F \to \mathbb{R}} \mathbb{C} \cong \mathbb{C}^{\Phi} : a \otimes r \mapsto (\rho'(a) r)_{\rho}, \quad \Phi = \{\rho' | \rho : F \to \mathbb{R}\}$$

⌟

Def. (15.8.2.8) [Primitive CM-Fields]. If E_0 is a CM-field and E/E_0 is a finite extension, then a CM-type Φ_0 on E_0 extends to a CM-type on E(15.8.2.6) by defining

$$\Phi = \{\varphi \in \mathrm{Hom}(E, \mathbb{C}) | \varphi|_{E_0} \in \Phi_0\}.$$

A **primitive CM-field** is a CM-pair(15.8.2.6) (E, Φ) where $E \in \mathtt{Field}$ and there doesn't exist a proper subfield $E_0 \subset E$ s.t. Φ is the extension of a CM-type on E_0. ⌟

Prop. (15.8.2.9). Every CM-pair (E, Φ) where E is a field is an extension of a unique primitive CM-pair (E_0, Φ_0) s.t. $E_0 \subset E$. Moreover, for any Galois CM-field E_1 containing E, E is the fixed field of E defined by the subgroup

$$H = \{\sigma \in \mathrm{Gal}(E_1/\mathbb{Q}) : \Phi_1^{\sigma} = \Phi_1\},$$

where Φ_1 is the extension of Φ to E_1. ⌟

Proof: If E is Galois over $\mathbb{Q}$, and E_0 is defined as above, then $\Phi\,\mathsf{c}_E = \mathsf{c}\,\Phi \neq \Phi$, so $\mathsf{c}_E \notin H$, thus c_E acts non-trivially on E_0. And c_E preserves E_0: We need to show that $\sigma\,\mathsf{c}_E\, a = \mathsf{c}_E\, a$ for any $a \in E_0$. For which it suffices to show that $\mathsf{c}_E\,\sigma\,\mathsf{c}_E \in H$. For this, notice

$$\Phi\,\mathsf{c}_E\,\sigma\,\mathsf{c}_E = \mathsf{c}\,\Phi\sigma\,\mathsf{c}_E = \mathsf{c}\,\Phi\,\mathsf{c}_E = \Phi.$$

Thus E_0 is CM-subfield of E. And $\Phi_0 = \Phi|_{E_0}$ is a CM-type on E_0, because if $\varphi'|_{E_0} = \mathsf{c}\,\varphi|_{E_0}$ for different $\varphi, \varphi' \in \Phi$, then $\mathsf{c}\,\varphi \in \varphi' H \subset \Phi$, contradiction.

And if E_0 is extended from another CM-subfield E', then any $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ fixing E' will fix Φ and lies in H. This shows $E_0 \subset E'$. So (E_0, Φ_0) is primitive.

For the general case, it suffices to notice that this E_0 is contained in E because any $\sigma \in \mathrm{Gal}(E_1/\mathbb{Q})$ fixing E will fix Φ_1 thus fixes E_0 by definition. And Φ clearly extends Φ_0. □

Cor. (15.8.2.10). A CM-pair (E, Φ) where E is a field is primitive iff there exists a Galois CM-field E_1 containing E s.t. E is the fixed field of E defined by the subgroup

$$H = \{\sigma \in \mathrm{Gal}(E_1/\mathbb{Q}) : \Phi_1^{\sigma} = \Phi_1\},$$

where Φ_1 is the extension of Φ to E_1. ⌟

Prop. (15.8.2.11) [Shimura-Taniyama]. Let E be a CM-field, $F = E^{c_E}$(15.8.2.2) and $E = F(\alpha)$ where $\alpha^2 \in F$ is totally negative. Then

$$\Phi = \{\varphi \in \mathrm{Hom}(E, \mathbb{C}) : \mathrm{Im}(\varphi(\alpha)) > 0\}$$

is a CM-type on E. And (E, Φ) is a primitive CM-pair iff

- $E = \mathbb{Q}(\alpha)$.
- $\sigma(\alpha)/\alpha$ is not totally positive for any $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$.

⌟

Proof: Φ is a CM-type on E because for any $\varphi \in \Phi$, $\varphi\, c_E \notin \Phi$ because $\mathrm{Im}(\varphi\, c_E(\alpha)) = -\mathrm{Im}(\varphi(\alpha)) < 0$.

Let F_1 be the Galois closure of F and $E_1 = F_1(\alpha)$, and Φ_1 is the extension of Φ to E_1, then

$$\Phi_1 = \{\varphi \in \mathrm{Hom}(E_1, \mathbb{C}) : \mathrm{Im}(\varphi(\alpha)) > 0\}.$$

and if

$$H = \{\sigma \in \mathrm{Gal}(E_1/\mathbb{Q}) : \Phi_1^\sigma = \Phi_1\},$$

then H is exactly the group of $\sigma \in \mathrm{Gal}(E_1/\mathbb{Q})$ s.t. $\sigma(\alpha)/\alpha \in \mathbb{R}_+$. Then the assertion follows from(15.8.2.10). □

Reflex Fields

Def. (15.8.2.12) [Reflex Fields of CM Pairs]. Let (E, Φ) be a CM-pair, then the **reflex field** E^* of (E, Φ) is the subfield of $\overline{\mathbb{Q}}$ generated by the elements $\{\sum_{\varphi\in\Phi} \varphi(a) | a \in E\}$. ⌟

Prop. (15.8.2.13). Let (E, Φ) be a CM-pair with reflex field E^*, then

- E^* is the fixed field of the group $\{\sigma \in \mathrm{Gal}_{\mathbb{Q}} | \sigma(\Phi) = \Phi\}$.
- E^* is a CM-field.
- If (E_1, Φ_1) is an extension of (E, Φ)(15.8.2.8), then the reflex field of (E_1, Φ_1) is just E^*.

⌟

Proof: 1: This group is clearly in the fixed group of E^*, and if σ is in the fixed group of E^*, then

$$\sum_{\varphi\in\Phi} \varphi(a) = \sum_{\varphi\in\Phi} \sigma\varphi(a),$$

so $\sigma(\Phi) = \Phi$ by the linear independence of characters.

2: For $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$ and $a \in E$,

$$c\,\sigma(\sum_{\varphi\in\Phi} \varphi(a)) = c \sum_{\varphi\in\Phi} \sigma\varphi(a) = \sum_{\varphi\in\Phi} \sigma\varphi(c_E(a)) = \sigma \sum_{\varphi\in\Phi} \varphi(c_E(a)) = \sigma\, c(\sum_{\varphi\in\Phi} \varphi(a)).$$

Thus E is a CM-field or totally real by(15.8.2.2). The latter case is not possible because of the linear independence of characters and the fact $c(\Phi) \neq \Phi$.

3 is trivial. □

Def. (15.8.2.14) [Reflex CM-Pairs]. Let (E, Φ) be a CM-pair that E is contained in $\mathbb{Q}$, let E_1 be the Galois closure of E, and Φ_1 the extension of Φ to E_1. Then (E_1, Φ^{-1}) is also a CM-pair. Then the primitive subfield (E^*, Φ^*) satisfies E^* is the reflex field of (E, Φ).

(E^*, Φ^*) is called the **reflex CM-pair** of (E, Φ). ⌟

Classification of Primitive CM-Pairs

Prop. (15.8.2.15). Milne, Prop1.30.**?** ⌟

Cor. (15.8.2.16). Milne, Prop1.31.**?** ⌟

Positive Involutions

Def. (15.8.2.17) [Positive Involutions]. Let $k \subset \mathbb{R}$ be a field, and B be a f.d. k-algebra, $\mathrm{tr} : B \to k$ a k-linear functional, then a **positive involution** w.r.t. tr is an involution ι on B s.t.

$$\mathrm{tr}(x) = \mathrm{tr}(\iota(x)), \quad \mathrm{tr}(\iota(x)\cdot x) > 0$$

for any nonzero $x \in B$. ⌟

Prop. (15.8.2.18) [Positive Involutions are Semisimple]. Let $k \subset \mathbb{R}$ be a field, and B be a f.d. k-algebra with a positive involution ι, then B is semisimple. And if Z is the center of B, then $Z = \prod_i K_i$ where $K_i \in$ `NField`, and each K_i are stable under ι. ⌟

Proof: By(3.6.2.8), it suffices to show that B is Jacobson semisimple: If $\mathfrak{a}$ is a nonzero nilpotent two-sided ideal of B, $a \neq 0 \in \mathfrak{a}$ is nilpotent, then $b = a\iota(a) \neq 0$ because $\mathrm{tr}(a\iota(a)) > 0$. Thus $b \neq 0 \in \mathfrak{a}$, and $\iota(b) = b$. So by the same reason $b^2 \neq 0$, and so on, so b is not nilpotent, contradicting(3.6.2.6).

The center is clearly invariant under the isomorphism given, so it is also semisimple, which is then a product of fields. To show each factor is stable under ι, notice that if $1 = \sum_i e_i$ is a decomposition w.r.t. this product, then $1 = \sum_i \iota(e_i)$, so $\{\iota(e_i)\} = \{e_i\}$. Moreover, $\iota(e_i) = e_i$ for each i, because otherwise $e_i\iota(e_i) = 0$, and $\mathrm{tr}(e_i\iota(e_i)) = 0$. □

Prop. (15.8.2.19). Let $k \subset \mathbb{R}$ be a field and B a f.d. k-algebra with an involution ι, then the following are equivalent:

- There is a faithful f.d. B-module V with a positive definite symmetric k-bilinear form $(-,-) : V \times V \to k$ s.t.
$$(bu, v) = (u, \iota(b)v), \quad b \in B, u, v \in V.$$
- For any f.d. B-module V, there exists a positive definite symmetric k-bilinear form $(-,-) : V \times V \to k$ s.t.
$$(bu, v) = (u, \iota(b)v), \quad b \in B, u, v \in V.$$
- There exists a k-linear functional tr on B s.t. ι is positive w.r.t. tr.

⌟

Proof: $1 \to 2$: As B is semisimple(15.8.2.18), any f.d. B-module is a direct summand of a direct sum of the faithful module V.

$2 \to 3$: Apply item2 to the B-module B itself, then we find a positive definite symmetric k-bilinear form $(-,-)$ on B, and an orthonormal basis $(e_1, \ldots, e_n)$ of B. Then we define

$$\mathrm{tr} : B \to \mathbb{Q} : \mathrm{tr}(b) = \sum_i (bb_i, b_i)$$

then $\mathrm{tr}(b) = \mathrm{tr}(\iota(b))$, and

$$\mathrm{tr}(b\iota(b)) = \sum_i (b\iota(b)b_i, b_i) = \sum_i (\iota(b)b_i, \iota(b)b_i) > 0.$$

$3 \to 1$: B is semisimple by(15.8.2.18), and then we can take $V = B$, and the positive definite symmetric k-bilinear form

$$(x, y) \mapsto \mathrm{tr}_{B/k}(\iota(y)x).$$

then $(bx, y) = \mathrm{tr}(\iota(y)bx) = \mathrm{tr}(\iota(\iota(b)y)x) = (x, \iota(b)y)$. □

Prop. (15.8.2.20) [Commutative Positive Involutions]. Every f.d. commutative $\mathbb{Q}$-algebra with a positive involution ι is a product of the following two:

- F is a totally real field and $\iota = \mathrm{id}_F$.
- E is a CM-field and $\iota = \mathtt{c}_E$.

⌟

Proof: Firstly, any product of these two are positive involutions. Conversely, if (B, tr) is a f.d. $\mathbb{Q}$-algebra with a positive involution, then by(15.8.2.18), B is semisimple, thus a finite product of number fields. Then by(15.8.2.18), each factor is fixed by the involution, so it suffices to consider the case $B \in \mathtt{NField}$. Let F be the fixed field of ι. Because the trace form $\mathrm{tr}_{B/\mathbb{Q}}$ is non-degenerate, we can assume $\mathrm{tr}(x) = \mathrm{tr}(\alpha x)$ for some $\alpha \in B^\times$.

If $F = B$, then F is totally real: if there exists a non-real embedding $\sigma : F \to \mathbb{C}$, then we can use weak approximation to find $x \in F^\times$ s.t. $\sigma(\alpha x^2)$ is near -1 and $\varphi(\alpha x^2)$ is near 0 for any other embedding $\varphi : F \to \mathbb{C}$. Then clearly $\mathrm{tr}(\alpha x^2) < 0$, contradiction.

If $F \neq B$, then $[B : F] = 2$, and $\mathrm{tr}_{B/\mathbb{Q}}(\alpha x \iota(x)) > 0$ for any $x \in B^\times$. Take $x = 1$, we see $\mathrm{tr}_{B/\mathbb{Q}}(\alpha) > 0$. In particular, $\alpha + \iota(\alpha) \neq 0 \in F$. Then in particular, $\mathrm{tr}_{B/\mathbb{Q}}(\alpha x \iota(x)) = \mathrm{tr}_{F/\mathbb{Q}}((\alpha + \iota(\alpha))x\iota(x)) > 0$. So by the argument above, F is totally real. And B is totally imaginary: If there exists a real embedding $\sigma : B \to \mathbb{C}$, then σ and $\sigma \circ \iota$ corresponds to different places, and by weak approximation, we can find $x \in B$ s.t. $\sigma((\alpha + \iota(\alpha))x)$ is near -1 and $\sigma(\iota(x))$ is near 1, and $\varphi(x)$ is near 0 for any other $\varphi : B \to \mathbb{C}$. Then $\mathrm{tr}_{F/\mathbb{Q}}((\alpha + \iota(\alpha))x\iota(x)) < 0$, contradiction. So in this case B is a CM-field, and $\iota = \mathtt{c}_B$. □

Cor. (15.8.2.21). There exists uniquely a positive involution on any CM-algebra, which is $\mathtt{c}_E$. ⌟

Weil q-Integers

Prop. (15.8.2.22) [Weil q-Integers and CM Fields]. If $p \in \mathbf{P}, q \in p^{\mathbb{Z}}$ and $\varpi \in \mathrm{Weil}(q^{1/2})$, then $\mathbb{Q}(\varpi)$ is either isomorphic to $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{q})$ or a CM-field. ⌟

Proof: For any embedding $\rho : \mathbb{Q}(\pi) \to \mathbb{C}$,

$$\rho(\pi)\overline{\rho(\pi)} = q = \rho(\pi)\rho(q/\pi),$$

so $\bar{(}\rho(\pi)) = \rho(q/\pi)$, and $E = \mathbb{Q}(\pi)$ is a CM-field with the endomorphism $\mathtt{c}_E : \pi \mapsto q/\pi$. □

Prop. (15.8.2.23). Let $p \in \mathbf{P}, q \in p^{\mathbb{Z}}$, $F \in \mathtt{NField}$ and $\pi, \pi' \in F \cap \mathrm{Weil}(q^{1/2})$. If $\mathrm{ord}_v(\pi) = \mathrm{ord}_v(\pi')$ for any $v \in \Sigma_F^p$, then π/π' is a roots of unity in E. ⌟

Proof: This is because there is an endomorphism of F(the conjugation) taking π to q/π, so for any $v \notin \Sigma_F^p$, $\mathrm{ord}_v(\pi) = 0$. Since the same is true for π', and $\mathrm{ord}_v(\pi) = \mathrm{ord}_v(\pi')$ for $v \in \Sigma_F^\infty$ too, by the definition of Weil q-integers. Thus $|\pi/\pi'|_v = 1$ for any $v \in \Sigma_F$, and the assertion follows from(14.4.4.30). □

3 CM Abelian Varieties

Def. (15.8.3.1) [Complex Multiplications]. For $k \in \texttt{Field}$ and $A \in \mathcal{A}b\mathcal{V}ar/k$,

$$[\mathrm{End}_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}} \leq 2\dim A.$$

And A is called an Abelian variety with **complex multiplication** or a CM Abelian variety if the equality holds. ⌟

Proof: Take $\ell \in \mathbf{P} \setminus \{\mathrm{char}\, k\}$, then $\mathrm{End}_{\mathbb{Q}}(A)$ acts faithfully on $T_\ell(A, \mathbb{Q}_\ell)$ by(15.13.2.3), which has dimension $2\dim A$(15.7.6.15), so we finish by(15.7.6.10) and(3.6.3.24). □

Prop. (15.8.3.2). For $k \in \texttt{Field}$ and $A \in \mathcal{A}b\mathcal{V}ar/k$, the following are equivalent:

- A is CM.
- $\mathrm{End}_{\mathbb{Q}}(A)$ contains an étale subalgebra of rank $2\dim A$ over $\mathbb{Q}$.
- For any Weil cohomology $\mathscr{H}^*$ with coefficients in $\Omega \in \texttt{Field}^0$, the centralizer of $\mathrm{End}_{\mathbb{Q}}(A)$ in $\mathrm{End}_\Omega(H^1(A))$ is commutative (and equals $Z(\mathrm{End}_{\mathbb{Q}}(A)) \otimes \Omega$).

⌟

Proof: 1 $\iff$ 2 follows from the fact the maximal étale subalgebra of $\mathrm{End}_{\mathbb{Q}}(A)$ has degree $[\mathrm{End}_{\mathbb{Q}}(A) : \mathbb{Q}]_{\mathrm{red}}$(3.6.3.23).

2 $\iff$ 3 follows by noticing $\dim_\Omega(\mathscr{H}^1(A)) = 2\dim A$, and $\mathrm{End}_\Omega(A)$ acts faithfully on it**?**. Then use(3.6.3.24). □

Lemma (15.8.3.3). Let $A \in \mathcal{A}b\mathcal{V}ar/\mathbb{C}$ and $F \subset \mathrm{End}_{\mathbb{Q}}(A)$. If F has a real place, then $[F : \mathbb{Q}] | \dim A$. ⌟

Proof: **?** □

Prop. (15.8.3.4). For $k \in \texttt{Field}$ and $A \in \mathcal{A}b\mathcal{V}ar/k$,

- if A is simple, then A is CM iff $\mathrm{End}_{\mathbb{Q}}(A)$ is a CM-field of degree $2\dim A$ over $\mathbb{Q}$.
- If A is isotopic, then A is CM if $\mathrm{End}_{\mathbb{Q}}(A)$ contains a CM-field of degree $2\dim A$ over $\mathbb{Q}$, which is invariant under some Rosati involution.
- A is CM iff $\mathrm{End}_{\mathbb{Q}}(A)$ contains an étale CM-algebra of degree $2\dim A$ over $\mathbb{Q}$, which is invariant under some Rosati involution. And in this case, for $\ell \in \mathbf{P} \setminus \{\mathrm{char}\, k\}$, $T_\ell(A)$ is free of rank 1 over this algebra.

⌟

Proof: We use(15.8.3.2).

1: It suffices to show that if $\mathrm{End}_{\mathbb{Q}}(A)$ is a field of degree $2\dim A$, then it is CM.**?**

2: **?**

3 follows from 2. □

Prop. (15.8.3.5) [Tate1966]. Every Abelian variety over a finite field has CM. ⌟

Proof: **?** □

Complex CM Abelian Varieties

Prop. (15.8.3.6) [CM-Types of Complex Abelian Varieties]. Let E be a CM-algebra of degree $2g$, $A \in \mathcal{A}b\,\mathcal{V}ar^g/\mathbb{C}$ and $E \subset \mathrm{End}_{\mathbb{Q}}(A)$, then the action of E on $\mathrm{Tgt}_0(A)$ is faithful, so

$$\mathrm{Tgt}_0(A) \cong \bigoplus_{\varphi\in\Phi} \mathbb{C}_\varphi$$

where Φ is a set of homomorphisms from E to $\mathbb{C}$. Then from the decomposition

$$H_1(A, \mathbb{R}) \cong \mathrm{Tgt}_0(A) \bigoplus \overline{\mathrm{Tgt}_0(A)}$$

and the fact $H_1(A, \mathbb{Q})$ is a free E-module of rank 1(15.8.3.4), we see $\Phi \coprod \mathsf{c}\,\Phi = \mathrm{Hom}(E, \mathbb{C})$. So Φ is a CM-type on E.

Thus A is said to have **CM-type** (E, Φ) if Φ is a CM-type on E and

$$\mathrm{Tgt}_0(A) \cong \mathbb{C}^\Phi$$

as E-algebras. ⌟

Def. (15.8.3.7) [Reflex Field of a CM Abelian Variety]. Let $A \in \mathcal{A}b\,\mathcal{V}ar/\mathbb{C}$ be CM, then if E_0 is the center of $\mathrm{End}_{\mathbb{Q}}(A)$, by(15.8.3.4) and(15.8.3.6), E_0 is a CM-algebra, and there exists a CM-type Φ_0 on E_0 s.t. for any CM-pair E s.t. A is of CM-type (E, Φ), there Φ is the extension of Φ_0 to E.

Then the reflex field of (E_0, Φ) equals that of (E, Φ) for any (E, Φ), called the **reflex field** of A. ? ⌟

Prop. (15.8.3.8) [Abelian Varieties attached to CM-Pairs]. Let (E, Φ) be a CM-pair and Λ is a $\mathbb{Z}$-lattice in E, then

$$\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \cong E \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow[\cong]{\Phi} \mathbb{C}^\Phi (15.8.2.7).$$

So $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ has a complex structure and we get a Riemann pair (Λ, J_Φ), which corresponds to a complex torus A_Φ.

Then $\mathcal{O} = \{x \in E | a\Lambda \subset \Lambda\} \subset \mathrm{End}(A_\Phi)$ is an order in E(14.4.1.37), and then $E \subset \mathrm{End}_{\mathbb{Q}}(A_\Phi)$.

Then there is a Riemann form on (Λ, J_Φ) whose associated positive Rosati involution(15.7.8.7) stabilizes E(and thus equals c_E on E by(15.8.2.21)). In particular, A_Φ is a complex Abelian variety(15.7.8.1). ⌟

Proof: To give such a Riemann form, by(12.9.5.9), it suffices to give a non-degenerate bilinear form $\psi : E \times E \to \mathbb{Q}$ that satisfies

1. $\psi(ax, y) = \psi(x, \overline{a}y)$ for $a, x, y \in E$.
2. $\psi(x, y) = -\psi(y, x)$ for $x, y \in E$.
3. $\psi(J_\Phi x, J_\Phi y) = \psi(x, y)$ for $x, y \in E \otimes_{\mathbb{Q}} \mathbb{R}$.
4. $\psi(x, J_\Phi x) > 0$ for any non-zero $x \in E \otimes_{\mathbb{Q}} \mathbb{R}$.

Now because the trace form $\mathrm{tr} : E \times E \to \mathbb{Q}$ is non-degenerate, non-degenerate $\mathbb{Q}$-bilinear forms of E are exactly of the form

$$\psi(x, y) = \mathrm{tr}_{E/\mathbb{Q}}(\overline{y}\alpha x), \alpha \in E^\times.$$

And the conditions (1) is automatic, and (3) is automatic because in the isomophism

$$E \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow[\cong]{\Phi} \prod_{\rho:F\to\mathbb{R}} \mathbb{C} \cong \mathbb{C}^\Phi : a \otimes r \mapsto (\rho'(a)r)_\rho, \quad \Phi = \{\rho' | \rho : F \to \mathbb{R}\}, (15.8.2.7)$$

$\psi_{\mathbb{R}}$ corresponds to

$$\psi'((x_\varphi),(y_\varphi)) = \sum_{\varphi\in\Phi} \mathrm{tr}_{\mathbb{C}/\mathbb{R}}(\varphi(a)\overline{y_\varphi}x_\varphi)$$

and J_Φ corresponds to the isomorphism

$$(x_\varphi)_{\varphi\in\Phi} \mapsto (\mathrm{i}\, x_\varphi)_{\varphi\in\Phi}.$$

Thus it suffices to choose α s.t. $\varphi(\alpha)\in \mathrm{i}\,\mathbb{R}_+$ for any $\varphi\in\Phi$.

By(15.8.2.4), there exists $\alpha\in E^\times$ s.t. $E = F(\alpha)$ s.t. $\varphi(\alpha)\in \mathrm{i}\,\mathbb{R}$ for any $\varphi\in\Phi$, and we can then use weak approximation on F to modify α s.t. $\varphi(\alpha)\in\mathrm{i}\,\mathbb{R}_+$ for any $\varphi\in\Phi$. So this α clearly exists. Moreover, any other element α' is α times some element $a\in F$ that is totally positive. □

Prop. (15.8.3.9)[Classifying Complex CM Abelian Varieties up to Isogeny]. The map $(A,i)\to(E,\Phi)$ defines a bijection between the set of isogeny classes of CM Abelian varieties $A/\mathbb{C}$ with an embedding $i: E\to \mathrm{End}_{\mathbb{Q}}(A)$ and the set of isomorphism classes of CM-pairs (E,Φ), with inverse $(E,\Phi)\mapsto(A_\Phi,i_\Phi)$ which is the Abelian variety corresponding to the lattice $\Lambda=\mathcal{O}_E$(15.8.3.8), called the **principally-CM Abelian variety** of type (E,Φ). ⌟

Proof: Notice in(15.8.3.8), any two choice of the lattice $\mathfrak{a}$ give isogenous Abelian varieties, and because $H_1(A,\mathbb{Q})$ is free of rank 1 over E, let $e\in H_1(A,\mathbb{Q})$ be a basis vector, then $\mathfrak{a}e = H_1(A,\mathbb{Z})$ for some lattice $\mathfrak{a}\subset E$. Then this e defines an isomorphism

$$Ee\cong H_1(A,\mathbb{Z})\otimes\mathbb{Q} = H_1(A,\mathbb{Q})$$

thus the isomorphism

$$A\cong H_1(A,\mathbb{C})/H_1(A,\mathbb{Z}) \xrightarrow[\cong]{e^{-1}} E\otimes_{\mathbb{Q}}\mathbb{C}/\mathfrak{a} \xrightarrow[\cong]{\Phi} \mathbb{C}^\Phi/\Phi(\mathfrak{a}) \sim \mathbb{C}^\Phi/\Phi(\mathcal{O}_E).$$

This is clearly a bijection. □

Prop. (15.8.3.10)[Classifying Simple Complex CM Abelian Varieties]. Let A be a simple complex Abelian variety over $\mathbb{C}$ with CM and $E=\mathrm{End}_{\mathbb{Q}}(A)$, then E is a CM-field, and the map $A\mapsto(E,\Phi_A)$ defines a bijection between the set of isomorphism classes of simple complex Abelian varieties with CM and the set of isomorphism classes of primitive CM-paris. ⌟

Proof: $E\in$ `Field` by(15.8.3.4), and if it is not primitive, then (E,Φ) is extended from a primitive CM-field (E_0,Φ_0), and a choice of E_0-basis of E defines an embedding $E\subset \mathrm{Mat}([E:E_0],E_0)\subset \mathrm{End}_0(A_{\Phi_0}^{[E:E_0]})$, and

$$E\otimes_{\mathbb{Q}}\mathbb{R} = E\otimes_{E_0}(E_0\otimes_{\mathbb{Q}}\mathbb{R})\cong E\otimes_{E_0}(\mathbb{C}^{\Phi_0})\cong\mathbb{C}^\Phi$$

shows $A_{\Phi_0}^{[E:E_0]}$ is also of type (E,Φ). Thus $A\sim A_{\Phi_0}^{[E:E_0]}$ by(15.8.3.9), contradicting the fact A is simple. □

Cor. (15.8.3.11). The simple Abelian varieties with complex multiplications are classified up to conjugacy by the $\mathrm{Gal}_{\mathbb{Q}}$-orbits of CM-types on $\mathbb{Q}^{\mathrm{cm}}$, by(15.8.2.16). ⌟

Good Reductions

Prop. (15.8.3.12)[Potential Good Reduction of CM-Abelian Varieties]. Let $E\in$ `NField`, $A\in \mathcal{A}b\,\mathcal{V}ar/\mathbb{C}$ has complex multiplication by E, then A is defined over some number field F. And F can be chosen s.t. A_F has good reduction. ⌟

Proof: Cf.[Milne, Abelian Varieties, P55].? □

4 Mumford-Tate Groups

5 Fundamental Theorem

Thm. (15.8.5.1) [Fundamental Theorem of Complex Multiplication, Shimura-Taniyama]. Let $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/\mathbb{F}_q$ be the reduction from an complex Abelian variety of CM-type (E, Φ), then the Weil-q-integers of A can be constructed as follows:

⌟

Proof: Cf.[Milne, Abelian Varieties, P83].**?** □

6 Elliptic Curves

References are [Deu58] and [Ser67].

Prop. (15.8.6.1) [Complex Elliptic Curves with CM]. If $E \cong E_\tau \in \mathcal{E}\mathrm{ll}/\mathbb{C}$ has CM, then $\mathcal{K} = \mathbb{Q}(\tau)$ is an imaginary quadratic extension of $\mathbb{Q}$ and $\mathrm{End}(E)$ is isomorphic to an order of $\mathcal{K}$.

By(15.11.1.28), if $E \in \mathcal{E}\mathrm{ll}/\mathbb{C}$ has CM(15.8.3.1), then $\mathrm{End}(E)$ is an $\mathbb{Z}$-order in $\mathcal{K}$, which by(14.4.1.47)must be of the form $\mathcal{O}_{\mathcal{K},f} = \mathbb{Z} + f\mathcal{O}_K$, where $f = [\mathcal{O}_\mathcal{K} : \mathrm{End}(E)]$. ⌟

Proof: Cf.[Sil16]P176.**?** □

Thm. (15.8.6.2) [Classifying CM Elliptic Curves]. Given any imaginary quadratic field $\mathcal{K}$ and an $\mathbb{Z}$-order $\mathcal{O}_{\mathcal{K},f} \subset \mathcal{K}$, the isomorphism classes of elliptic curves over $\mathbb{C}$ with maximal CM by $\mathcal{O}_{\mathcal{K},f}$ is in bijection with $\mathrm{Cl}(\mathcal{O}_{\mathcal{K},f})$, denoted by $\mathcal{E}\mathrm{ll}_\mathbb{C}(\mathcal{O}_{\mathcal{K},f})$.

In particular, $\#\,\mathcal{E}\mathrm{ll}_\mathbb{C}(\mathcal{O}_{\mathcal{K},f}) < \infty$. The j-values of elliptic curves with maximal CM by $\mathcal{O}_{\mathcal{K},f}$ are called singular moduli **associated to** $\mathcal{O}_{\mathcal{K},f}$. ⌟

Proof: If $E \cong \mathbb{C}/\Lambda \cong E_\tau$, then $\mathbb{Z} + \mathbb{Z}\tau$ is an $\mathcal{O}_{\mathcal{K},f}$-module of rank 1, and by definition it is a proper fractional ideal of $\mathcal{O}_{\mathcal{K},f}$ thus invertible(14.4.1.48). Conversely, any such an invertible fractional ideals $\mathfrak{a}$ is a lattice in $\mathcal{K}$ thus defines an elliptic curve $E_\mathfrak{a}$ with $\mathrm{End}(E_\mathfrak{a}) = \mathcal{O}$ by(14.4.1.48). Finally it follows from(12.9.5.2) that two such $E_\mathfrak{a}$ and $E_{\mathfrak{a}'}$ are isomorphic iff $\mathfrak{a}, \mathfrak{a}'$ differ by a principle ideal. □

Prop. (15.8.6.3). Let $\mathcal{K}$ be an imaginary quadratic field, $E \in \mathcal{E}\mathrm{ll}_\mathbb{C}(\mathcal{O}_\mathcal{K})$, and $\mathfrak{a} \in \mathrm{Ideal}(\mathcal{O}_\mathcal{K})$, then

- $E[\alpha]$ is the kernel of the isogeny $E \to \overline{\mathfrak{a}} * E$.
- $E[\alpha]$ is a free $\mathcal{O}_\mathcal{K}/\mathfrak{a}$-module of rank 1.
- The degree of isogeny $E \to \overline{\mathfrak{a}} * E$ is $\mathrm{Nm}_{\mathcal{K}/\mathbb{Q}}(\mathfrak{a})$.
- For $\alpha \in \mathcal{O}_K^\times$, $\deg([\alpha]_E) = \mathrm{Nm}_{\mathcal{K}/\mathbb{Q}}(\alpha)$.

⌟

Proof: Cf.[Sil99]P102. □

Thm. (15.8.6.4) [Singular Moduli, Weber-Fueter]. Let $E \in \mathcal{E}\mathrm{ll}_\mathbb{C}(\mathcal{O}_{\mathcal{K},f})$, then

- $j(E) \in \mathcal{O}_{\overline{\mathbb{Q}}}$, and $\mathcal{K}(j(E))$ is the ray class field $\mathcal{K}_f$ of $\mathcal{K}$.
- $\mathrm{Gal}(\mathcal{K}_f/\mathcal{K})$ acts transitively on the j-values associated to $\mathcal{O}_{\mathcal{K},f}$(15.8.6.2).

In particular, $\deg(j(E)) = \mathrm{cl}(\mathcal{O}_{\mathcal{K},f})$. ⌟

Proof: Cf.[Serre] or [Sutherland]L21. or [Silverman]P447 or [Cox, Chap11]. Notice this should be a special case of Shimura-Taniyama. □

Cor. (15.8.6.5). There are 13 elliptic curves $E \in \mathcal{E}\text{ll}/\mathbb{Q}$ with CM, namely they are associated to $\mathcal{O}_{\mathcal{K},f}$ with

- $f = 1, \mathcal{K} = \mathbb{Q}(\sqrt{-d})$ with $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$, with corresponding j-invariances
$$j = 2^6{\cdot}3^3,\quad 2^6{\cdot}5^3,\quad 0,\quad -3^3{\cdot}5^3,\quad -2^{15},\quad -2^{15}{\cdot}3^3,\quad -2^{18}{\cdot}3^3{\cdot}5^3,\quad -2^{15}{\cdot}3^3{\cdot}5^3{\cdot}11^3,\quad -2^{18}{\cdot}3^3{\cdot}5^3{\cdot}23^3{\cdot}29^3.$$
- $f = 2, \mathcal{K} = \mathbb{Q}(\sqrt{-d})$ with $d \in \{1, 3, 7\}$, with corresponding j-invariances
$$j = 2^3 \cdot 3^3 \cdot 11^3,\quad 2^4 \cdot 3^3 \cdot 5^3,\quad 3^3 \cdot 5^3 \cdot 17^3.$$
- $f = 3, \mathcal{K} = \mathbb{Q}(\sqrt{-3})$ with corresponding j-invariances $j = 2^{15} \cdot 3 \cdot 5^3$.

⌟

Proof: □

Thm. (15.8.6.6) [Hasse]. For $[\Lambda] \in \mathrm{Pic}(\mathcal{O}_{\mathcal{K},f})$, denoted $j(\Lambda) = j(\mathbb{C}/\Lambda)$, then if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_{\mathcal{K}}$ prime to the conductor and $\mathfrak{p}_f = \mathfrak{p} \cap \mathcal{O}_{K,f}$, then
$$(\mathrm{Art}(\mathrm{Frob}_{\mathfrak{p}}))(j(\Lambda)) = j(\Lambda{\cdot}\mathfrak{p}_f^{-1}).$$
⌟

Proof: ? □

Prop. (15.8.6.7) [CM j-Invariants are Integral]. For $K \in p\text{-}\mathtt{LField}$ and $E \in \mathcal{E}\text{ll}/K$ with CM, $j(E) \in \mathcal{O}_{\overline{K}}$. ⌟

Proof: □

Prop. (15.8.6.8). If $k \in \mathtt{Field}^p$, and $E \in \mathcal{E}\text{ll}/k$ has CM, then $j(E) \in \overline{\mathbb{F}}_q \cap k$, by(15.11.3.5). ⌟

Thm. (15.8.6.9) [Kronecker's Jugendtraum]. Let $\mathcal{K}$ be an imaginary quadratic field and $E \in \mathcal{E}\text{ll}(\mathcal{O}_{\mathcal{K}})$, then
$$\mathcal{K}^{\mathrm{ab}} = \mathcal{K}(j(E), \{x_{\mathrm{tor}}(E)\}),$$
where $\{x_{\mathrm{tor}}(E)\}$ is the set of x-coordinates of torsion points of E. ⌟

Proof: ? □

CM-Lifting

Thm. (15.8.6.10) [Honda/Chai-Conrad-Oort2014]. For any $A \in \mathcal{A}b\mathcal{V}ar/\mathbb{F}_q$, there exists an isogeny $A \sim B_0$ s.t. B_0 admits a CM lift to characteristic 0. ⌟

Proof: □

Thm. (15.8.6.11)[Deuring CM-Lifting Lemma]. Let $p \in \mathbf{P}$ and $E \in \mathcal{E}\text{ll}/\overline{\mathbb{F}}_p$, and $\alpha_0 \in \mathrm{End}(E_0)\backslash\mathbb{Z}$, then there exists $F \in \mathtt{NField}$, $\mathcal{E} \in \mathcal{E}\text{ll}/\mathcal{O}_F$ and $\alpha \in \mathrm{End}(\mathcal{E})$, $\mathfrak{p} \in \Sigma_F^p$ s.t.
$$\mathcal{E}_{\overline{\kappa(\mathfrak{p})}} \cong E_0$$
s.t. $\alpha_{\overline{\kappa(\mathfrak{p})}}$ corresponds to α_0. ⌟

Proof: Cf.[Suw19]P5? □

Hilbert Class Polynomials

Def. (15.8.6.12) [Hilbert Class Polynomials]. Let $\mathcal{O}$ be a order in an imaginary quadratic field $\mathcal{K}$, the **Hilbert class polynomial** associated to $\mathcal{O}$ is defined to be

$$H_{\mathcal{O}}(X) = \prod_{E\in\mathcal{E}\mathrm{ll}_{\mathbb{C}}(\mathcal{O})} (X - j(E)).$$

And for $D \in \mathbb{Z}, D \equiv 0, 1 (\mathrm{mod}\ 4)$, the **Hilbert class polynomial** of discriminant D is defined to be the class polynomial for the order $\mathcal{O}_D$. ⌟

Lemma (15.8.6.13). For $\ell \equiv -1 (\mathrm{mod}\ 4) \in \mathbf{P} \setminus \{3\}$ and $D = -\ell$ or -4ℓ, $H_D(1728) \equiv 0 (\mathrm{mod}\ \ell)$. ⌟

Proof: Consider the curve $E : y^2 = x^3 - x$, it is supersingular by(15.11.3.12) or(15.8.6.20), and has j-invariant 1728. Thus $\varphi_E^2 = -\ell$ by (15.11.3.9)(15.11.3.3). Notice $E[2] = \{\infty, (0, 0), (\pm 1, 0)\}$, which are all defined over $\mathbb{F}_p$, so $2|(1 + F)$, and $\mathbb{Z}[\frac{1+\varphi_E}{2}] \cong \mathcal{O}_\ell$. Thus by Deuring CM-lifting lemma(15.8.6.11), there is an elliptic curve over some $\mathcal{O}_F$ with maximal CM by $\mathcal{O}_{-\ell}$ whose j-invariant is mapped to $1728 (\mathrm{mod}\ \ell)$, so $H_{-\ell}(1728) \equiv 0 (\mathrm{mod}\ \ell)$.

Similarly, E has endomorphism $I : (x, y) \mapsto (-x, \mathrm{i}\, y)$, $I^2 = -1, IF = -FI$, so we can lift IF to get an elliptic curve over some $\mathcal{O}_F$ with CM by $\mathcal{O}_{-4\ell}$. And it is maximal CM, because $\frac{1+IF}{2} \notin \mathrm{End}(E)$, as $(1 + IF)(P = (1, 0)) = (1, 0) + (-1, 0) \neq O$. □

Lemma (15.8.6.14). For $\ell \equiv -1 (\mathrm{mod}\ 4) \in \mathbf{P} \setminus \{3\}$ and $D = -\ell$ or -4ℓ, let $\mathcal{K}_D$ be the ray class field of $\mathcal{O}_D$, then for any root x_0 of $H_D(X)$ s.t. $x_0 \equiv 1728 (\mathrm{mod}\ \ell)$, there exists a unique $\mathfrak{l} \in \Sigma^\ell_{\mathcal{K}_D}$ s.t. $x_0 - 1728 \in \mathfrak{l}$. The j-invariant of this elliptic curve is mapped to $1728 (\mathrm{mod}\ \ell)$, so $H_{-\ell}(1728) \equiv 0 (\mathrm{mod}\ \ell)$. ⌟

Proof: The existence follows from(15.8.6.13), and if there are two primes $\mathfrak{l}, \mathfrak{l}'$ that divides $x - 1728$, then there exists $\sigma \neq \mathrm{id}$ s.t. $x_1 = \sigma(x_1) \equiv 1728 (\mathrm{mod}\ \ell)$. Then there are two elliptic curves $E_1, E_2/\overline{\mathbb{Q}}$ with j-invariants x_0, x_1 that reduces to the elliptic $E/\mathbb{F}_\ell : y^2 = x^3 - x$. Then we get a degree-preserving injection $\mathrm{Hom}(E_1, E_2) \hookrightarrow \mathrm{End}(E_{\overline{\mathbb{F}}_\ell}) = A$.

For the rest, see[Suw19]P8**?** □

Prop. (15.8.6.15). For $\ell \equiv -1 (\mathrm{mod}\ 4) \in \mathbf{P} \setminus \{3\}$, there exists $R, S \in \mathbb{Z}[X]$ s.t.

$$H_{-\ell}(X) = (X - 1728)R(X)^2, \quad H_{-4\ell}(X) = (X - 1728)S(X)^2.$$

⌟

Proof: Notation as in(15.8.6.14), there exists an involution τ of $\mathcal{K}_D$ s.t. $\sigma(x_0) = x_0$. Thus by the lemma, $\tau(\mathfrak{l}) = \mathfrak{l}$, and $f(\mathfrak{l}/\ell)$ is odd because $\mathrm{Gal}(\mathcal{K}_D/\mathcal{K})$ does(14.4.3.8). So σ acts trivially on $\kappa(\mathfrak{l})$. But τ doesn't fix any roots x of $H_D(X)$ other than x_0(because x_i corresponds to ideal classes of $\mathcal{O}_D$ where x_0 corresponds to the trivial class, and τ acts by $[I] \mapsto [I]^{-1}$), so the other roots come in pairs, and the assertion follows. □

Prop. (15.8.6.16). For $\ell \equiv -1 (\mathrm{mod}\ 4) \in \mathbf{P} \setminus \{3\}$, the only real roots of $H_\ell(X)$ and $H_{4\ell}(X)$ are $j(\frac{1}{2}(1 + \sqrt{-\ell}))$ and $j(\sqrt{-\ell})$ resp.. ⌟

Proof: For $D = \ell$ or -4ℓ, since the complex conjugation is compatible with the correspondence in(15.8.6.2), and because $I\overline{I} = \mathrm{Nm}(I)\mathcal{O}_D$, so the fixed points of $\mathfrak{c}$ are just 2-torsions in $\mathrm{Pic}(\mathcal{O}_D)$. But $\mathrm{Pic}(\mathcal{O}_D)$ is odd by(14.4.3.8), thus the only real j-value corresponds to the trivial class. □

Cor. (15.8.6.17). For any $j \in \mathbb{R}$, for $\ell \equiv -1 \pmod 4 \in \mathbf{P} \setminus \{3\}$ sufficiently large, $H_{-\ell}(j) > 0$ and $H_{-4\ell}(j) < 0$. ⌟

Proof: This is because $j(\frac{1}{2}(1+\sqrt{-\ell})) \to -\infty$ and $j(\sqrt{-\ell}) \to \infty$ as $\ell \to \infty$, by the power expansion(20.2.4.22). □

Applications

Prop. (15.8.6.18). For $p \in \mathbf{P}$,

- $$\sum_{x\in\mathbb{F}_p} \left(\frac{x^3+x}{p}\right) = \begin{cases} 0 & , p \equiv 3 \pmod 4 \\ -2a & , p = a^2+4b^2, a \equiv 1 \pmod 4 \end{cases}.$$
- $$\sum_{x\in\mathbb{F}_p} \left(\frac{x^3+1}{p}\right) = \begin{cases} 0 & , p \equiv 2 \pmod 3 \\ -2a & , p = a^2+3b^2, a \equiv 1 \pmod 3 \end{cases}.$$
- $$\sum_{x\in\mathbb{F}_p} \left(\frac{x^3+x}{p}\right) = \begin{cases} 0 & , \left(\frac{p}{7}\right) = -1 \\ -2a & , p = a^2+7b^2, \left(\frac{a}{7}\right) = 1 \end{cases}.$$

⌟

Proof: Because these corresponds to elliptic curves with CM by an imaginary quadratic field with class number 1, thus there exists , so the trace of φ_p can be determined.(**?** How, can it be lifted into $\mathcal{O}_{\mathcal{K}}$?). □

Supersingular Primes

References are [Elk87] and [Suw19].

Lemma (15.8.6.19). Let $k \in \mathtt{Field}^p$ and $E \in \mathcal{E}\mathrm{ll}/k$, E is supersingular iff there exists an order $\mathcal{O}$ of an imaginary quadratic field $\mathcal{K}$ s.t. $\mathcal{O} \subset \mathrm{End}(E)$ and p doesn't split in $\mathcal{K}$. ⌟

Proof: By(15.11.3.6), if it is ordinary, then $\mathrm{End}(\mathcal{O})$ is a $\mathbb{Z}$-order in an imaginary quadratic field $\mathcal{K}$. Then consider the p-adic representation

$$\mathcal{K} \otimes \mathbb{Q}_p = \mathrm{End}(E) \otimes \mathbb{Q}_p \to \mathrm{End}_{\mathbb{Q}_p}(V_p(E)) \cong \mathbb{Q}_p.$$

Then this map has a kernel, so $\mathcal{K} \otimes \mathbb{Q}_p$ is not a field, and p splits in $\mathcal{K}$. □

Thm. (15.8.6.20) [Supersingular Criterion for CM Elliptic Curves, Deuring]. Let $F \in \mathtt{NField}$ and $E \in \mathcal{E}\mathrm{ll}/F$ with CM by an imaginary quadratic field $\mathcal{K}$. If $\mathfrak{p} \in \Sigma_F^p$ is a good reduction for E, then $\widetilde{E}/\kappa(\mathfrak{p})$ is ordinary/supersingular iff p is split/non-split in $\mathcal{K}$. ⌟

Proof: Cf.[Lang, Elliptic Functions, Thm13.12].**?** □

Cor. (15.8.6.21) [Supersingular Reductions for CM Elliptic Curves]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ with CM by $\mathcal{K}$, then

$$\#\{p \in \mathbf{P}, p \le X | \widetilde{E}/\mathbb{F}_p \text{ is supersingular elliptic}\} = \frac{X}{2\log X} + O(\frac{X}{\log X}).$$

⌟

Proof: This follows from the effective Chebotarev density theorem(14.6.5.4). □

Prop. (15.8.6.22) [Elkies]. For any $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$, there are infinitely many $p \in \mathbf{P}$ s.t. $\widetilde{E}/\mathbb{F}_p$ is supersingular elliptic. (This is also true if $\mathbb{Q}$ is replaced by a real field, Cf.[Elkies, 1989]). ⌟

Proof: By Deuring's CM-lifting lemma(15.8.6.11), for $D = -\ell$ or -4ℓ, $\widetilde{E}/\mathbb{F}_p$ has CM by $\mathcal{O}_D$ iff $H_D(j(E)) = 0 \in \mathbb{F}_p$. So by(15.8.6.19), p is a supersingular prime for E if

- $H_{-\ell}(j(E)) \in p\mathbb{Z}_p$ or $H_{-4\ell}(j(E)) \in p\mathbb{Z}_p$, and
- $\mathrm{ord}_p(\ell)$ is odd or $-\ell$ is a quadratic non-residue modulo p.

Suppose that there is a finite set S containing all the supersingular primes of E, assume $2 \in S$. By Dirichlet's theorem, there exists $\ell \in \mathbf{P}$ sufficiently large s.t.

$$\ell \equiv 3 (\mathrm{mod}\ 4), \quad \left(\frac{p}{\ell}\right) = 1, \quad p \in S.$$

Then by quadratic reciprocity, if $p \in \mathbf{P}$ and $H_{-\ell}(j(E)) \in p\mathbb{Z}_p$ or $H_{-4\ell}(j(E)) \in p\mathbb{Z}_p$, then $p \neq \ell$ and $\left(\frac{p}{\ell}\right) = 1$, otherwise there would be a new supersingular prime for E that is not in S.

As $H_{-\ell}, H_{-4\ell} \in \mathbb{Z}[X]$, for any $p \in \mathbf{P}$,

$$H_{-\ell}(j(E))^{-1} \in p\mathbb{Z}_p \iff j(E)^{-1} \in p\mathbb{Z}_p \iff H_{-4\ell}(j(E))^{-1} \in p\mathbb{Z}_p,$$

and if $j(E)^{-1} \in p$, then

$$\mathrm{ord}_p(H_{-\ell}(j(E))^{-1}) + \mathrm{ord}_p(H_{-4\ell}(j(E))^{-1}) = \mathrm{ord}_p(j(E)^{-1}) \cdot (\deg(H_{-\ell}) + \deg(H_{-4\ell}))$$

which is even by(15.8.6.15). And $H_{-\ell}(j(E))H_{-4\ell}(j(E)) < 0$ by(15.8.6.17). So $H_{-\ell}(j(E))H_{-4\ell}(j(E))$ would be a quadratic non-residue modulo ℓ by our hypothesis. But this contradicts(15.8.6.15). □

Without CM case

Thm. (15.8.6.23) [Serre]. For $F \in$ `NField` and $E \in \mathcal{E}\mathrm{ll}/F$ without CM, $\rho_E(\mathrm{Gal}_F) \subset \mathrm{GL}(2; \mathbf{A}^f)$ has finite index. ⌟

Proof: Cf.[Abelian l-adic representations and elliptic curves, Serre]. or [Bounds for Serre's open image theorem for elliptic curves over number fields]. □

Conj. (15.8.6.24) [Lang-Trotter]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ without CM,

$$\#\{p \in \mathbf{P}, p \leq X | \widetilde{E}/\mathbb{F}_p \text{ is supersingular elliptic}\} \sim \frac{\sqrt{X}}{\log X}.$$

⌟

Proof: □

Prop. (15.8.6.25) [Serre-Elkies]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ without CM,

$$\#\{p \in \mathbf{P}, p \leq X | \widetilde{E}/\mathbb{F}_p \text{ is supersingular elliptic}\} \leq X^{3/4+\varepsilon}.$$

In particular, supersingular primes have density 0. ⌟

Proof: [N. D. Elkies. Distribution of supersingular primes. Asterisque, (198-200):127–132 (1992), 1991. Journe´es Arithme´tiques, 1989]. □

Conj. (15.8.6.26) [Sato-Tate]. Let $F \in \texttt{NField}$ and $E \in \mathcal{E}\mathrm{ll}/F$ without CM, then for any place v, define $a_v = q_v + 1 - \#\widetilde{E}_v(\kappa_v)$, then by Weil conjecture, $|a_v| \le 2\sqrt{q_v}$, Let $a_v/2\sqrt{q_v} = \cos\theta_v, 0 \le \theta \le \pi$, then $\{\theta_v\}$ for places v leveled by q_v has distribution density $\frac{2}{\pi}\sin^2\theta$. ⌟

Proof: □

Remark (15.8.6.27) [Clozel-Harris-Shepherd-Barron-Taylor]. If $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ with $j(E) \notin \mathbb{Z}$, then the Sate-Tate conjecture(15.8.6.26) is true. ⌟

Proof: [Clozel-Harris-Taylor, Automorphy for some ℓ-adic lifts of automorphic mod ℓ representations], [A family of Calabi-Yau varieties and potential automorphy]. □

Cor. (15.8.6.28) [Birch]. Given $p \in \mathbf{P}$, for any $E \in \mathcal{E}\mathrm{ll}/\mathbb{F}_p$, define $a_v(E) = p + 1 - \#\widetilde{E}_v(\mathbb{F}_p)$ and $a_v(E)/2\sqrt{p} = \cos\theta_p(E), 0 \le \theta \le \pi$, then the distribution density of $\{\theta_p(E)\}$ for $E \in \mathcal{E}\mathrm{ll}/\mathbb{F}_p$ tends to $\frac{2}{\pi}\sin^2\theta$ for $p \to \infty$ when $p \to \infty$. ⌟

Proof: ? □

7 Singular Moduli

References are [Traces of Moduli, Zagier], and [On Singular Moduli, Gross-Zagier].

Def. (15.8.7.1) [Singular Moduli]. A **singular modulus** is a number $j(\tau) \in \mathbb{C}$ where $\tau \in \mathcal{K} \setminus \mathbb{Q}$ and $\mathcal{K}$ is an imaginary quadratic field. ⌟

8 CM Modular Forms

Def. (15.8.8.1) [CM Modular Forms]. A **CM modular form** is a modular form constructed from a binary quadratic form $Q(a,b)$ and a spherical polynomial $P(a,b)$ of order d.

For example,

$$f(z) = \sum_{a \equiv 1 \pmod 4, 2|b} a q^{a^2+b^2}$$

is a modular form, which corresponds exactly to $L(E,s)$, where $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q} : y^2 = x^3 + x$. ⌟

Proof: Cf.[1-2-3 of Modular Forms, P93].? □

Prop. (15.8.8.2). For $n \in 2\mathbb{Z}_+$, $\eta(z)^n$ is a CM modular form iff $n \in \{2, 4, 6, 8, 10, 14, 26\}$. For example,

$$\eta(z) =$$

⌟

Proof: Cf.[Serre1985, Sur la lacunarité des puissances de]. □

Prop. (15.8.8.3) [Lacunary of CM Modular Forms]. ⌟

Proof: Cf.[Serre1981, Quelques applications du théorème de densité de Chebotarev]. □

15.9 Surfaces and Arithmetic Surfaces

Main references are [Sil99], [Liu Qing].

Notation (15.9.0.1).
- In this section, let $S \in \mathcal{S}ch$ be a Dedekind scheme with generic point η or a spectrum of a field, and $\eta = S$.

⌟

1 over Fields

Main references are [Liu Qing, Algebraic Geometry and Arithmetic Curves].

Prop. (15.9.1.1) [27-Lines]. Any smooth cubic surface in $\mathbb{P}^3_k$ contains exactly 27 lines. ⌟

Proof: □

Prop. (15.9.1.2). Any birational transformation of non-singular surfaces will be factorized into f.m blowing-ups and blowing-downs of points. ⌟

Proof: □

Prop. (15.9.1.3). Any smooth surface over a field k is projective. ⌟

Proof: Cf.[Badescu, Algebraic Surfaces]Thm1.28. □

Prop. (15.9.1.4) [Non-Projective Smooth Proper Threefold]. Cf.[Vak17]P671. ⌟

Proof:

□

Resolution of Surfaces

Cf.[Sta]Chap51.

Regular Surfaces

2 Fibered presurfaces

Def. (15.9.2.1) [fibered presurfaces]. Let $S \in \mathcal{S}ch$ be Dedekind, a **fibered presurface** over S is proper? flat S-scheme integral of dimension 2. ⌟

Prop. (15.9.2.2). Let $S \in \mathcal{S}ch$ be Dedekind, X a fibered presurface over S, then X_s has dimension 1 for any $s \in S$, and X_η is a precurve. ⌟

Proof: Cf.[Qing Liu]P348. □

Example (15.9.2.3). Let $q \in \mathbb{Z}_+$ be a square-free integer, then $\mathcal{C} = \mathbf{Proj}(\mathbb{Z}[X, Y, Z]/(X^q + Y^q + Z^q))$ is a normal fibered presurface over Spec Z. ⌟

Proof: Cf.[Qing Liu]P455. □

Prop. (15.9.2.4) [Horizontal and Vertical Divisors]. Let $S \in \mathcal{S}ch$ be Dedekind, X a fibered presurface over S, then

- If x is a closed point of X_η, then $\overline{\{x\}}$ is an integral closed subscheme of X that is finite surjective over S, called a **horizontal divisor**.
- If $D \subset X$ is a prime Weil divisor, then D is either a horizontal divisor, or an integral component of a special fiber, called a **vertical divisor**.
- If $x_0 \in X$ is closed, then $\dim \mathcal{O}_{X,x_0} = 2$.

Moreover, call a Weil divisor D on X horizontal or vertical if it consists of horizontal or vertical prime divisors. ⌟

Proof: Cf.[Qing Liu]P349. □

Prop. (15.9.2.5) [Generically Smoothness]. Let $S \in \mathcal{S}\mathrm{ch}$ be Dedekind and $\pi : X \to S$ be a fibered presurface s.t. X_η is smooth, then there is a dense open subscheme $V \subset S$ s.t. $\pi^{-1}(V) \to V$ is smooth. ⌟

Proof: Cf.[Qing Liu]P352. □

Regular Fibered Presurfaces

Prop. (15.9.2.6) [Regular Fibered Presurfaces are Projective]. Let S be affine and X/S be a flat morphism with fibers of dimension 1, then X/S is projective. In particular, a regular fibered presurface is projective. ⌟

Proof: Cf.[Qing Liu]P353. □

Prop. (15.9.2.7) [Sections are Regular]. Let $\pi : \mathcal{C} \to S$ be a regular fibered presurface and $s \in S$, then

- If $s \in S$ is closed and $x \in \mathcal{C}_s$ is closed, then $\mathcal{C}_s$ is regular at x iff $\pi^\sharp(\mathfrak{p}_s) \not\subseteq \mathfrak{m}_x^2$.
- If $P : U \to \mathcal{C}$ is a rational section, then $\mathcal{C}_p$ is smooth at $P(s)$ for $s \in U$.

⌟

Proof: 1: This is because $\mathcal{O}_{\mathcal{C}_s,x} = \mathcal{O}_{\mathcal{C},x}/\pi^\sharp(\mathfrak{p}_s)$, $\mathfrak{m}_{\mathcal{C}_s,x} = \mathfrak{m}_{\mathcal{C},x}/\pi^\sharp(\mathfrak{p}_s)$ and use the definition of regularity.

2: We show that $\pi^\sharp(\mathfrak{p}_s) \not\subseteq \mathfrak{m}_x^2$: Suppose otherwise, then

$$\mathfrak{p}_s = (\pi \circ P)^\sharp(\mathfrak{p}_s) \subset \pi^\sharp(\mathfrak{m}_x^2) = \mathfrak{p}^2,$$

which is impossible. □

Cor. (15.9.2.8). Let $\mathcal{C}/S$ be a regular fibered presurface, then $\mathcal{C}(S) = \mathcal{C}_{\mathrm{sm}}(S)$. If moreover $\mathcal{C}/S$ is proper, then $\mathcal{C}(S) = \mathcal{C}_{\mathrm{sm}}(S) = \mathcal{C}_\eta(K)$. ⌟

Example (15.9.2.9).

- $\mathcal{C} \subset \mathbb{P}^2_{\mathbb{Z}}$ defined by the equation $y^2 = x^3 + 2x^2 + 6$ is a regular fibered presurface over $\mathbb{Z}$ with 3 singular points.
- $\mathcal{C} \subset \mathbb{P}^2_{\mathbb{Z}}$ defined by the equation $y^2 = x^3 + 2x^2 + 6$ is not regular at $(x, y, 2)$.

⌟

Proof: 1: The determinant $\Delta = -2^6 \cdot 3 \cdot 97$, so it is has three singular fibers $\mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_{97}$:

$$\mathcal{C}_2 : y^2 = x^3, \quad \mathcal{C}_3 : y^2 = x^2(x+2), \quad \mathcal{C}_{97} : y^2 = (x+66)^2(x+64).$$

By(15.11.1.16), they are singular at a single point, and we check these points are regular in $\mathcal{C}$:

For $\mathcal{C}_2$, the singular point is defined by $(x, y, 2)$, and has residue field $\mathbb{F}_2$. To show it is regular, it suffices to show that $(x, y, 2)/(x, y, 2)^2$ is generated by 2 elements x, y: $2 = 3^{-1}(y^2 - x^3 - 3x^2)$. The $\mathcal{C}_3, \mathcal{C}_{97}$ cases are similar. □

3 Arithmetic Surfaces

Def. (15.9.3.1) [Arithmetic Surfaces]. An **arithmetic surface** is a flat of f.t. over S that is integral normal and excellent, such that its generic fiber is a non-singular projective curve, and its special fibers are unions of curves. ⌟

Prop. (15.9.3.2). Any arithmetic surface is regular in codimension 1. ⌟

Prop. (15.9.3.3) [Mordell-Weil for Function Fields]. Let $\mathcal{E} \to C$ be an elliptic surface defined over a field k. Let $E/K(C)$ be the generic fiber. If k is a number field or $\mathcal{E}/C$ is not split, then $E(K(C))$ is a f.g. Abelian group. ⌟

Proof: Cf.[Sil99]P230. □

4 Intersection Theory

Def. (15.9.4.1) [Canonical Divisors]. $K_{X/S}$, Cf.[Qing Liu]P389. ⌟

Def. (15.9.4.2) [Vertically Nef]. Let X/S be a regular fibered presurface, then $D \in \mathrm{Cl}(X)$ is called **vertically nef** if $D \cdot C \geq 0$ for any vertical divisor C. ⌟

Prop. (15.9.4.3) [Factorization Theorem]. Any birational morphism of regular fibered presurfaces over S is a finite composition of blowing-up along a single closed point. ⌟

Proof: Cf.[Qing Liu]P395. □

Arithmetic Surfaces

Prop. (15.9.4.4) [Intersection between Vertical Divisors]. Let X/S be an arithmetic surface and $s \in S$ a closed point, then for any $\Gamma \in \mathrm{Div}_s(X)$, $\Gamma \cdot X_s = 0$. In particular, if $\Gamma_1, \ldots, \Gamma_r$ are irreducible components of X_s of multiplicities $d_1, \ldots, d_r$, then

$$\Gamma_i^2 = -\frac{d_j}{d_i} \sum_{j \neq i} \Gamma_i \cdot \Gamma_j \leq 0.$$

⌟

5 Minimal Arithmetic Surfaces

Def. (15.9.5.1) [Exceptional Divisors]. Let X/S be a regular fibered presurface, then an **exceptional divisor** or (-1)**-curve** $E \subset X$ is a prime divisor s.t. there is a morphism of regular fibered presurfaces $f : X \to Y$ s.t. $f(E)$ is a closed point. Notice an exceptional divisor must be a vertical divisor. ⌟

Prop. (15.9.5.2) [Castelnuovo's criterion, Lichtenbaum/Shafarevich]. Let X/S be a regular fibered presurface, $E \subset X_s$ a vertical prime divisor. Let $k' = H^0(E, \mathcal{O}_E)$, then E is an exceptional divisor iff $E \cong \mathbb{P}^1_{k'}$. And this is the case if $E^2 = -[k' : k(s)]$. ⌟

Proof: Cf.[Qing Liu]P416. □

Prop. (15.9.5.3) [Characterizing Exceptional Divisors]. Let X/S be a regular fibered presurface, then for a vertical prime divisor E on X,

- E is exceptional iff $K_{X/S} \cdot E < 0$(15.9.4.1) and $E^2 < 0$. And in this case, $K_{X/S} \cdot E = E^2$.
- If $\dim S = 0$ and $H^0(X, [\omega_{X/S}]^q) \neq 0$ for some $q \geq 1$ or $\dim S = 1$ and $p_a(X_\eta) > 0$, then E is exceptional iff $K_{X/S} \cdot E < 0$.

⌟

Proof: Cf.[Qing Liu]P417. □

Def. (15.9.5.4) [Minimal Surfaces]. A **relatively minimal surface** over S is a regular fibered presurface $\mathcal{C}/S$ s.t. for any other such regular fibered presurface $\mathcal{C}'$ and any birational morphism $\mathcal{C} \to \mathcal{C}'$ is an isomorphism. Equivalently, $\mathcal{C}$ is a regular proper model that doesn't contain an exceptional curve of the first kind, i.e. cannot be blown down by(15.9.4.3). Cf.[Sta]0C21.

A **minimal surface** over S is a regular fibered presurface $\mathcal{C}/S$ s.t. for any other such regular fibered presurface $\mathcal{C}'$ and any birational map $\mathcal{C}' \to \mathcal{C}$ is a birational morphism. In particular, a minimal surface $\mathcal{C}/S$ is relatively minimal, and $\mathrm{Aut}_S(\mathcal{C}) \cong \mathrm{Aut}_K(\mathcal{C}_\eta)$ is an isomorphism. ⌟

Cor. (15.9.5.5). If a relatively minimal arithmetic surface over S is birational to a minimal surface over S, then they are isomorphic over S. ⌟

Prop. (15.9.5.6) [Étale Descent]. Let X/S be an arithmetic surface with $p_a(X_\eta) > 0$, and $S' \to S$ is an étale covering or $S = \mathrm{Spec}\, R$ where R is a DVR and $S' = \mathrm{Spec}\, \widehat{R}$, then X/S is minimal iff $X \times_S S'/S'$ is minimal. ⌟

Proof: Cf.[Qing Liu]P423. □

Cor. (15.9.5.7). Let X/S be an arithmetic surface with $p_a(X_\eta) > 0$ and $T \to S$ is a smooth morphism, then for any $\xi \in T$ of codimension 1, $X \times_S \mathcal{O}_{T,\xi}$ is a minimal regular surface over $\mathcal{O}_{T,\xi}$. ⌟

Proof: Cf.[Qing Liu]P424. □

Minimal Models

Prop. (15.9.5.8) [Minimal Models]. Let $\mathcal{C}/S$ be a normal fibered presurface, then a **regular model** for $\mathcal{C}/S$ is a regular fibered presurface $\mathcal{C}'/S$ with a birational map $\mathcal{C}' \to \mathcal{C}$ over S. Notice $\mathcal{C}'_\eta \to \mathcal{C}_\eta$ is a birational map of regular projective precurve, thus an isomorphism.

A (relatively)**minimal model** for $\mathcal{C}/S$ is a regular model for $\mathcal{C}/S$ that is (relatively) minimal. Notice if a minimal model exists, it is unique up to a unique isomorphism. ⌟

Lemma (15.9.5.9). If X/S is an arithmetic surface, then there exists only f.m. fibers X_s containing an exceptional divisor. ⌟

Proof: Cf.[Qing Liu]P420. □

Prop. (15.9.5.10) [Blowing Down to Relatively Minimal Surfaces]. If X/S is an arithmetic surface, then X is a finite blowing-up of relatively minimal arithmetic surface over S. ⌟

Proof: The number of exceptional divisors decreases along contractions? □

Prop. (15.9.5.11) [Lichtenbaum/Shafarevich]. Let X/S be an arithmetic surface with $p_a(X_\eta) \geq 1$, then X admits a unique minimal model over S. ⌟

Proof: Cf.[Qing Liu]P422. □

Remark (15.9.5.12). This is not true for $p_a(X_\eta) = 0$, Cf.[Qing Liu]P422. ⌟

Cor. (15.9.5.13) [Minimal and Relatively Minimal Surfaces]. If X/S is an arithmetic surface s.t. $p_a(X_\eta) > 1$, then X is minimal iff it is relatively minimal iff $K_{X/S}$ is vertically nef, by(15.9.5.5) and(15.9.5.4)(15.9.5.3). ? In the field case, why the hypothesis is satisfied? ⌟

Cor. (15.9.5.14). If X/S is a smooth arithmetic surface, then X/S is relatively minimal by(15.9.4.4) as in this case X_s is a disjoint union of irreducible curves. And if $p(X_\eta) > 0$, then X is minimal. ⌟

15.10 Reductions

1 Semistable Reductions

Def. (15.10.1.1) [Models]. Let S be a Dedekind domain with function field K and X an algebraic K-scheme, a **model over** S for X is a proper flat f.t. S-scheme $\mathcal{X}$ s.t $\mathcal{X} \times_S K \cong X$. ⌟

Def. (15.10.1.2) [Good Reduction]. Let (R, K, k) be a CDVR and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}}/K$, X is said to have **good reduction** over R if there is a smooth model $\mathcal{X}$ for X. If this is the case, then $\widetilde{X} = \mathcal{X}_k$ is a smooth scheme over k, called the **reduction of** X.

In this case, the reduction map $X(\overline{K}) \cong \mathcal{X}(\mathcal{O}_{\overline{K}}) \to \widetilde{X}(\overline{k})$ is surjective, by valuation criterion and formal smoothness criterion. ⌟

2 Reduction of Curves

Main references are [Sta]Chap55 and [Qing Liu].

Def. (15.10.2.1) [Semistable and Stable Unions of Curves]. Let $k \in \mathtt{Field}, k$, C an algebraic union of curves over k, then C is called a **semistable union of curves** iff $C_{\overline{k}}$ is reduced and the singular points of $C_{\overline{k}}$ are all ordinary double points. C is called a **stable union of curves** if moreover it satisfies:

- $C_{\overline{k}}$ is connected and projective, with $p_a(C) \geq 2$.
- Let Γ be an integral component of C that is isomorphic to $\mathbb{P}^1_k$, then it meets other integral components at at least 3 points.

⌟

<u>**Minimal Models**</u>

Def. (15.10.2.2) [Minimal Models]. Let R be a DVR with fraction field K. Let C be a smooth projective curve over K, then a **minimal model for** C is a regular proper model $\mathcal{C}$ for C s.t. for any other such model $\mathcal{C}'$, any birational map of models $\mathcal{C} \to \mathcal{C}'$ is an isomorphism.

Equivalently, $\mathcal{C}$ is a regular proper model that doesn't contain an exceptional curve of the first kind, i.e. cannot be blown down**?** Cf.[Sta]0C21. ⌟

Prop. (15.10.2.3) [Resolution of Singularities for Arithmetic Surfaces]. Let (R, K) be a DVR, C a smooth projective curve over K of genus g. Then there exists a proper regular model for C. ⌟

Proof: Cf.[Sil99] □

Thm. (15.10.2.4) [Minimal Model for Curves]. Let (R, K) be a Dedekind domain and C a smooth projective precurve over K of genus≥ 1, then there exists a minimal model $\mathcal{C}$ for C(15.10.2.2).

Moreover, for any other regular proper model $\mathcal{C}'$, there exists a unique domination map $\mathcal{C}' \to C$. ⌟

Proof: Cf.[Sil99]. □

Prop. (15.10.2.5) [Semistable Reductions]. Let (R, K) be a DVR, for a smooth complete curve C over K, the following are equivalent:

- There exists a proper model of C that is at-most-nodel of relative dimension 1 over R.
- There exists a minimal model of C that is at-most-nodel of relative dimension 1 over R.

- Any minimal model of C that is at-most-nodel of relative dimension 1 over R.

If this is the case, then C is said to have **semistable reduction**. ⌟

Proof: Cf.[Sta]0CDG. □

Prop. (15.10.2.6)[Good Reductions]. Let R be a DVR with fraction field K, for a smooth projective curve C over K, the following are equivalent:

- C has good reduction over R.
- There exists a minimal model of C that is smooth over R.
- Any minimal model of C is smooth over R.

⌟

Proof: Cf.[Sta]0CDI. □

Good Reduction for Curves

Prop. (15.10.2.7) [Reduction of Morphisms]. For any morphism $\varphi : C \to C'$ of smooth projective curves over $\mathbb{Q}$ with good reduction at p and $g(C') > 0$, there exists a unique reduction morphism $\widetilde{\varphi} : \widetilde{C} \to \widetilde{C}'$ that commutes with the reduction map(15.10.1.2). This defines a functor from the category of smooth projective curves of positive genus with good reduction to the category of smooth curves over $\mathbb{F}_p$.

Moreover, $\deg(\varphi) = \deg(\widetilde{\varphi})$, and by(15.10.1.2), if φ is surjective, $\widetilde{\varphi}$ is also surjective. And φ is an isomorphism iff $\widetilde{\varphi}$ is an isomorphism. ⌟

Proof: Cf.[BLR90]Prop 9.5.1**?** □

Cor. (15.10.2.8). If $\varphi : E \to E'$ is an isogeny of elliptic curves over $\mathbb{Q}$ with good reduction at p, then the reduction morphism $\widetilde{\varphi} : \widetilde{E} \to \widetilde{E}'$ is also an isogeny. ⌟

Proof: Because it maps $\widetilde{O}_E$ to $\widetilde{O}_{E'}$ and is surjective, this follows from(15.7.1.4). □

Prop. (15.10.2.9)[Pushforward of Divisors]. Let C be a smooth projective curve over $\mathbb{Q}$ with good reduction at p, then the reduction map $X(\overline{K}) \to \widetilde{X}(\overline{F}_p)$ induces a map

$$\mathrm{Div}^0(X) \to \mathrm{Div}^0(\widetilde{X})$$

that maps principal divisors to principal divisors, so inducing a map $\varphi_* : \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(C')$, which is compatible with pushforward of divisors along morphisms of curves: if $h : C \to C'$ is a morphism of smooth projective curves over $\mathbb{Q}$ with good reductions at p, then the following digram is commutative:

$$\begin{array}{ccc} \mathrm{Pic}^0(C) & \xrightarrow{h_*} & \mathrm{Pic}^0(C') \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0(\widetilde{C}) & \xrightarrow{\widetilde{h}_*} & \mathrm{Pic}^0(\widetilde{C}') \end{array}$$

⌟

Proof: Cf.[BLR90]Prop 9.5.1**?** □

Classification of Special Fibers of the Minimal Regular Models of Curves of Genus 2

Cf.[Y. Namikawa, K. Ueno, The complete classification of fibers in pencils of curves of genus two, Manuscripta Math. 9 (1973), 143–186.] and [A. P. Ogg, On pencils of curves of genus two, Topology 5 (1966), 355–362.].

15.11 Arithmetic of Elliptic Curves

Main References are [Sil16] and [Sil99], [Sil11]. Should add Sutherland's noteshttps://math.mit.edu/classes/18.783/2017/lectures.htmlL2-11, 13-14, 17-24. and Snowden's noteshttp://www-personal.umich.edu/~asnowden/teaching/2013/679/index.htmlL5,6,7,9,11, 14, 15, 17-23.

Notation (15.11.0.1).

- Use notations defined in Arithmetic of Abelian Varieties.
- Use notations defined in Global Fields.

⌟

1 Basics

Def. (15.11.1.1) [Elliptic Schemes]. For $k \in \texttt{Field}$, an **elliptic curve** E over k is a complete non-singular curve of genus 1 over a field k, together with a specified rational pt O. In(15.11.1.10), we will see an elliptic curve is smooth.

More generally, for $S \in \mathcal{S}\mathrm{ch}$, an **Elliptic scheme** $f : E \to S$ is an Abelian scheme over S of relative dimension 1(15.7.1.1). The category of elliptic schemes over S is denoted by $\mathcal{E}\mathrm{ll}\,/S$. ⌟

Remark (15.11.1.2). Elliptic curves are Abelian varieties by(15.11.1.10). Thus the theory of Abelian varieties apply to elliptic curves. ⌟

Prop. (15.11.1.3) [Invertible Sheaf]. Let $S \in \mathcal{S}\mathrm{ch}, E \in \mathcal{E}\mathrm{ll}\,/S$, and $e \in E(S)$ be the unit, then we can define

$$\omega_{E/S} = e^*\Omega_{E/S} = f_*\Omega_{E/S} \cong R^1 f_*\mathcal{O}_E \in \mathcal{M}\mathrm{od}(\mathcal{O}_S),$$

⌟

Proof: □

Weierstrass Theory

Def. (15.11.1.4) [Weierstrass Equations]. A **Weierstrass equations** is an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

⌟

Def. (15.11.1.5) [Important Invariants]. Let $k \in \texttt{Field}, E \in \mathcal{E}\mathrm{ll}\,/k$, given any Weierstrass equation as in(15.11.1.4), we can define

- $b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6, \quad b_8 = a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2.$
- $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ the **discriminant of** E, to determine whether E is singular.
- the quantity $c_4 = b_2^2 - 24b_4$, used in the singular case to determine iff it has a node or cusp.
- the quantity $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$, used to determine twisted elliptic curves(15.11.6.3).
- the j**-invariant** $j = c_4^3/\Delta$, which is used to in the non-singular case to characterize E.

They satisfy the equations:

$$4b_8 = b_2b_6 - b_4^2, \quad 1728\Delta = c_4^3 - c_6^2.$$

⌟

Prop. (15.11.1.6) [Reduced Weierstrass Equations]. Let $k \in \texttt{Field}, E \in \mathcal{E}\mathrm{ll}/k$, given any Weierstrass equation as in(15.11.1.4),

- If $\mathrm{char}\, k \neq 2$, we can replace (x, y) by $(x, y - (a_1 x + a_3)/2)$ to eliminate a_1, a_3 to transform the original Weierstrass equation to
$$y^2 = x^3 + \frac{b_2 x^2 + 2b_4 x + b_6}{4}.$$
- If $\mathrm{char}\, k \neq 2, 3$, then we can further replace (x, y) to $((x - 3b_2)/36, y/216)$ to eliminate b_2 to transform the Weierstrass equation to
$$y^2 = x^3 - 27c_4 x - 54c_6.$$
In particular, E has a Weierstrass equation of the form
$$y^2 = x^3 + a_4 x + a_6, \quad \Delta = -16(4a_4^3 + 27a_6^2), \quad j = 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}$$
- If char $k = 3$, then E has a Weierstrass equation of the form
$$y^2 = x^3 + a_2 x^2 + a_6, \quad \Delta = -a_2^3 a_6, \quad j = -a_2^3/a_6, \text{or} \quad y^2 = x^3 + a_4 x + a_6, \quad \Delta = -a_4^3, \quad j = 0$$
- If char $k = 2$, then E has a Weierstrass equation of the form
$$y^2 + xy = x^3 + a_2 x^2 + a_6, \quad \Delta = a_6, \quad j = 1/a_6, \text{or} \quad y^2 + a_3 y = x^3 + a_4 x + a_6, \quad \Delta = a_3^4, \quad j = 0.$$

⌟

Prop. (15.11.1.7) [Explicit Embedding of Elliptic Curves]. Any $E \in \mathcal{E}\mathrm{ll}/k$ is isomorphic to a plane curve in $\mathbb{P}_k^2$ defined by an affine Weierstrass equation in $k[x, y]$.

And any isomorphism between elliptic curves defined by affine Weierstrass equations over k and fixes $[0, 1, 0]$ are linear maps of the form
$$(X, Y) \mapsto (u^2 X + r, u^3 Y + s u^2 X + t), \quad u \in k^*, s, r \in k.$$

⌟

Proof: If E is an elliptic curve over k, consider a rational point $O \in E(k)$, Riemann-Roch(6.12.2.9) tells $l(nP) = \deg(nP) = n$ for $n \geq 1$. Now $L(kP) = k$ by Riemann-Roch(6.12.2.9). So we choose a basis $1, x$ for $\mathcal{O}_X(2O)$, and extend it to a basis $1, x, y$ of $L(3P)$. Since $L(6O) = 6$, there is a linear relation between the seven elements $1, x, x^2, xy, y^2, x^3$. And y^2, x^3 must occur by observing the pole order at P. Thus by rescaling, we can write the relation as
$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

So x, y defines a rational map of E to $\mathbb{P}^2 : a \mapsto (x(a), y(a), 1)$. This map extends to an embedding of E into $\mathbb{P}^2$, by(6.12.1.15). Moreover, by the above proof, if E' is another Weierstrass form, then $1, x'$ are basis for $\mathcal{O}_X(2O)$ and $1, x', y'$ are basis for $\mathcal{O}_X(3O)$. Thus we have the linear relation between (X, Y) and (X', Y').

To define an Abelian structure on E, first notice that
$$E(k) \to \mathrm{Cl}^0(E) : Q \mapsto [Q] - [P]$$

is an isomorphism. Using Riemann-Roch, it is injective because $l(Q) = 1$ for $Q \in E(k)$, and for any divisor A of degree 0, $L(A+P) > 0$, so there exists an effective divisor that is equivalent to $A+P$, but this must be a rational point $Q \in E(k)$. Thus we can endow $E(k)$ with a group structure inherited from $\mathrm{Cl}^0(E)$. By(15.11.1.9), there is a group variety structure prolonging this construction, so E is a group scheme. □

Remark (15.11.1.8). There is a more advanced way to prove that this is a group action, in [Qing Liu]P492.? ⌟

Lemma (15.11.1.9) [Explicit Group Structure]. Let E be an elliptic curve given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

then the group addition on $E\backslash O$ is given by

- $-(x_0, y_0) = (x_0, -y_0 - a_1x - a_3)$.
- $(x_1, y_1) + (x_2, y_2) = O$ iff $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$. Otherwise

$$(x_1, y_1) + (x_2, y_2) = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3)$$

where

$$\lambda = \begin{cases} \frac{y_1-y_2}{x_1-x_2} & x_1 \neq x_2 \\ \frac{3x^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3} & x_1 = x_2 \end{cases}, \quad \nu = \begin{cases} \frac{y_2x_1-y_1x_2}{x_1-x_2} & x_1 \neq x_2 \\ \frac{-x_1^3+a_4x_1+2a_6-a_3y_1}{2y_1+a_1x_1+a_3} & x_1 = x_2 \end{cases}$$

- (Doubling Formula) $x([2]P) = \frac{x^4-b_4x^2-2b_6x-b_8}{4x^3+b_2x^2+2b_4x+b_6}$.

Thus the group actions defined in(15.11.1.7) are all morphisms. In particular, E is a group variety. ⌟

Proof: Cf.[Sil16]P53. □

Cor. (15.11.1.10) [Elliptic Curves and Abelian Varieties]. If X is an Abelian variety of dimension 1, then X is an elliptic curve. The converse is also true, by(15.11.1.7). In particular, the theory of Abelian varieties15.7 applies to elliptic curves. And we will use notations for Abelian varieties. ⌟

Proof: By(9.1.4.35)(9.1.4.34), the tangent space $\mathcal{T}_{X/k}$ is trivial of rank 1, thus it is a curve of genus 1 by(6.12.1.24). it is also regular, by(6.6.4.16). □

Prop. (15.11.1.11) [Normalized Invariant Differential Form]. Let $k \in \texttt{Field}$ and E a plane cubic over k defined by the equation $W : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Then the differential form given by

$$\omega = \frac{\mathrm{d}x}{2y + a_1x + a_3} = \frac{\mathrm{d}y}{3x^2 + 2a_2x + a_4 - a_1y}$$

is a non-zero section of $\mathcal{K}_{E_{\mathrm{sm}}}$. It is normalized s.t. at the origin, with the uniformizer $z = -x/y$, it has value 1.

Moreover, it is invariant under translation. It is called the **normalized invariant differential form** on E w.r.t W. ⌟

Proof: Firstly we show $\mathrm{div}(\omega) = 0$: consider a finite smooth point $P_0 = (x_0, y_0)$, then it cannot have pole, otherwise P_0 is singular. Because $x - x_0 \in L(2O)$, $\mathrm{ord}_{P_0}(x - x_0) \leq 2$, and if $\mathrm{ord}_{P_0}(x - x_0) = 2$, $\mathrm{ord}_{P_0}(y - y_0) \geq 2$ also by inspecting the Weierstrass equation. Thus $\mathrm{ord}_P(\omega) = 0$. Then consider the situation at O: $\mathrm{ord}_O(x) = -2, \mathrm{ord}_O(y) = -3$, thus $\mathrm{ord}_O(\frac{\mathrm{d}x}{2y+a_1x+a_3}) = 0$ except possibly $\mathrm{char}\, k = 2$.

But the same calculation shows $\mathrm{ord}_O(\frac{dy}{3x^2+2a_2x+a_4-a_1y}) = 0$ except possibly when $\mathrm{char}\, k = 3$. Thus we are done.

Now any translation action induces a map $\tau_x^*\omega = a(x)\omega$, where $a \in K(C)^\times$. But $a(x)$ has no pole and zeros, thus $a(x) \in k^\times$. But then $a(x)$ is rational function with no zero and poles, thus $a(x) = a(O) = 1$. □

Cor. (15.11.1.12). $[m]_E^*\omega = \mathrm{pr}_1^*\omega + \mathrm{pr}_2^*\omega$. ⌟

Proof: It follows from this and the see-saw principal that $m_E^*\mathcal{K}_E \cong \mathrm{pr}_1^*\mathcal{K}_E \otimes \mathrm{pr}_2^*\mathcal{K}_E$. □

Prop. (15.11.1.13) [Change of Variables]. A change of variables of the form (x, y) replaced by $(u^2x + a, u^3y + bx + c)$ changes c_4 to $u^{-4}c_4$, c_6 to $u^{-6}c_6$, Δ to $u^{-12}\Delta$, and preserves j. ⌟

Proof: This is just a equation of identities, so it suffices to prove for k of characteristic 0, then in this case, by(15.11.1.6), c_4, c_6 is just the coefficients of the Weierstrass equation transformed into the reduced form(times a constant). So it suffices to prove for transformation between reduced Weierstrass equations. In this case, $a = b = c = 0$, and the assertion is clear. □

Prop. (15.11.1.14) [Characterizing Singularities]. Let $k \in$ `Field`, then

- The plane cubic E over k defined by a Weierstrass formula f is never singular at $O = [0, 1, 0]$, and it is a curve.
-
  - E is smooth iff its determinant $\Delta \neq 0$. And in this case it is an elliptic curve by genus formula.
  - E has a node iff $\Delta = 0$ and $c_4 \neq 0$.
  - E has a cusp iff $\Delta = c_4 = 0$.
- For $E, E' \in \mathcal{E}\mathrm{ll}/k$, $E_{\overline{k}} \cong E'_{\overline{k}}$ iff $j(E) = j(E')$. In fact, they are isomorphic over a separable field extension k'/k of degree 24, and if $j \neq 0, 1728$, then they are isomorphic over a separable field extension k'/k of degree 2.

⌟

Proof: 1: Firstly, E is never singular at $[0, 1, 0]$: On $U(z)$, the curve is given by $z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$, which is not singular at $(0, 0)$. Secondly, E has genus 1. Finally it is a curve by(3.2.3.14) and checking f doesn't has a root $y \in \overline{k}(x)$: This is true by degree reasons using reduced Weierstrass equations(15.11.1.6).

2: (1): By(15.11.1.10), non-singular is equivalent to smoothness. So we may base change to $\overline{k}$. If P is non-singular, linearly transform it to $(0, 0)$, then by Jacobian criterion, $\frac{\partial}{\partial x}f = \frac{\partial}{\partial y}f = 0$, so $a_3 = a_4 = a_6 = 0$, and it can be verified that $\Delta = 0$. Conversely, if $\Delta = 0$, then use the reduced Weierstrass equations and argue case by case, we can find a singular point.

(2), (3): In this case, assume $a_3 = a_4 = a_6 = 0$, then $c_4 = (a_1^2 + 4a_2)^2$, and $E : y^2 + a_1xy - a_2x^2 - x^3 = 0$, so the assertion is clear.

2: We use the reduced Weierstrass equations, derive an equation between their coefficients, and take a suitable change of variables. Details are omitted. □

Prop. (15.11.1.15)[Fields of Moduli]. For any element $j_0 \in \overline{k}$, there exists an elliptic curve over $k(j_0)$ with j-invariant j_0. In particular, any elliptic curve over k is defined over $k(j(E))$, by(15.11.1.14). ⌟

Proof: If $j_0 \neq 0, 1728$, then we can take the curve

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

with $\Delta(E) = \frac{j_0^3}{(j_0-1728)^3}, j(E) = j_0$.

If $j = 0$ or 1728, we can take one of the curves

$$E : y^2 + y = x^3, \quad \Delta = -27, \quad j = 0$$

$$E : y^2 = x^3 + x, \quad \Delta = -64, \quad j = 1728.$$

Notice for $\mathrm{char}\, k = 2$ or 3, $0 = 1728$, and at least one of these are elliptic curves. □

Prop. (15.11.1.16) [Singular Weierstrass]. If $k \in \texttt{Field}$ is perfect or $\mathrm{char}\, k \neq 2, 3$, $E \in \mathbb{P}^2_k$ is a plane cubic given by a Weierstrass equation W is singular, then

- E has a unique singular point, and it is a rational point.
- E is birational to $\mathbb{P}^1_k$, i.e. its non-singular projective model is $\mathbb{P}^1$(6.12.1.18).
- E_{sm} is a commutative k-group under the group action given in(15.11.1.9) with origin $O = [0, 1, 0]$, and $E_{\mathrm{sm}} \cong \mathbb{G}_m$ if E has a split node, and $E_{\mathrm{sm}} \cong \mathbb{G}_a$ if E has a cusp.

⌟

Proof: 1: By(15.11.1.14), the singular points must be a finite point, and $\Delta = 0$. Over $\overline{k}$, the singular points of E is characterized by the equations $W = \frac{\partial}{\partial x} W = \frac{\partial}{\partial y} W = 0$. Then we can use the reduced Weierstrass equations(15.11.1.6): If $\mathrm{char}\, k \neq 2, 3$, then clearly $(x_0, y_0) \in k^2$. The perfect case is similar.

2: Because the curve is never singular at O by(15.11.1.14), by a linear change, we can assume that one of the singular point is $(0, 0)$. Then by Jacobian criterion, it must be of the form

$$y^2 + a_1 xy = x^3 + a_2 x^2.$$

Then the projection along $(0, 0)$ is an isomorphism**?** this is wrong!

$$E \backslash \{0, \infty\} \to \mathbb{P}^1_k \backslash \{[0 : 1]\} : (x, y) \mapsto [x : y]$$

with inverse

$$[1, t] \mapsto (t^2 + a_1 t - a_2, t^3 + a_1 t^2 - a_2 t).$$

E_{sm} is a group scheme because we can verify on closed points, and the fact any line through $(0, 0)$ has multiplicity more than 1. To determine the group structure, Cf.[Sil16]P56**?**. □

Prop. (15.11.1.17) [Legendre Forms]. Let $\mathrm{char}\, K \neq 2$, then

- every elliptic curve over $\overline{K}$ is isomorphic to an elliptic curve in **Legendre form**

$$E_\lambda : y^2 = x(x - 1)(x - \lambda), \quad \lambda \neq 0, 1 \in \overline{K}.$$

- $\Delta(E_\lambda) = 16\lambda^2(\lambda - 1)^2, j(E_\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}, c_4 = 16(1 - \lambda(1 - \lambda))$.
- If K is a valued field, we may take $v(\lambda) \geq 0$ as $j(E_\lambda) = j(E_{\lambda^{-1}})$.
- The map $\overline{K} \to \overline{K} : \lambda \mapsto j(E_\lambda)$ is 6 to 1 except above the points 0 and 1728, where for $\mathrm{char} K \neq 2, 3$, $\# j^{-1}(0) = 2$, $\# j^{-1}(1728) = 3$, and for $\mathrm{char} K = 3$, $j^{-1}(0 = 1728) = 1$.

⌟

Proof: 1: put the Weierstrass equation of E in the reduced form(15.11.1.6), then it is of the form

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

in $\overline{K}[x, y]$, and because $\Delta = 16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2 \neq 0$, so e_1, e_2, e_3 are pairwise distinct. Thus the linear transform

$$x \mapsto (e_2 - e_1)x' + e_1$$

makes the Weierstrass equation in the Legendre form with $\lambda = \frac{e_3 - e_1}{e_2 - e_1}$.

2: Direct calculation.

3: Directly calculating the differential of j.**?** □

Prop. (15.11.1.18)[Duering Normal Form]. Every elliptic curve over $\overline{K}$, except possibly char $K = 3$ and $j(E) = 0$, is isomorphic to an elliptic curve in **Deuring normal form**

$$E_\alpha : y^2 + \alpha xy + y = x^3, \quad \alpha \in \overline{K}, \quad \Delta(E_\alpha) = \alpha^3 - 27 \neq 0, \quad j(E_\alpha) = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27}, \quad c_4 = \alpha(\alpha^3 - 24).$$

And if K is a valued field, we can take $v(\alpha) > 0$. ⌟

Proof: Use(15.11.1.14), it suffices to show that $j(\alpha)$ can take any value $j \in \overline{K}$.

The last assertion is because if $v(\alpha) < 0$, then the product of roots of $\frac{x(x-24)^3}{x-27} = \frac{\alpha^3(\alpha^3-24)^3}{\alpha^3-27}$ other than α is $-72^3/(\alpha - 27)$ has positive valuations. □

Prop. (15.11.1.19) [Automorphism Group]. Let $k \in \texttt{Field}, E \in \mathcal{E}\mathrm{ll}/k$, then the the automorphic group of E is

$$\mathrm{Aut}(E) \cong \begin{cases} \mu_2(k) & j(E) \neq 0, 1728 \\ \mu_4(k) & j(E) = 1728, \mathrm{char}\, k \neq 2, 3 \\ \mu_6(k) & j(E) = 0, \mathrm{char}\, k \neq 2, 3 \\ D_{12} & j(E) = 0 = 1728, \mathrm{char}\, k = 3, k = \overline{k} \\ C_3 \ltimes Q_8 & j(E) = 0 = 1728, \mathrm{char}\, k = 2, k = \overline{k} \end{cases}$$

⌟

Proof: Any automorphism of E is defined by a linear maps of the form

$$(X, Y) \mapsto (u^2 X + r, u^3 Y + su^2 X + t), \quad u \in k^\times, s, r \in K.$$

If char $k \neq 2, 3$, use the reduced Weierstrass form $E : y^2 = x^3 + Ax + B$, so it is of the form $(X, Y) \mapsto (u^2 X, u^3 Y)$, which is possible iff $u^{-4}A = A, u^{-6}B = B$. Thus by arguing case by case, we are done.

The char $k = 2, 3$ cases are similar, use reduced Weierstrass forms(15.11.1.6) and argue case by case. □

Prop. (15.11.1.20) [Dual Elliptic Curves]. An elliptic curve E is canonically isomorphic to its dual $\widehat{E}$, by the mapping $P \mapsto \mathcal{L}(P - O)$. ⌟

Proof: This morphism is induced by the ample line bundle $\mathcal{L}(O)$(15.7.4.3), and it is an isomorphism because it has degree 1, by Riemann-Roch(15.7.5.2). □

Cor. (15.11.1.21). For any $\mathcal{L} \in \mathrm{Pic}(E)$ of degree d, $\varphi_{\mathcal{L}} = [d] : E \to E$ via the canonical duality, because $\mathrm{Pic}^0(E)$ induces trivial maps by(15.7.4.9) and(8.1.12.5). ⌟

Cor. (15.11.1.22)[Characterizing Principal Divisors]. Let $E \in \mathcal{E}\mathrm{ll}/k$ and $D = \sum n_i[P_i] \in \mathrm{Div}(E)$, where P_i are rational points, then D is a principal divisor iff $\sum n_i = 0$ and $\sum[n_i]P_i = O$. ⌟

Proof: Of course $\sum n_i = 0$. In this case, $\sum[n_i]P_i$ is mapped to the line bundle corresponding to $[D] \in \widehat{E}$ via $E \to \widehat{E}$, so $[D] = 0$ iff $\sum[n_i]P_i = O$. □

Isogenies

Prop. (15.11.1.23). Let $\varphi, \varphi' : E' \to E$ be isogenies of elliptic curves over k, and let ω be an invariant differential on E, then by(15.11.1.12),

$$(\varphi + \varphi')^*\omega = \varphi^*\omega + (\varphi')^*\omega.$$

⌟

Cor. (15.11.1.24). $[m]^*\omega = m\omega$. ⌟

Cor. (15.11.1.25) [$\mathrm{End}(E)$ **is Commutative in Characteristic 0].** Let $E \in \mathcal{E}\mathrm{ll}/k$ with the normalized invariant differential form ω, then there is a ring homomorphism

$$\mathrm{End}(E_{\overline{k}}) \to \overline{k} : \varphi \mapsto a_\varphi, \text{where } \varphi^*\omega = a_\varphi\omega.$$

And the kernel is the set of inseparable endomorphisms of $E_{\overline{k}}$. In particular, if $\mathrm{char}\, k = 0$, then $\mathrm{End}(E_{\overline{k}})$ is commutative. ⌟

Proof: Cf.[Sil16]P79.? □

Prop. (15.11.1.26) [Dual Isogenies]. Let $k \in \mathtt{Field}, E, E' \in \mathcal{E}\mathrm{ll}/k$ and $\varphi \in \mathrm{Hom}(E, E')$, then under the canonical isomorphism(15.11.1.20), the dual map $\widehat{\varphi}$ can be regarded as a map $\widehat{\varphi} : E' \to E$. Then

$$\widehat{\varphi} \circ \varphi = [\deg(\varphi)]_E, \varphi \circ \widehat{\varphi} = [\deg(\varphi)]_{E'}.$$

$\mathrm{End}(E) \to \mathrm{End}(E) : \varphi \mapsto \widehat{\varphi}$ is additive, and defines an involution on $\mathrm{End}(E)$. ⌟

Proof: Let $d = \deg(\varphi)$. By unwinding definition, $\widehat{\varphi} \circ \varphi : E \to E' \to \widehat{E}' \to \widehat{E}$ is just $\varphi_{\varphi^*\mathcal{L}(O)}$. But for elliptic curves, $\varphi_{\mathcal{L}}$ only depends on $\deg(\mathcal{L})$, thus $\varphi_{\varphi^*\mathcal{L}(O)} = \varphi_{\mathcal{L}(dO)} = [d]\varphi_{\mathcal{L}(O)}$. The second assertion follows by noticing $\varphi = \widehat{\widehat{\varphi}}$ and $\deg(\varphi) = \deg(\widehat{\varphi})$(15.7.6.4). □

Cor. (15.11.1.27) [$\mathrm{End}(E)$]**.** Let k be a field and $E \in \mathcal{E}\mathrm{ll}/k$, then $\mathrm{End}(E) \otimes \mathbb{Q}$ is a division ring. ⌟

Prop. (15.11.1.28) [Classification of $\mathrm{End}(E)$]**.** Let $k \in \mathtt{Field}, E \in \mathcal{E}\mathrm{ll}/k$, then $\mathrm{End}(E)$ has the following three possibilities:

- $\mathbb{Z}$.
- an $\mathbb{Z}$-order in an imaginary quadratic extension over $\mathbb{Q}$.
- an $\mathbb{Z}$-order in a definite quaternion algebra over $\mathbb{Q}$.

And the third case won't happen in characteristic0, by(15.11.1.25). ⌟

Proof: This follows from(3.6.5.1) and(15.13.2.3). □

2 Formal Groups of Elliptic Curves

In this subsection, the formal group structure of an elliptic is studied.

In this subsection, E is an elliptic curve over a field K given by Weierstrass equation $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$.

Prop. (15.11.2.1) [Calculation of Formal Group Law]. Make a change of variable $z=-x/y, w=-1/y$ to the Weierstrass equation of E, the equation becomes

$$w=z^3+(a_1z+a_2z^2)w+(a_3+a_4z)w^2+a_6w^3=f(z,w).$$

Then

- $\widehat{\mathcal{O}}_{E,O}\cong K[[z]]$.
- There is a unique power series $w(z)\in\mathbb{Z}[a_1,\ldots,a_6][[z]]$ satisfying $w(0)=0$ and $w(z)=f(z,w(z))$.
- $w(z)=z^3(1+A_1z+A_2z^2+\ldots)$, where A_n is a homogenous polynomial in $a_1,\ldots,a_6$, where a_i has weight i.
- $$x(z)=z/w(z)=z^{-2}-a_1z^{-1}-a_2-a_3z-(a_4+a_1a_3)z^2+\ldots\in\mathbb{Z}[a_1,\ldots,a_6][[z]]$$
$$y(z)=-1/w(z)=-z^{-3}+a_1z^{-2}+a_2z^{-1}+a_3+(a_4+a_1a_3)z+\ldots\in\mathbb{Z}[a_1,\ldots,a_6][[z]]$$
- The formal group law of E(15.7.2.1) is given by
$$F(z_1,z_2)=z_1+z_2-a_1z_1z_2-a_2(z_1^2z_2+z_1z_2^2)+(-2a_3z_1^3z_2+(a_1a_2-3a_3)z_1^2z_2^2-2a_3z_1z_2^3)+\ldots\in\mathbb{Z}[a_1,\ldots,a_6][[z_1,z_2]].$$
- The normalized invariant differential form(15.11.1.11)
$$\omega(z)=\frac{dx(z)}{2y(z)+a_1x(z)+a_3}=[1+a_1z+(a_1^2+a_2)z^2+(a_1^3+2a_1a_2+2a_3)z^3+(a_1^4+3a_1^2a_2+6a_1a_3+a_2^2+2a_4)z^4+\ldots]dz\in\mathbb{Z}[a_1,\ldots,a_6][[z]]dz$$
- $$i(z)=\frac{x(z)}{y(z)+a_1x(z)+a_3}=\frac{z^{-2}-a_1z^{-1}+\ldots}{-z^{-3}+2a_1z^{-2}+\ldots}\in\mathbb{Z}[a_1,\ldots,a_6][[z]].$$

In particular, this formal group law is defined over $\mathbb{Z}[a_1,\ldots,a_6]$. ⌟

Proof: $\omega(z)\in\mathbb{Z}[a_1,\ldots,a_6][[z]]dz$ by(9.5.3.16).

For $F(z_1,z_2)$: ? □

Prop. (15.11.2.2) [Inseparable Degree and Heights]. Let K be a field of characteristic $p>0$ and $E_1/K, E_2/K$ be two elliptic curves, and $\varphi:E_1\to E_2$ a non-zero isogeny of elliptic curves over K, and let $\widehat{\varphi}:\widehat{E}_1\to\widehat{E}_2$ be the homomorphism of formal group schemes, then

$$\deg_i(\varphi)=p^{\mathrm{ht}(\widehat{\varphi})}.$$

⌟

Proof: Cf.[Sil16]P134.? □

Cor. (15.11.2.3). Let K be a field of characteristic $p>0$, then $\mathrm{ht}(\widehat{E})=1$ or 2, because $\deg([p]_E)=p^2$(15.7.6.14). ⌟

3 char $k > 0$ case

Notation (15.11.3.1).

- Let $k \in \texttt{Field}^p$,
- Let $E \in \mathcal{E}\mathrm{ll}/k$ be given by a Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

⌟

Prop. (15.11.3.2). Let $k = \mathbb{F}_q$, $\#E(k) \equiv 0 \mod 4$. ⌟

Proof: There are two involutions on E: $(x, y, z) \mapsto (x, -y, z)$, $(x, y, z) \mapsto (z, y/x, x)$. The fixed points of these elements contain

$$(0, 1, 0), \quad (0, 0, 1), \quad (\varepsilon_1, \varepsilon_2\sqrt{2\varepsilon_1}, 0), \quad (\varepsilon_3\sqrt{-1}, 0, 1).$$

Considering either cases s.t. $-1 \in \mathbb{F}_q^2$ or $2 \in \mathbb{F}_q^2$, the number of these points are divisible by 4, thus we are done. □

Prop. (15.11.3.3) [Hasse-Weil]. Let $p \in \mathbf{P}, q = p^r$, $k = \mathbb{F}_q$ and $E \in \mathcal{E}\mathrm{ll}/k$, then

- If $a = 1+q-\#E(\mathbb{F}_q)$, α, β be the two roots of $T^2-aT+q = 0$, then $\#E(\mathbb{F}_{q^n}) = 1+q^n-\alpha^n-\beta^n$.
- $|\#E(\mathbb{F}_q) - 1 - q| \leq 2\sqrt{q}$.
- The Frobenius map $\varphi_E : E \to E$ satisfies $\varphi^2 - a\varphi + [q] = 0$.
- $a = 1 + q - \deg(1 - \varphi)$, and $[a] = \varphi + \widehat{\varphi}$.

⌟

Proof: $1, 2$ are special cases of(15.7.9.3). $3, 4$ follow from(15.7.7.13) and(15.7.6.17). □

Cor. (15.11.3.4). Let $k = \mathbb{F}_q$, $p \neq 2$ and E is given by $y^2 = x^3 + a_2x^2 + a_4x + a_6$, then

$$|\sum_{x\in\mathbb{F}_q}(\frac{x^3 + a_2x^2 + a_4x + a_6}{\mathbb{F}_q})| \leq 2\sqrt{q}.$$

⌟

Proof: This is because $\#E(\mathbb{F}_q) = \sum_{x\in\mathbb{F}_q}(1 + (\frac{x^3+a_2x^2+a_4x+a_6}{\mathbb{F}_q}))$. □

Supersingular Elliptic Curves

Main references are [Igu58].

Def. (15.11.3.5) [Supersingular Elliptic Curve]. Let $p \in \texttt{Prime}, k \in \texttt{Field}^p$, $F_{E/k,r} : E \to E^{(p^r)}$ the relative Frobenius(6.2.10.1), and $\widehat{F}_{E/k}$ be its dual. Then the following are equivalent:

- $E[p^r] = 1$ for all $r \geq 1$.
- $E[p^r] \not\cong \mathbb{Z}/p^r\mathbb{Z}$ for some $r \geq 1$.
- $\widehat{F}_{E/k,r}$ is purely inseparable for one(thus all) r.
- $[p] : E \to E$ is purely inseparable, and $j(E) \in \mathbb{F}_{p^2}$.
- $\mathrm{End}(E)$ is an order in a quaternion algebra.
- The formal group $\widehat{E}/K$ associated to E has height $2(\neq 1)$.

Such curves are called **supersingular elliptic curves**, otherwise E is called an **ordinary elliptic curve**.

Being supersingular is stable and reflective under base change. ⌟

Proof: Cf.[Silverman P144].**?** □

Prop. (15.11.3.6) [Ordinary Elliptic Curves]. Let $k \in \texttt{Field}$, $\operatorname{char} k = p > 0$, $E \in \mathcal{E}\mathrm{ll}/k$ be an ordinary elliptic curve, then

- If $j(E) \in \overline{\mathbb{F}}_p$, then $\mathrm{End}(E)$ is an order in an imaginary quadratic field. In particular, this is the case when k is a finite field.
- If $j(E) \notin \overline{\mathbb{F}}_p$, then $\mathrm{End}(E) \cong \mathbb{Z}$.

⌟

Proof: 1: If $j(E) \in \overline{\mathbb{F}_p}$, then E is defined over some $\mathbb{F}_q$. Let $\varphi = \varphi_q$, then if $\varphi^r \in \mathbb{Z}$, $\varphi^r = [\pm q^r]$, so $\#E[\varphi^r] = \deg_s(\varphi^r) = 1$ by(15.7.6.2), contradicting the fact E is ordinary. Thus the assertion follows from(15.11.1.28).

2: **?** □

Cor. (15.11.3.7). For $E \in \mathcal{E}\mathrm{ll}/\overline{\mathbb{F}_p}$, E is ordinary iff $\mathrm{End}(E)$ is an order in an imaginary quadratic field, and E is supersingular iff $\mathrm{End}(E)$ is an order in a quaternion algebra. ⌟

Def. (15.11.3.8) [Hasse Invariant]. The **Hasse invariant** for E is a number which is 0 if E is supersingular and 1 if E is ordinary. The definition of it is in [Katz, p-adic Modular Forms].**?** ⌟

Prop. (15.11.3.9) [Supersingular and Trace]. Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{F}_q$ and φ_E be the Frobenius of $E/\mathbb{F}_q$, then

- E is supersingular iff $\#E(\mathbb{F}_q) \equiv 1 \mod p$, iff $a_p = \alpha + \beta \equiv 0 \mod p$ in(15.11.3.3).
- If $q = p \geq 5$ is a prime, then E is supersingular iff $\#E(\mathbb{F}_p) = p + 1$. This is false for $p = 2$ or $p = 3$.

⌟

Proof: 1: By(15.11.3.3), let $a = 1 + q - \#E(\mathbb{F}_q)$, then $\widehat{\varphi}_E = [a] - \varphi$ is separable iff $a = 0 \in \mathbb{F}_q$ by**??**. Thus the assertion follows from(15.11.3.5).

2: Because $|\alpha + \beta| \leq 2\sqrt{p} < p$ in this case. □

Cor. (15.11.3.10). Let $p \geq 5$ and $E \in \mathcal{E}\mathrm{ll}/\mathbb{F}_p$ be supersingular, then

$$\#E(\mathbb{F}_{p^n}) = \begin{cases} p^n + 1 & n = 2k+1 \\ (p^{n/2} - (-1)^{n/2})^2 & n = 2k \end{cases}$$

⌟

Proof: This is because $\alpha = -\beta = \sqrt{p}\,\mathrm{i}$. □

Prop. (15.11.3.11)[Supersingular in Characteristic2]. Let k be a field of characteristic2, then E/k is supersingular iff $j(E) = 0$. In particular, $y^2 + y = x^3$ is the only supersingular elliptic curve over $\overline{k}$. ⌟

Proof: We use the condition $\#E(\mathbb{F}_2) = 2$. We use the reduced Weierstrass equations in(15.11.1.5). By doubling formula(15.11.1.9), this is equivalent to the non-existence of a point $(x, y) \in E(\overline{k})\backslash O$ s.t. $a_1 x + a_3 = 0$. And it can be checked this is true iff $j(E) = 0$. □

Prop. (15.11.3.12) [Supersingular Elliptic Curves over Finite Fields, Igusa]. Let $p \in \mathbf{P}$ and $E \in \mathcal{E}\mathrm{ll}/\overline{\mathbb{F}}_p$.

1. If $p = 2$, the only supersingular elliptic curve over $\overline{\mathbb{F}}_2$ is isomorphic to $y^2 + y = x^3$.
2. If $p \geq 3$ and E is given by a Weierstrass form $y^2 = f(x)$, then E is supersingular iff $\mathrm{Coef}(\frac{f(x)^{(p-1)/2}}{x^{p-1}}) = 0 \in \overline{\mathbb{F}}_p$.
3. If $p \geq 3$ and E is given by a Legendre form $y^2 = x(x-1)(x-\lambda)$, then E is supersingular iff
$$H_p(\lambda) = \sum_{i=1}^{(p-1)/2} \binom{\frac{(p-1)}{2}}{i}^2 \lambda^i = 0.$$
4. If $p \geq 3$, the polynomial H_p has distinct roots in $\overline{\mathbb{F}}_p$, and the number of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ is
$$\begin{cases} 1 & , p = 3 \\ [\frac{p}{12}] & , p \equiv 1 \mod 12 \\ [\frac{p}{12}] + 1 & , p \equiv 5, 7 \mod 12 \\ [\frac{p}{12}] + 2 & , p \equiv 11 \mod 12 \end{cases}$$
5. (Mass Formula)
$$\sum_{E/\overline{\mathbb{F}}_p \text{ supersingular}} \frac{1}{\mathrm{Aut}(E)} = \frac{p-1}{24}.$$

⌟

Remark (15.11.3.13). This has relations to the class number of normal quaternion algebras over $\mathbb{Q}$ ramified at p, Cf.[Igu58]. ⌟

Proof: 1: This follows from(15.11.3.11).

2: Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{F}_q$, denote $A_q = \mathrm{Coef}(\frac{f(x)^{(q-1)/2}}{x^{q-1}})$, then
$$\#E(\mathbb{F}_q) \equiv \sum_{x \in \mathbb{F}_q} (1 + (\frac{x^3 + a_2x^2 + a_4x + a_6}{\mathbb{F}_q})) \equiv 1 - A_q \mod p.$$
Then $A_q \equiv a_E \mod p$, and the assertion follows from(15.11.3.9).

Finally, it can be seen from the equation $f(x)^{(p^{r+1}-1)/2} = f(x)^{(p^r-1)/2}[f(x)^{(p-1)/2}]^{p^r}$ that $A_{p^{r+1}} = A_{p^r} A_p^{p^r}$. So by an induction argument, $A_q = 0$ iff $A_p = 0$.

3:
$$\mathrm{Coef}(\frac{(x(x-1)(x-\lambda))^{(p-1)/2}}{x^{p-1}}) = \mathrm{Coef}(\frac{(x-1)^{(p-1)/2}(x-\lambda)^{(p-1)/2}}{x^{(p-1)/2}}) = \sum_{i=1}^{(p-1)/2} \binom{\frac{(p-1)}{2}}{i}^2 \lambda^i = H_p(\lambda)$$

4: Consider the **Picard-Fuchs differential operator**
$$D = 4t(t-1)\frac{\partial^2}{\partial t^2} + 4(1-2t)\frac{\partial}{\partial t} - 1,$$
then direct calculation shows
$$DH_p(t) = p \sum_{i=1}^{(p-1)/2} (p-2-4i) \binom{\frac{(p-1)}{2}}{i}^2 t^i = 0.$$

Thus possible multiple roots of H can only be 1 or 0. But $H_p(0)=1$, and $H_p(1)=\binom{p-1}{\frac{p-1}{2}}=(-1)^{\frac{p-1}{2}}$, thus $H_p(t)$ has no multiple roots.

Let $\varepsilon_p(j)=1$ if the elliptic curve E with the indicated j-invariant is supersingular, and $\varepsilon_p(j)=0$ otherwise. Notice for $p\geq 5$, $j:\lambda\to j(E_\lambda)$ is 6 to 1 except $\#j^{-1}(0)=2$ and $\#j^{-1}(1728)=3$, thus by counting the number of zeros of $H_p(\lambda)$, the number of supersingular elliptic curves is

$$\frac{1}{6}(\frac{p-1}{2}-2\varepsilon_p(0)-3\varepsilon_p(1728))+\varepsilon_p(0)+\varepsilon_p(1728)=\frac{p-1}{12}+\frac{2}{3}\varepsilon_p(0)+\frac{1}{2}\varepsilon_p(1728).$$

Thus the assertion follows from determining elliptic curves of j-invariants 0 and 1728 are supersingular or not, which is done by(15.11.3.14).

5: It follows from the proof of item4 that this number is 1/2 of number of roots of $H_p(\lambda)=\frac{p-1}{24}$. □

Lemma (15.11.3.14) [Examples of Supersingular Elliptic Curves].

- For $p\geq 5$, the elliptic curve $E:y^2=x^3+1$ with j-invariant 0 is supersingular iff $p\equiv 2\mod 3$.
- For $p\geq 3$, the elliptic curve $E:y^2=x^3+x$ with j-invariant 1728 is supersingular iff $p\equiv 3\mod 4$.

⌟

Proof: These follows form calculating the x^{p-1}-term of $(x^3+1)^{(p-1)/2}$ or $(x^3+x)^{(p-1)/2}$ and(15.11.3.12) item2. □

4 Reduction of Elliptic Curves

Main references are [Liu02].

In this subsection, let S be a Dedekind scheme with generic point η and function field K.

Prop. (15.11.4.1) [Minimal Models of Elliptic Curves]. Let $E\in\mathcal{E}\mathrm{ll}/K$ and $\mathcal{E}/S$ be a minimal model for E, then

- $\mathcal{E}_{\mathrm{sm}}(S)=\mathcal{E}(S)=E(K)$.
- The automorphism $(m,\mathrm{pr}_2):E\times_K E\to E\times_K E$ extends to an automorphism $t:\mathcal{E}\times_S\mathcal{E}_{\mathrm{sm}}\to\mathcal{E}\times_S\mathcal{E}_{\mathrm{sm}}$.
- t induces an automorphism $\mathcal{E}_{\mathrm{sm}}\times_S\mathcal{E}_{\mathrm{sm}}\to\mathcal{E}_{\mathrm{sm}}\times_S\mathcal{E}_{\mathrm{sm}}$, and $\mathrm{pr}_1\circ E$ makes $\mathcal{E}_{\mathrm{sm}}$ a smooth group scheme over S extending that of E.

⌟

Proof: Cf.[Liu02]P492. □

Thm. (15.11.4.2)[$\mathcal{N}=\mathcal{E}_{\mathrm{sm}}$]. Let (R,K) be a DVR, $E\in\mathcal{E}\mathrm{ll}/K$ with minimal model $\mathcal{E}$(15.10.2.4), then $\mathcal{E}_{\mathrm{sm}}$ is a Néron model of E. ⌟

Proof: Cf. [Liu, Prop10.2.12] or [BLR, 1.5/1].

To show universal property, let X/S be smooth, and $f:X_\eta\to E$ be a morphism considered as a rational morphism $X\to\mathcal{E}_{\mathrm{sm}}$. Let $\xi\in X$ be a point of codimension 1, and $T=\operatorname{Spec}\mathcal{O}_{X,\xi}$, then by(15.9.5.7) and the proof of(15.11.4.1), $\mathcal{E}\times_S T\to T$ is an arithmetic surface with smooth locus $\mathcal{N}\times_S T$**?**, so by(15.9.2.8), $\mathcal{N}(T)=\mathcal{N}_T(T)=E(K)$, which means f can be extended to ξ. Then in fact f is a morphism by(9.1.1.20). □

over DVRs

In this subsubsection, let $(R, K, \mathfrak{m}, k)$ be a DVR, $S = \operatorname{Spec} R$.

Prop. (15.11.4.3) [Weierstrass Models are Normal]. Let $E \in \mathcal{E}\mathrm{ll}/K$, then any Weierstrass equation for E over R is normal. ⌟

Proof: Cf.[Conrad, Minimal model for Elliptic Curves]. □

Def. (15.11.4.4) [Minimal Weierstrass Equation]. Let $E \in \mathcal{E}\mathrm{ll}/K$, then a **minimal Weierstrass equation** for E is an Weierstrass equation for E in $R[X, Y]$ with determinant Δ with minimal valuation. ⌟

Prop. (15.11.4.5) [Uniqueness of Minimal Weierstrass Equations]. Let $E \in \mathcal{E}\mathrm{ll}/K$, then E has a minimal Weierstrass equation, and it is unique up to change of variables of the form

$$(X, Y) \mapsto (u^2 X + r, u^3 Y + su^2 X + t), \quad u \in R^*, r, s, t \in R.$$

Moreover, given any Weierstrass equation, then any change of coordinates that is used to produce a minimal Weierstrass equation is of the form

$$(X, Y) \mapsto (u^2 X + r, u^3 Y + su^2 X + t), \quad u, r, s, t \in R.$$

⌟

Proof: Cf.[Sil16]P186.? □

Cor. (15.11.4.6) [Weierstrass Models]. Let $E \in \mathcal{E}\mathrm{ll}/K$, a minimal Weierstrass of E defines a model $\mathcal{W}/R$ of E, and it is invariant of the Weierstrass equation chosen, called the **Weierstrass model** of E. Denote $\widetilde{E} = \mathcal{W}_k$. ⌟

Prop. (15.11.4.7) [Weierstrass Model of Elliptic Curves]. Let (R, K) be a DVR, if $E \in \mathcal{E}\mathrm{ll}/K$, then a Weierstrass equation with $a_i \in R$ defines a scheme $\mathcal{W} \in \mathbb{P}^2_R$. Then

- Both $\mathcal{W}_{\mathrm{sm}}$ and $\mathcal{W}$ has generic fiber E. If E has good reduction and W is a minimal Weierstrass equation, then $\mathcal{W} = \mathcal{W}_{\mathrm{sm}}$ is smooth.
- The natural map $\mathcal{W}(R) \to E(K)$ is a bijection. If $\mathcal{W}$ is regular, then $\mathcal{W}_{\mathrm{sm}}(R) \to \mathcal{W}(R)$ is also a bijection.
- The group structure on E/K extends to a group structure on $\mathcal{W}_{\mathrm{sm}}/R$, and the addition further extends to a group action of $\mathcal{W}_{\mathrm{sm}}/R$ on $\mathcal{W}/R$.

⌟

Proof: Cf.[**?**]P321. □

Prop. (15.11.4.8) [Weierstrass Model and Minimal Models]. Let (R, K) be a DVR, if $E \in \mathcal{E}\mathrm{ll}/K$ with minimal model $\mathcal{E}$, then any minimal Weierstrass model $\mathcal{W}$ can be obtained by blowing down the finitely many components of $\mathcal{E}_k$ which are disjoint from the closure in $\mathcal{E}$ of O_E. In particular, by(15.11.4.2), $\mathcal{W}_{\mathrm{sm}}$ is isomorphic to the relative identity component(15.7.11.16) $\mathcal{N}_0$ of the Néron model of E. ⌟

Proof: Cf.[Liu Qing, Thm. 9.4.35] □

Def. (15.11.4.9) [Reduction Types]. Let (R, K, k) be a DVR, and $E \in \mathcal{E}\mathrm{ll}/K$, then

- E has good reduction iff $(\mathcal{N}_0)_k \in \mathcal{E}\mathrm{ll}/k$.
- E has semistable reduction(15.7.12.1) iff $(\mathcal{N}_0)_{k^{\mathrm{sep}}} \cong \mathbb{G}_m$. And it is called a **split multiplicative reduction** if $(\mathcal{N}_0)_k \cong \mathbb{G}_m$, otherwise it is called a **non-split multiplicative reduction**.
- E has bad reduction iff $(\mathcal{N}_0)_{k^{\mathrm{sep}}} \cong \mathbb{G}_a$.

⌟

Proof: These follow from(15.7.12.1)(15.11.1.16) and the fact $\mathcal{N}_0 \cong \mathcal{W}_{\mathrm{sm}}$ for any minimal Weierstrass model for E. □

Def. (15.11.4.10) [Reduction of Elliptic Curves]. Let (R, K, k) be a CDVR and $E \in \mathcal{E}\mathrm{ll}/K$ with Néron model $\mathcal{N}/\mathcal{O}_K$. Then $\mathcal{N}(\mathcal{O}_K) = E(K)$, and by infinitesimal lifting property of smoothness**?**, the reduction map $r : \mathcal{N}(\mathcal{O}_K) \to \mathcal{N}_k(k)$ is surjective. Define

$$E_0(K) = r^{-1}(\mathcal{N}_0(k))(15.11.4.8), \quad E_1(K) = \ker(r).$$

$E_1(K)$ is called the **kernel of the reduction**. In particular,

$$\mathcal{N}_0(k) \cong E_0(K)/E_1(K).$$

⌟

Prop. (15.11.4.11) [Formal Group is the Kernel]. Let (R, K, k) be a CDVR and $E \in \mathcal{E}\mathrm{ll}/K$, then with notations as in(15.11.2.1),

$$\widehat{E}(\mathfrak{m}) \to E_1(K) : z \mapsto [z, -1, w(z)]$$

is an isomorphism of groups. ⌟

Proof: By(15.11.2.1), $\omega(z) \in z^3R[[z]]$, and by the definition of $w(z)$, $[z, -1, w(z)] \in E_1(K)$, and it is a group homomorphism by the definition of formal group law associated to E. It remains to prove that this map is surjective:

Clearly O is in the image, suppose $(x_0, y_0) \in E_1(K)$, then $v(x_0) < 0, v(y_0) < 0$, thus by inspecting the Weierstrass equation, $v(x_0) = -2r, v(y_0) = -3r$ for some $r > 0 \in \mathbb{Z}$. Then $z_0 = x_0/y_0 \in \mathfrak{m}$, and (x_0, y_0) is the image of z_0. □

Prop. (15.11.4.12) [Characterizing Reductions]. Let (R, K, k) be a CDVR and $E/K \in \mathcal{E}\mathrm{ll}/K$ be given by a minimal Weierstrass equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ over $\mathcal{O}_K$, then by(15.11.1.14),

- $\widetilde{E}$ is a good reduction iff $\Delta \in \mathcal{O}_K^*$.
- $\widetilde{E}$ is a semistable reduction iff $\Delta \in \mathfrak{m}$ and $c_4 \in \mathcal{O}_K^*$.
- $\widetilde{E}$ is an additive reduction iff $\Delta, c_4 \in \mathfrak{m}$.

⌟

Prop. (15.11.4.13) [Characterizing Potentially Good Reduction]. E has potentially good reduction iff $j(E) \in \mathcal{O}_K$.

In particular, an elliptic curve with complex multiplication over K has potentially good reduction.

⌟

Proof: If $E_{\overline{k}}$ has good reduction, then $j(E) = (c_4')^3/\Delta' \in R'$. Conversely, if $j(E) \in R$, use Legendre form or Deuring form(15.11.1.17)(15.11.1.18), the equation

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2} \text{ or } j = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27}$$

implies $\lambda \in \mathcal{O}_K^*, \lambda(\lambda-1) \in \mathcal{O}_K^*$(or $\alpha \in \mathcal{O}_K^*, \alpha^3 - 27 \in \mathcal{O}_K^*$), so $E_{\overline{k}}$ has good reduction. □

Prop. (15.11.4.14) [Tamagawa Numbers]. Let $E \in \mathcal{E}\mathrm{ll}/K$ with a minimal model $\mathcal{E}/\mathcal{O}_K$, then $c(E)$ equals the number of geo.integral components occuring with multiplicity 1 in $\mathcal{E}_k$. ⌟

Proof: Cf.[Liu Qing, 10.2.24]. □

Prop. (15.11.4.15) [Tamagawa Numbers]. Let $E \in \mathcal{E}\mathrm{ll}/K$. If E has split multiplicative reduction over K, then $E(K)/E_0(K)$ is a cyclic group of order $v(\Delta) = -v(j)$. And in other cases, the group is finite and has order at most 4. ⌟

Proof:

□

Cor. (15.11.4.16). If $K \in$ `p-Field` and $E \in \mathcal{E}\mathrm{ll}/K$, then $E(K)$ contains a subgroup of finite index that is isomorphic to $\mathcal{O}_K$. ⌟

Proof: Because $E(K)/E_0(K)$ and $E_0(K)/E_1(K) \cong \widetilde{E}_{ns}(k)$ are all finite by(15.11.4.15), it suffices to prove that $E_1(K) \cong \widehat{E}(\mathfrak{m})$ has a subgroup of finite index that is isomorphic to $\mathcal{O}_K$. But this follows from the fact $\widehat{E}(\mathfrak{m}^r) \cong \mathfrak{m}^r$ for r large(9.5.4.7). □

Tate Algorithm

Prop. (15.11.4.17) [Kodaira-Néron]. Let $(R, \mathfrak{m})$ be a DVR with fraction field K and alg.closed residue field k. Let E/K be an elliptic curve, and $\mathcal{C}/R$ a minimal proper regular model for E over R, then the special fiber of $\mathcal{C}$ has one of the following Forms:

- (Type I_0) An elliptic curve.
- (Type I_1) A rational curve with a node.
- (Type $\mathrm{I}_n, n \geq 2$) n smooth rational curves intersecting transversally at a single point one-by-one in the shape of a n-gon.
- (Type II) A rational curve with a cusp.
- (Type III) Two non-singular rational curves which intersects tangentially at a single point.
- (Type I_0^*) A non-singular rational curve of multiplicity 2 with 4 non-singular rational curves of multiplicity1 attached.
- (Type I_n^*) A chain of $n+1$ non-singular rational curves of multiplicity2, with two non-singular curves of multiplicity1 attached at each end.
- (Type IV^*) ?
- (Type III^*) ?
- (Type II^*) ?

⌟

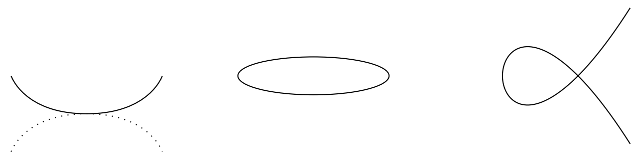


Figure (15.11.4.1): Kodaira Types

Proof: Cf.[Sil99]P354. □

Prop. (15.11.4.18)[Tate Algorithm]. There is an algorithm that determines if a Weierstrass equation for E is minimal.?

Torsion Points

Prop. (15.11.4.19) [Controlling Torsion Points]. Let $m \in \mathbb{Z} \cap k^\times$, then

- $E_1(K)[m] = O$
- The reduction map $E_0(K)[m] \to \widetilde{E}_{\mathrm{sm}}(k)[m]$ is injective.
- If E has good reduction and $K = K^{\mathrm{sep}}$, then it is also an isomorphism.

Proof: 1: By(15.11.4.11), $E_1(K)[m] \cong \widehat{E}(\mathfrak{m})[m]$, which has only one element because $[m]_{\widehat{E}}$ is an isomorphism(9.5.3.5).

2 follows from 1 and the exact sequence in(15.11.4.10).

3 follows as they have the same cardinality. □

Prop. (15.11.4.20) [Controlling Torsion Points]. Let $\operatorname{char} K = 0$ and $\operatorname{char} k = p > 0$, let E be given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in R[X, Y].$$

Let $P = (x_0, y_0) \in E(K)$ be a torsion point of exact order m, then

- If m is not a p-power, then $x_0, y_0 \in R$.
- If $m = p^n$, then $v(x) \geq -2\lfloor \frac{v(p)}{p^n - p^{n-1}} \rfloor$, $v(y) \geq -3\lfloor \frac{v(p)}{p^n - p^{n-1}} \rfloor$.

Proof: Change the Weierstrass equation to a minimal Weierstrass equation, then by(15.11.4.4), the coordinates in the new equation satisfies $v(x') \leq v(x_0), v(y') \leq v(y_0)$, thus it suffices to prove for minimal Weierstrass equations.

If $v(x_0) \geq 0$, then $v(y_0) \geq 0$. Suppose $v(x_0) < 0$, then $v(y_0) < 0$, and $v(x_0) = -2r, v(y_0) = -3r$ for some $r > 0$. thus $P \in E_1(K)$ and thus corresponds to $z \in \widehat{E}(\mathfrak{m})$(15.11.4.11). Then the theorem follows from(9.5.4.6). □

Over Dedekind Domains

Def. (15.11.4.21)[Canonical Heights]. For $F \in \mathtt{NField}$ and $E \in \mathcal{E}\mathrm{ll}/F$, by(15.7.10.4) and(15.7.4.9), $\widehat{h}_{\mathcal{L}}$ only depends on $\deg(\mathcal{L})$. And by(6.12.2.20), any degree 1 line bundle is ample, and the Néron-Tate bilinear form $\langle \cdot, \cdot \rangle_{\text{N-T}}$ given by this line bundle is called the **canonical height pairing** of E.

It is a positive-definite quadratic form on $E(\overline{K})\otimes\mathbb{R}$ by(15.13.1.4). And for $P\in E(\overline{K})$, $\langle P,P\rangle_{\text{N-T}}$ is called the **canonical height** of P.

In particular we can take the line bundle $\mathcal{O}(O)$, then $\langle O,O\rangle_{\text{N-T}}=0$, and for any $P\neq 0$ in $\mathcal{L}(O)$,

$$\langle P,P\rangle_{\text{N-T}}=\lim_{n\to\infty}h(x([2^n]P))/4^N.$$

⌟

Proof: For the final assertion, apply(15.2.1.23) to the morphism $\varphi:E\to\mathbb{P}^1$ associated to the rational function x:

$$\langle P,P\rangle_{\text{N-T}}=\lim_{n\to\infty}\widehat{h}_{\mathcal{O}(2O)}([2^n]P)/4^N=\lim_{n\to\infty}h_{\mathcal{O}_{\mathbb{P}^1}(1)}(\varphi([2^n]P))/4^N=\lim_{n\to\infty}h(x([2^n]P))/4^N.$$

□

Prop. (15.11.4.22) [Elliptic Regulators]. Let F be a number field and $E\in\mathcal{E}\mathrm{ll}/F$, then the **elliptic regulator** is the volume of a fundamental domain of $E(K)/E(K)_{\text{tor}}$ computed using the canonical height. In particular, it is the discriminant of $(\langle X_i,X_j\rangle_{E,F})_{i,j}$ where $\{X_i\}$ is a basis for $E(K)/E(K)_{\text{tor}}$. ⌟

Def. (15.11.4.23) [Minimal Discriminants]. For $F\in\texttt{GField}$ and $E\in\mathcal{E}\mathrm{ll}/F$, define the **minimal discriminant** $\Delta^{\min}_{E/F}$ to be $\Delta^{\min}_{E/F}=\prod_{v\in\Sigma_F^{\text{fin}}}\mathfrak{p}_v^{\operatorname{ord}(\Delta_v^{\min})}$, where $\Delta_v^{\min}$ is the discriminant of a minimal Weierstrass equation for E_v.

Then for any Weierstrass equation W for E, by(15.11.1.13), $\mathfrak{D}_{E/F}=\Delta^{\min}_{E/F}(\mathfrak{a}_W)^{12}$ for some ideal $\mathfrak{a}$ of F, and the ideal class of $\mathfrak{a}_\Delta$ is stable under change of Weierstrass equations, called the **Weierstrass class** of E, denoted by $\overline{\mathfrak{a}}_{E/F}$. ⌟

Def. (15.11.4.24) [Unstable Minimal Discriminants]. For $F\in\texttt{GField}$ and $E\in\mathcal{E}\mathrm{ll}/F$, suppose $(j_E)=\mathfrak{a}\mathfrak{b}^{-1}$ where $\mathfrak{a},\mathfrak{b}\in\mathrm{Ideal}^*(\mathcal{O}_F)$ are relatively prime, then the **unstable minimal discriminant** of E is defined to be

$$\Upsilon_{E/F}=\Delta^{\min}_{E/F}\cdot\mathfrak{b}^{-1}.$$

Then

- $\Upsilon_{E/F}\in\mathrm{Ideal}^*(\mathcal{O}_F)$.
- For $v\in\Sigma_F^{\text{fin}}$, $v(\Upsilon_{E/F})=0$ iff E has good or semistable reduction at v.
- $v\in\Sigma_F^{\text{fin}}$, $v(\Upsilon_{E/F})<12+12v(2)+6v(3)$.

⌟

Proof: 1, 2: These follow from the fact $j(E)=c_4^3/\Delta$(15.11.1.5) and(15.11.4.12).

3: For any minimal Weierstrass equation, maybe it follows from the change of variable formula(15.11.1.13)**?**. □

Prop. (15.11.4.25) [A Curve Related to Fermat's Last Theorem]. Let $a,b,c\in\mathbb{Z}^\times$ satisfy $(a,b,c)=1$, let E be the elliptic curve defined by the Weierstrass equation

$$E:y^2=x(x+a)(x-b),$$

then

- the minimal discriminant(15.11.4.23) $\Delta^{\min}_{E/K}$ of E is either $2^4|abc|^2$ or $2^{-8}|abc|^2$.

- E has semistable reduction for any odd prime.

⌟

Proof: By calculation

$$\mathfrak{D}_W = 2^4(abc)^2, \quad c_4 = 2^4(a^2+ab+b^2), \quad c_6 = -2^5(2a^3+3a^2b+3ab^2+2b^3),$$

$$(22a^2-8ab-8b^2)c_4+(a+2b)c_6 = 288a^2, \quad -(8a^2+8ab-22b^2)c_4-(2a+b)c_6 = 288b^2.$$

1: Any change of variable of E to the minimal Weierstrass equation satisfies $u^4|c_4, u^6|c_6$, so

$$u^4|(288a^2, 288b^2)$$

so $u=1$ or 2, and $\Delta_E^{\min} = u^{-12}\mathfrak{D}_W = 2^4|abc|^2$ or $2^{-8}|abc|^2$.

2: If $p\in\mathbf{P}\backslash\{2\}$ and $p|\Delta_E^{\min}$, then p divides a or b or c. In each case, $p\nmid c$, so E has multiplicative reduction at these p(15.11.4.12). □

Prop. (15.11.4.26) [Global Minimal Weierstrass Equation]. For $F\in\texttt{NField}$ and $E\in\mathcal{E}\mathrm{ll}/F$, E has a global minimal Weierstrass equation if its Weierstrass class is trivial.

In particular, if $\mathrm{cl}(F)=1$, e.g. $F=\mathbb{Q}$, then any $E\in\mathcal{E}\mathrm{ll}/F$ has a global minimal Weierstrass equation. ⌟

Proof: Choose any Weierstrass equation for E over K, let

$$x = u_v^2x+r_v, \quad y = u_v^3y+s_vu_v^2x+t_v, \quad u_v,r_v,s_v,t_v\in\mathcal{O}_{K,v}$$

be the local change of variable to get the minimal Weierstrass equation at place v, then by hypothesis, $(u_v)_v$ is principal, which means there is some $u\in K$ s.t. $v(u)=v(u_v)$ for any v. Then choose by Chinese remainder theorem $r,s,t\in\mathcal{O}_K$ that is closed to r_v,s_v,t_v for each relevant v, then the change of variables

$$x = u^2x+r, \quad y = u^3y+su^2x+t$$

changes the coordinates to a minimal Weierstrass equation. □

Cor. (15.11.4.27). Let $F\in\texttt{GField}$ with $6\nmid\mathrm{cl}(F)$ and $E\in\mathcal{E}\mathrm{ll}/F$ with everywhere good reduction, then E has a minimal model. ⌟

Proof: Because in this case the Weierstrass class $\mathfrak{a}_\Delta$ is a 12-torsion in $\mathrm{Cl}(F)$, which implies it is trivial. □

Cor. (15.11.4.28). If $F\in\texttt{NField}$ and S is a finite set of places of K s.t. $\mathrm{Cl}(\mathcal{O}_{F,S})=1$, then any elliptic curve over F has a minimal Weierstrass equation of the form $W: y^2=x^3+Ax+B$ with $A,B\in\mathcal{O}_{K,S}$ satisfying $\mathfrak{D}_W\mathcal{O}_{F,S}=\Delta_{E/F}^{\min}\mathcal{O}_{F,S}$. ⌟

Proof: The proof is easier than that(15.11.4.26). □

Prop. (15.11.4.29). If $F\in\texttt{NField}$ with $\mathrm{Cl}(F)\neq 1$, then there exists $E\in\mathcal{E}\mathrm{ll}/F$ with no global minimal Weierstrass equations. ⌟

Proof: Cf.[Weierstrass equations and the minimal discriminant of an elliptic curve", Mathematika 31 (1984), no. 2, 245–251]. □

Prop. (15.11.4.30) [Density of Global Minimal Models]. ⌟

Proof: Cf.[The density of elliptic curves having a global minimal Weierstrass equation", J. Number Theory 109 (2004), no. 1, 41–58.]. □

5 Tate Curve

Def. (15.11.5.1). Define formal power series

$$s_k(q)=\sum_{n\geq 1}\sigma_k(n)q^n=\sum_{n\geq 1}\frac{n^kq^n}{1-q^n}\in\mathbb{Z}[[q]],$$

$$a_4(q)=-5s_3(q),\quad a_6(q)=-\frac{5s_3(q)+7s_5(q)}{12}\in\mathbb{Z}[[q]],$$

$$X(u,q)=\sum_{n\in\mathbb{Z}}\frac{q^nu}{(1-q^nu)^2}-2s_1(q),\quad Y(u,q)=\sum_{n\in\mathbb{Z}}\frac{(q^nu)^2}{(1-q^nu)^3}+s_1(q)\in\mathbb{Z}[u][[q]].$$

⌟

Prop. (15.11.5.2).

$$s_1(q)=\sum_{n\geq 1}\frac{q^n}{(1-q^n)^2}\in\mathbb{Z}[[q]],$$

$$X(u,q)=\frac{u}{(1-u)^2}+\sum_{n\geq 1}[\frac{q^nu}{(1-q^nu)^2}+\frac{q^nu^{-1}}{(1-q^nu^{-1})^2}-\frac{2q^n}{(1-q^n)^2}]\in\mathbb{Z}[u][[q]],$$

$$Y(u,q)=\frac{u^2}{(1-u)^3}+\sum_{n\geq 1}[\frac{(q^nu)^2}{(1-q^nu)^3}+\frac{q^nu^{-1}}{(1-q^nu^{-1})^3}+\frac{q^n}{(1-q^n)^2}]\in\mathbb{Z}[u][[q]],$$

Thus

$$X(qu,q)=X(u,q)=X(u^{-1},q),\quad Y(qu,q)=Y(u,q)\in\mathbb{Z}[u,u^{-1}][[q]].$$

⌟

Proof: The first one follows from(9.5.2.2). □

Prop. (15.11.5.3) [Relation to Weierstrass $\mathfrak{P}$-Functions]. Let $\wp(z;\tau)$ be the Weierstrass $\wp$-function associated to the lattice $\Lambda_z=\mathrm{span}\{1,\tau\}$(11.5.4.5), then $X(e^{2\pi iz},q(\tau)),Y(e^{2\pi iz},q(\tau))$ converges and uniformly and absolutely on $\mathbb{C}\backslash\Lambda_z$ in $\mathbb{C}$ to holomorphic functions, and

$$\frac{1}{(2\pi\,\mathrm{i})^2}\wp(z;\tau)=X(e^{2\pi\,\mathrm{i}\,z},q(\tau))+\frac{1}{12},\quad \frac{1}{(2\pi i)^3}\wp(z;\tau)'=X(e^{2\pi iz},q(\tau))+2Y(e^{2\pi iz},q(\tau)).$$

⌟

Proof: The convergence of X,Y is clear. By(15.11.5.1), $X(e^{2\pi iz},q(\tau))$ is $\{1,\tau\}$-doubly periodic, and clearly it has a double pole at the origin. Also the Laurent part of $X(e^{2\pi iz},q(\tau))$ at $z=0$ is the Laurent part of $\frac{e^{2\pi iz}}{(1-e^{2\pi iz})^2}$, which is $\frac{1}{(2\pi i)^2z^2}-\frac{1}{12}$. Then by comparison with that of $\mathfrak{P}(z;\tau)$(11.5.4.6) and use Liouville's theorem.

The second identity follows from applying $\frac{\partial}{\partial z}$. □

Prop. (15.11.5.4) [Formal Identities]. There are identities

1. $$-a_6(q)+a_4^2(q)+72a_4a_6-64a_4^3-432a_6^3=\Delta(q)\in\mathbb{Z}[[q]].$$

2. $$Y(u^{-1},q)=-Y(u,q)-X(u,q)\in\mathbb{Z}[u,u^{-1}][[q]].$$

3.
$$Y(u,q)^2 + X(u,q)Y(u,q) = X(u,q)^3 + a_4(q)X(u,q) + a_6(q) \in \mathbb{Z}[u][[q]].$$

4.
$$(X(u_2,q) - X(u_1,q))^2 X(u_1u_2,q) = (Y(u_2,q) - Y(u_1,q))^2 + (Y(u_2,q) - Y(u_1,q))(X(u_2,q) - X(u_1,q)) - (X(u_2,q) - X(u_1,q))^2 (X(u_2,q) + X(u_1,q))$$

$$(X(u_2,q) - X(u_1,q))Y(u_1u_2,q) = -[(Y(u_2,q) - Y(u_1,q)) + (X(u_2,q) - X(u_1,q))]X(u_1u_2,q) - (Y(u_1,q)X(u_2,q) - Y(u_2,q)X(u_1,q))$$

⌟

Proof: Verify these in the complex analytic case.?
3: By(11.5.4.7) and(15.11.5.3)(20.2.4.5),

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z)^2 - g_3\wp(z)$$

implies the desired equation.

□

Cor. (15.11.5.5) [Tate Curve]. Notation as in(15.11.5.1), $\mathrm{Tate}(q) : y^2 + xy = x^3 + a_4(q)x + a_6(q)$ is an elliptic scheme over $\mathbb{Z}[[q]]$, called the **Tate curve**. The discriminant and j-invariant of $\mathrm{Tate}(q)$ is given by

$$\Delta(\mathrm{Tate}(q)) = \Delta(q) : q\prod_{n\geq 1}(1-q^n)^{24}(20.2.4.20), \quad j(\mathrm{Tate}(q)) = j(q)(20.2.4.22).$$

And it has the normalized differential form $\omega = \mathrm{d}x/(2y+x)$. Also denote $\omega_{\mathrm{can}} = 2\pi\,\mathrm{i}\,\omega$. ⌟

Prop. (15.11.5.6) [N-Torsion Points]. It can be shown formally from(15.11.5.10) that

$$\mathrm{Tate}(q^N)[N] = \{(X(\zeta_N^i q^j, q^N), Y(\zeta_N^i q^j, q^N))\}?,$$

which are all defined over $\mathbb{Z}[[q]][\frac{1}{N}, \zeta_N]$. In particular, all the level N structures of $\mathrm{Tate}(q^N)$ are defined over $\mathbb{Z}[[q]][\frac{1}{N}, \zeta_N]$. ⌟

Proof:

□

Prop. (15.11.5.7) [Tate Curve over $\mathbb{C}$]. Notation as in(15.11.5.1), then for $q \in \mathbb{C}, 0 < |q| < 1$,

- $E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$ is an elliptic curve over $\mathbb{C}$, and

$$\varphi : \mathbb{C}^*/q^{\mathbb{Z}} \to E_q^{\mathrm{an}} : u \mapsto [X(u,q), Y(u,q), 1]$$

is a complex analytic isomorphism.

- The discriminant of E_q is given by

$$\Delta(E_q) = \Delta(q) : q\prod_{n\geq 1}(1-q^n)^{24}(20.2.4.20), \quad j(E_q) = j(q)(20.2.4.22)$$

- For any elliptic curve $E/\mathbb{C}$, there exists a $q \in \mathbb{C}^*, |q| < 1$ s.t. E is isomorphic to E_q.

⌟

Proof: Cf.[Sil99]P410.**?** □

Prop. (15.11.5.8) [Tate Curve over $\mathbb{R}$]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{R}$, there exists a unique $q \in \mathbb{R}, 0 < |q| < 1$ s.t.

- E is isomorphic to $E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$ over $\mathbb{R}$.
- the isomorphism composed with

$$\varphi : \mathbb{C}^*/q^{\mathbb{Z}} \cong E_q^{\mathrm{an}} : u \mapsto (X(u, q), Y(u, q))$$

as in(15.11.5.10) induces an isomorphism of complex Lie groups $\psi : \mathbb{C}^*/q^{\mathbb{Z}} \to E_{\mathbb{C}}^{an}$ that commutes with complex conjugation. In particular, ψ induces an isomorphism of real Lie groups

$$\psi : \mathbb{R}^*/q^{\mathbb{Z}} \cong E_{\mathbb{R}}^{\mathrm{an}}.$$

⌟

Proof: 1: By(15.7.8.16) and(15.7.8.17), there are exactly on $\tau \in \mathcal{C}' = \{\mathrm{i}\,t|t \geq 1\} \cup \{1/2 + \mathrm{i}\,t|t > 1/2\}$ s.t. $j(\tau) = j(E) \in \mathbb{R}$, and

$$\mathcal{J} = \{\mathrm{i}\,t|t > 0\} \cup \{1/2 + \mathrm{i}\,t|t > 0\}.$$

corresponds to $q \in \mathbb{R}, 0 < |q| < 1$ via $\tau \mapsto q = e^{2\pi\,\mathrm{i}\,\tau}$. Also there are identifications

$$\begin{bmatrix} & -1 \\ 1 & \end{bmatrix} \{\mathrm{i}\,t|t > 1\} = \{\mathrm{i}\,t|t < 1\}, \quad \begin{bmatrix} 1 & -1 \\ 2 & -1 \end{bmatrix} \{1/2 + \mathrm{i}\,t|t > 1/2\} = \{1/2 + \mathrm{i}\,t|t < 1/2\}, \quad \begin{bmatrix} & -1 \\ 1 & -1 \end{bmatrix} (\mathrm{i}) = \frac{1}{2} + \frac{i}{2},$$

thus it suffices to show that for any two $q, q' \in \mathcal{J}$ with $q \neq q'$, $E_q \ncong E_{q'}$. It suffices to show for the twists, where we can use(15.11.6.3) to show that their c_4, c_6 changed sign, so they are not isomorphic over $\mathbb{R}$.

2: This follows from(15.11.5.10). □

Cor. (15.11.5.9) [Connected Components]. Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{R}$, then

$$E(\mathbb{R}) \cong \begin{cases} \mathbb{R}/\mathbb{Z} & \Delta(E) < 0 \\ \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/(2) & \Delta(E) > 0 \end{cases}$$

as real Lie groups. ⌟

Proof: Notice $\mathrm{sgn}(\Delta) = \mathrm{sgn}(q)$ by(15.11.5.10). The $q > 0$ case is clear. For $q < 0$, notice there is an isogeny $E_{q^2} \to E_q$ with kernel q, so $E_{\mathbb{R}}^{\mathrm{an}} \cong [\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/(2)]/(1/2, -1) \cong \mathbb{R}/\mathbb{Z}$. □

Prop. (15.11.5.10) [over Complete Valued Fields]. Notation as in(15.11.5.1), let K be a complete non-Archimedean valued field, then for $q \in K, 0 < |q| < 1$,

- $E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q) \in \mathcal{E}\mathrm{ll}/K$. The discriminant of E_q is given by

$$\Delta(E_q) = \Delta(q) : q \prod_{n \geq 1} (1 - q^n)^{24} (20.2.4.20), \quad j(E_q) = j(q) (20.2.4.22)$$

- $$\varphi : \overline{K}^\times \to E_q(\overline{K}) : u \mapsto [X(u,q), Y(u,q), 1]$$

  is a continuous surjective homomorphism with kernel $q^{\mathbb{Z}}$, and it is Gal_K-invariant, thus for any $K \subset L \subset \overline{K}$ inducing a continuous surjective homomorphism

  $$\varphi : L^\times \to E_q(L)$$

  with kernel $q^{\mathbb{Z}}$.

⌟

Proof: 1: This follows from(15.11.5.5) by base change.

2: Clearly $X(u,q), Y(u,q)$ converges for any $u \in K^\times/q^{\mathbb{Z}}$, and by(15.11.5.1) it suffices to consider the case $|q| < |u| < |q|^{-1}$. In this case, the formal power series for $X(u,q), Y(u,q)$ are convergent in the complete field $K(u)$, and it follows from(15.11.5.4) that $\varphi(\overline{K}^*) \in E$. It is clearly continuous for $u \neq 1$, and if u converges to 1, $X(u,q)/Y(u,q) \to 0$ by the expansion in(15.11.5.4), so $\varphi(1) = O$.

To show φ is a homomorphism, it suffices to verify for $1 < |u_1| < |q|^{-1}, |q| < |u_2| < 1$ that $\varphi(u_1) + \varphi(u_2) = \varphi(u_1 u_2)$. Notice by the argument above, $\varphi(u) = O$ iff $u = 1$. If $u_1 = 1$ or $u_2 = 1$, then $\varphi(u_1) + \varphi(u_2) = \varphi(u_1 u_2)$ is clear, and if $u_1 u_2 = 1$, then $\varphi(u_1) + \varphi(u_2) = O$ by the identities in(15.11.5.4) and(15.11.1.9). When $u_1 \neq 1, u_2 \neq 1,_1 u_2 \neq 1$, $\varphi(u_1) \neq \varphi(u_2)$, $\varphi(u_1) + \varphi(u_2)$ are determined by polynomial equations with coordinates of $\varphi(u_1), \varphi(u_2)$, and we can show this equation holds for $\varphi(u_1 u_2)$ because it holds in the complex case(15.11.5.10). For the case $\varphi(u_1) = \varphi(u_2)$, notice that $\mathrm{Im}(\varphi)$ is infinite, as for $|t| < 1$, $|X(1+t)| = |t|^{-2}$ by the formula in(15.11.5.4). Now this case follows from(3.1.2.14).

Next, we show $\varphi : L^\times \to E_q(L)$ is surjective. As K is arbitrary, we may assume $L = K$. For this, Cf.[Tate, a review of non-Archimedean Elliptic Functions]**?**. □

Cor. (15.11.5.11). $\mathrm{Tate}(q)(\mathbb{Q}((q))) \cong \mathbb{Q}((q))^\times/q^{\mathbb{Z}}$. ⌟

Lemma (15.11.5.12). Let $\alpha \in K$ with $|\alpha| > 1$, then there exists a unique $q \in K$ s.t. $|q| < 1$ s.t. $j(q) = \alpha$. Moreover, $q \in \mathbb{Z}[[\frac{1}{\alpha}]]$. ⌟

Proof: Let $f(q) = j(q)^{-1} \in q + q^2\mathbb{Z}[[q]]$, thus by(9.5.1.3) there exists a $g \in q\mathbb{Z}[[q]]$ s.t. $f(g(q)) = q = g(f(q))$. So if $f(q) = \frac{1}{\alpha}$, then $q = f(\frac{1}{\alpha})$. And this q do satisfies $j(q) = \alpha$. □

Thm. (15.11.5.13) [p-Adic Uniformization, Tate]. Let K be a complete valued field, $E \in \mathcal{E}\mathrm{ll}/K$ with $|j(E)| > 1$, then

- There exists a unique $q \in K$ s.t. $E_{\overline{K}} \cong (E_q)_{\overline{K}}$.
- For this q, the following are equivalent:
  - $E \cong E_q$.
  - $\gamma(E) = 1$(15.11.6.3).
  - E has split multiplicative reduction.

⌟

Proof: 1 follows from(15.11.5.12) and(15.11.1.14).

2: Firstly $\gamma(E_q) = 1$, because

$$c_4(E_q) = 1 - 48a_4(q) = 1 + 240s_3(q), \quad -c_6(E_q) = 1 - 72a_4(q) - 864a_6(q) = 1 - 504s_5(q)$$

are all of the form $1+4\alpha, |\alpha|<1$, thus they are both squares in $K^\times$, as $1+4\alpha = [(1+4\alpha)^{1/2}]^2$**??**

Next, $|a_4(q)|, |a_6(q)| \le 1$, so $\widetilde{E}_q : y^2+xy = x^3$ has split multiplicative reduction. Then $1 \iff 2$ by(15.11.6.3), and to show $1 \iff 3$, it suffices to show that if E has split multiplicative reduction, then $\gamma(E) = 1$: Let the valuation ring of K be R with maximal ideal $\mathfrak{m}$ and residue field k. Let $y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$ be a minimal polynomial. We may assume the singular point is $(0,0) \in \widetilde{E}(k)$, then $a_3 \equiv a_4 \equiv a_6 \equiv 0 \mod \mathfrak{m}$, thus $b_4 = a_1a_3 + 2a_4 \equiv 0 \mod \mathfrak{m}$, and $c_4 = b_2^2 - 2b_4 \equiv b_2^2 \mod m$. Thus $b_2 \in R^*$, and

$$\gamma(E) = -\frac{c_4}{c_6} = \frac{1}{b_2}\frac{1-24b_4/b_2^{-2}}{1-36b_4/b_2^2+216b_6/b_2^3} \mod (K^\times)^2.$$

So by**??**gain, $\gamma(E) \cong b_2 \mod (K^\times)^2$.

Because E has multiplicative split reduction, $y^2 + \overline{a}_1xy - \overline{a}_2x^2 = (y-\overline{\alpha}x)(y-\overline{\beta}x) \in k$, $\overline{\alpha} \neq \overline{\beta}$. Thus by Henselian lifting, $y^2+a_1xy-a_2x^2 = (y-\alpha x)(y-\beta x) \in K$ for some α,β, and $b_2 = a_1^2+4a_2 = (\alpha-\beta)^2 \in (K^\times)^2$. □

Cor. (15.11.5.14). If $\gamma(E) \neq 1$, let $L = K(\sqrt{\gamma(E)})$, then $E_L \cong (E_q)_L$, and

$$E(K) \cong \{u \in L^*/q^{\mathbb{Z}} | N_{L/K}(u) \in {}^{\mathbb{Z}}\}.$$

⌟

Proof: Cf.[Sil99]P444. □

6 Twists of Elliptic Curves

Cf.[Sil16]Chap10.6.

Prop. (15.11.6.1)[Twists of Elliptic Curves]. Because the category of smooth curves is an algebraic stack, for $k \in$ `Field` and $C \in \mathfrak{Cur}^{\mathrm{sm}}/k$, the set $\mathrm{Twist}(C/k)$ of twisted smooth curves of C is in bijection with $H^1(k, \mathrm{Isom}(C_{k^s}))$ by(6.1.5.2).

Also the category of elliptic curves(with the origin fixed) is an algebraic stack, thus the set $\mathrm{Twist}((E,O)/k)$ of twisted elliptic curves of an elliptic curve over k is in bijection with $H^1(k, \underline{\mathrm{Aut}}(E))$. ⌟

Remark (15.11.6.2). [Sil16]P318,342 has a direct proof, and can find the twist corresponding to a cocycle explicitly.**?** ⌟

Prop. (15.11.6.3) [$\mathrm{Twist}((E,O)/k)$]**.** Let $k \in$ `Field`, $\mathrm{char}\, k \neq 2,3$ and $E \in \mathcal{E}\mathrm{ll}/k$. Denote $n = \#\mathrm{Aut}(E_{\overline{k}})$, then

- $\mathrm{Twist}((E,O)/k)$ is canonically isomorphic to $k^\times/(k^\times)^n$.
- For E/k given by Weierstrass equation $y^2 = x^3 + Ax + B$, the twisted elliptic curve of E corresponding to $D(\mathrm{mod}\ (K^\times)^n)$ has the Weierstrass equation

$$E^{(D)} : \begin{cases} y^2 = x^3 + D^2Ax + D^3B, & j(E) \neq 0, 1728 \\ y^2 = x^3 + DAx, & j(E) = 1728 \\ y^2 = x^3 + DB, & j(E) = 0 \end{cases}.$$

- In case $j(E) \neq 0, 1728$, $n = 2$, define $\gamma(E) = -c_4/c_6 \in \mathbb{K}^\times/(K^\times)^2$(which equals A/B in the short form), then for $E, E' \in \mathcal{E}\mathrm{ll}/k$ with $j(E), j(E') \neq 0, 1728$,

$$E \cong E' \iff j(E) = j(E') \ \&\ \gamma(E) = \gamma(E').$$

⌟

Proof: This is because the Kummer sequence and(15.11.1.19) implies $H^1(k, \underline{\mathrm{Aut}}(E)) \cong H^1(k, \mu_n) = k^\times/(k^\times)^n$. For the corresponding elliptic curve, Cf.[Sil16]P343.**?** □

Def. (15.11.6.4) [Weil-Châtelet Groups]. For $k \in \mathtt{Field}, E \in \mathcal{E}\mathrm{ll}/k$, define the **Weil-Châtelet Group** $\mathrm{WC}(E/k)$ to be the isomorphism classes of X-torsors on $\mathcal{S}\mathrm{ch}_{\text{ét}}/k$. Then there is a bijection of pointed sets $\mathrm{WC}(E/k) \cong H^1(k, E)$, by(6.3.2.18). So $\mathrm{WC}(E/k) \subset \mathrm{Twist}(E/k)$(15.11.6.1). ⌟

Prop. (15.11.6.5). If $k \in \mathtt{Field}, E \in \mathcal{E}\mathrm{ll}/k$ and $C \in \mathrm{WC}(E/k)$, then $\mathrm{Jac}(C) \cong E$. ⌟

Proof: Because C is a smooth curve, let $p \in C$ be a geometric point, and take the line bundle $\mu^*\mathcal{L}(p) - \mathrm{pr}_2^*\mathcal{L}(p) - \mathrm{pr}_1^*\mathcal{L}(O)$, where $\mu : E \times C \to C$ is the action. Then after a base change to $k(p)$, this map corresponds to the canonical isomorphism $E \cong E^\vee$(15.11.1.20), thus it is also an isomorphism because $\mathcal{S}\mathrm{ch}_X$ is a prestack over $\mathcal{S}\mathrm{ch}_{\mathrm{fpqc}}$. □

Prop. (15.11.6.6). Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{R}$, then

$$\mathrm{WC}(E/\mathbb{R}) \cong \begin{cases} 0 & \Delta(E) > 0 \\ \mathbb{Z}/(2) & \Delta(E) < 0 \end{cases}.$$

⌟

Proof: By(15.11.6.4) and(15.11.5.8), the Galois cohomology of the exact sequence $1 \to q^{\mathbb{Z}} \to \mathbb{C}^\times \to E(\mathbb{C}) \to 1$ says

$$0 \to \mathrm{WC}(E/\mathbb{R}) \to H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), q^{\mathbb{Z}}) \to H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times),$$

and $\mathbb{H}^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), q^{\mathbb{Z}}) \cong q^{\mathbb{Z}}/q^{2\mathbb{Z}}, H^2(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times) \cong \mathbb{R}^\times/(\mathbb{R}^\times)^2$ by(8.7.3.5)(8.7.1.20). So we are done by observing $\mathrm{sgn}(\Delta) = \mathrm{sgn}(q)$ by(15.11.5.10). □

Goldfeld Conjecture

Cf.[Gol79].

Conj. (15.11.6.7) [Goldfeld]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$, consider its twists $E^{(D)}$ as in(15.11.6.3), then

$$\lim_{X\to\infty} \frac{\#\{d \in \mathbb{Z}^\times : d \text{ is square-free }, r_{\mathrm{an}}(E^{(d)}) = r, |d| < X\}}{\#\{d \in \mathbb{Z}^\times : d \text{ is square-free }, |d| < X\}} = \begin{cases} \frac{1}{2} & r = 0 \\ \frac{1}{2} & r = 1 \\ 0 & r \geq 2 \end{cases}.$$

⌟

Proof: □

Conj.Cor. (15.11.6.8) [Weak Goldfeld Conjecture]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$,

$$\liminf_{X\to\infty} \frac{\#\{d \in \mathbb{Z}^\times : d \text{ is square-free }, r_{\mathrm{an}}(E^{(d)}) = r, |d| < X\}}{\#\{d \in \mathbb{Z}^\times : d \text{ is square-free }, |d| < X\}} > 0.$$

⌟

Thm& Conj.Cor. (15.11.6.9) [Kriz-Li]. If $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ has a rational 3-isogeny, then the weak Goldfeld conjecture is true.

And for the sextic family $\{y^2 = x^3 + d\}$, the proportion is$\geq 1/6$ for $r = 0$ and $\geq 1/6$ for $r = 1$. ⌟

Proof: [Daniel Kriz and Chao Li. Goldfeld's conjecture and congruences between Heegner points]. □

Thm& Conj.Cor. (15.11.6.10) [Tian–Yuan–Zhang, Smith]. For the sextic family $\{y^2 = x^3 + d\}$, the proportion is$\geq 1/6$ for $r = 0$ and $\geq 1/6$ for $r = 1$. ⌟

Proof: [Ye Tian, Xinyi Yuan, and Shou-Wu Zhang. Genus periods, genus points and congruent number problem], [Smith. The congruent numbers have positive natural density]. □

7 Integral Points

Thm. (15.11.7.1) [Siegel]. Let E/K be an elliptic curve with $\#E(K) = \infty$. Let v be an absolute valuation of $\overline{K}$, $Q \in E(\overline{K})$ and $f \in R(E)^\times$ which corresponds to a morphism $\varphi : E \to \mathbb{P}^1 : P \mapsto [1, f(P)]$, then

$$\varinjlim_{P \in E(K), h(\varphi(P)) \to \infty} \frac{\log d_v(P; Q)}{h(\varphi(P))} = 0.\text{(15.2.1.31)}$$

⌟

Proof: Cf.[Sil16]P276. □

Cor. (15.11.7.2) [Finiteness of Integral Points]. If C/K is a complete smooth curve of genus 1 and $f \in R(C)^\times$, $S \subset \Sigma_K$ a finite set, then $\{P \in C(K) | f(P) \in \mathcal{O}_{K,S}\}$ is a finite set. ⌟

Proof: By a finite base change of fields, we may assume $\varphi^{-1}(\infty)$ contains a rational point O, and this point makes C into an elliptic curve. Let $\varphi : E \to \mathbb{P}^1 : P \mapsto [1, f(P)]$. It follows from the definition that there is some $v \in S$ s.t.

$$h(\varphi(P)) \leq \#S \cdot \log |f(P)|_v$$

for any $P \in C(K)$ s.t. $f(P) \in \mathcal{O}_{K,S}$. Then if $\#\{P \in C(K) | f(P) \in \mathcal{O}_{K,S}\} = \{P_1, \ldots, P_n, \ldots\}$ is infinite, it follows from Northcott's theorem(15.2.1.7) that $h(\varphi(P_i)) \to \infty$, and $|f(P_i)|_v \to \infty$ for a specific $v \in S$. Suppose $e_O(\varphi) = e$, then **?** □

8 Elliptic Surfaces

15.12 Arithmetic of K3 Surfaces

References are [Arithmetic and Geometry of K3 surfaces and Calabi-Yau Threefolds].

15.13 Abelian Varieties over Global Fields

References are [Mordell Seminar notes, Bhatt], http://virtualmath1.stanford.edu/~conrad/mordellsem/, [Fal86] and [Mil08].

1 Néron-Tate Heights

Prop. (15.13.1.1) [Néron-Tate Heights]. Let $F \in \texttt{GField}, X \in \mathcal{A}b\mathcal{V}ar/F, \mathcal{L} \in \mathrm{Pic}(X)$, then there are uniquely defined bilinear form $b_{\mathcal{L}}$, additive homomorphism $l_{\mathcal{L}}$ on $X(\overline{F})$ s.t.

$$\widehat{h}_{\mathcal{L}}(x) = \frac{1}{2}b_{\mathcal{L}}(x,x) + l_{\mathcal{L}}(x) \sim h_{\mathcal{L}}(x),$$

called the **Néron-Tate height** of $\mathcal{L}$. ⌟

Proof: We want to use(3.1.3.13) for the Weil height(15.2.1.23) $h_{\mathcal{L}}$ on $X(\overline{K})$: apply the theorem of the cube(15.7.1.22) to the projections $\pi_i : X \times X \times X \to X$ and pullback to X via the diagonal map, then taking the Weil heights, we will get the desired relation

$$h_{\mathcal{L}}(\sum_{i=1}^{3} x_i) - \sum_{1\leq i<j\leq 3} h_{\mathcal{L}}(x_i + x_j) + \sum_{i=1}^{3} h_{\mathcal{L}}(x_i) \sim 0.$$

□

Remark (15.13.1.2). Another way to get this is through Tate's limiting argument(15.17.3.2). ⌟

Cor. (15.13.1.3). The Néron-Tate height is a refinement of Weil heights(15.2.1.23) made for Abelian varieties:

- The map $\widehat{h} : \mathrm{Pic}(X) \mapsto \mathbb{R}^{X(\overline{K})} : \mathcal{L} \mapsto \widehat{h}_{\mathcal{L}}$ is an additive homomorphism.
- (Symmetry)If $\varphi : A \to B$ is a homomorphisms of Abelian varieties, then $\widehat{h}_{\varphi^*(\mathcal{L})} = \widehat{h}_{\mathcal{L}} \circ \varphi$.
- (Positivity)Let $\mathcal{L} \in \mathrm{Pic}(X)$ be even. If $\mathcal{L}$ is base-free or ample, then $\widehat{h}_{\mathcal{L}} \geq 0$.
- (Boundedness)Let $\mathcal{L} \in \mathrm{Pic}(X)$ be even and ample(such an $\mathcal{L}$ exists by(15.7.1.28)), then $\widehat{h}_{\mathcal{L}}$ induces a symmetric bilinear form on $X(K)$ satisfying $\{x \in X(\overline{K}) | \deg(x) \leq d, (x,x) < C\}$ is finite for all $C > 0$

⌟

Proof: $1, 2$ follow from the corresponding property of Weil heights(15.2.1.23) and the uniqueness in(3.1.3.13).

3: Notice that the fact $\mathcal{L}$ is even implies $\widehat{h}_{\mathcal{L}} = \frac{1}{2}b(x,x)$. The ample case reduces to the base-free case, because there is a multiple $m\mathcal{L}$ that is very ample, and then $\widehat{h}_{m\mathcal{L}} = m\widehat{h}_{\mathcal{L}}$. For the base-free case, c is the pullback of $\mathcal{O}(1)$ for some morphism $X \to \mathbb{P}^n$, thus $h_{\mathcal{L}}$ is non-negative by(15.2.1.3), and $h_{\mathcal{L}} \sim \widehat{h}_{\mathcal{L}}$, thus $\widehat{h}_{\mathcal{L}}$ must also be non-negative.

4 follows from Northcott's theorem(15.2.1.24). □

Cor. (15.13.1.4)[Positive Definiteness]. For any ample line bundle $\mathcal{L} \in \mathrm{Pic}(A)$, $b_{\mathcal{L}}$ induces a positive definite symmetric bilinear form on $A(\overline{F}) \otimes_{\mathbb{Z}} \mathbb{R}$ ⌟

Proof: We want to use(3.1.3.14). Notice $b_{\mathcal{L}}$ is just $2\widehat{h}_{\mathcal{L}\otimes[-1]^*\mathcal{L}}$, thus satisfies the conditions by(15.13.1.3). □

Prop. (15.13.1.5) [Zero of Heights and Torsion]. If $F \in \texttt{GField}$, $A \in \mathcal{A}b\mathcal{V}ar/F$ and $\mathcal{L}$ is ample, then $\widehat{h}_{\varphi,\mathcal{L}}(x) = 0$ iff x is preperiodic, i.e. the sequence $\{x, \varphi(x), \varphi^2(x), \ldots\}$ is finite.

In particular, $\widehat{h}_{\mathcal{L}}(x) = 0$ iff x is torsion. ⌟

Proof: Assume $l \neq 0$. If x is preperiodic, then clearly $\widehat{h}_{\varphi,\mathcal{L}}(x) = \lim_{r\to\infty} \lambda^{-r} h_{\mathcal{L}}(\varphi^r(x)) = 0$. Conversely, if $\widehat{h}_{\varphi,\mathcal{L}}(x) = 0$, then $\widehat{h}_{\varphi,\mathcal{L}}(\varphi^r(x)) = 0$ for any r, then $|h_{\mathcal{L}}(\varphi^r(x))| \leq |\widehat{h}_{\varphi,\mathcal{L}}(\varphi(x))| + C(\varphi,\mathcal{L}) = C(\varphi,\mathcal{L})$ is bounded and also $\varphi^r(x) \in X(k(x))$, thus has bounded degree. So by Northcott's theorem(15.2.1.24), there are only f.m. such points. □

Cor. (15.13.1.6) [Kronecker]. For $\zeta \in \overline{\mathbb{Q}}$, $h^+(\zeta) = 0$(15.2.1.5). ⌟

Proof: This is a special case of(15.13.1.5), where $\varphi : \mathbb{P}^1 \to \mathbb{P}^1 : [x,y] \mapsto [x^n, y^n]$ and $\mathcal{L} = \mathcal{O}(1)$, thus the preperiodic points are just $0, \infty$ and all the roots of unity. □

Prop. (15.13.1.7) [Néron-Tate Pairings]. Let $F \in \texttt{NField}$ and $A \in \mathcal{A}b\mathcal{V}ar/F$, then $A \times \widehat{A}$ is also an Abelian variety with the even Poincaré class p(15.7.4.7), thus generating a function:

$$\widehat{h}_{A\times A^\vee,p} : A(\overline{F}) \times \widehat{A}(\overline{F}) \to \mathbb{R}.$$

Then in fact this pairing is bilinear, called the **Néron-Tate pairing** $\langle\cdot,\cdot\rangle_{A,\text{N-T}}$.

The Weil-Tate pairing satisfies the functoriality property: If $f : A \to B$ is a homomorphism of Abelian varieties, then $\langle f(a), b\rangle_{B,\text{N-T}} = \langle a, \widehat{f}(b)\rangle_{A,\text{N-T}}$. ⌟

Proof: Use functoriality of heights for $A \to A \times \widehat{A}$, then $\widehat{h}_{A\times\widehat{A},p}((a,0)) = \widehat{h}_{A,0}(a) = 0$. Similarly, $\langle 0, a\rangle_{A,K} = 0$. Thus $\widehat{h}_{A\times\widehat{A},p}$ is bilinear by(3.1.3.8).

The last assertion follows from(9.7.2.36). □

Prop. (15.13.1.8). Let $\mathcal{L} \in \text{Pic}(A)$ and $\varphi_{\mathcal{L}} : A \to \widehat{A}$ the associated homomorphism(15.7.4.3), then for any $a, a' \in A(\overline{K})$,

- $\widehat{h}_{\tau_{a'}^*\mathcal{L}}(a) = \widehat{h}_{\mathcal{L}}(a) + b(a,a')$.
- $\widehat{h}_{\mathcal{L}}(a) = \langle a, \mathcal{L}\rangle_{A,\text{N-T}}$.
- $b_{\mathcal{L}}(a,a') = \langle a, \varphi_{\mathcal{L}}(a')\rangle_{A,\text{N-T}} = \widehat{h}_{\varphi_{\mathcal{L}}(a')}(a)$.

⌟

Proof: 1: $b_{\mathcal{L}}(a,a') = \widehat{h}_{\mathcal{L}}(a+a') - \widehat{h}_{\mathcal{L}}(a) - \widehat{h}_{\mathcal{L}}(a') = \widehat{h}_{\mathcal{L}}(\tau_{a'}a) - \widehat{h}_{\mathcal{L}}(a) - \widehat{h}_{\mathcal{L}}(a')$. Then $b(\cdot,a') + \widehat{h}_{\mathcal{L}}$ is a representative in the class $h_{\tau_{a'}^*(\mathcal{L})}$ by functoriality. And it is a quadratic function, thus by uniqueness, we are done.

2: Because the pullback of p to $A \times \{\mathcal{L}\}$ is $\mathcal{L}$ by(9.7.2.34), and thus this follows from functoriality and(15.13.1.7).

3: By(15.7.4.3) and item1, $b(a,a') = \widehat{h}_{\varphi_{\mathcal{L}}(a')}(a)$. Thus we are done by item2. □

Cor. (15.13.1.9) [Regulator]. The Néron-Tate pairing induces a non-degenerate pairing $A(K)/A(K)_{\text{tor}} \times \widehat{A}(K)/\widehat{A}(K)_{\text{tor}} \to \mathbb{R}$. The discriminant of this pairing is called the **regulator** of A, denoted by $R(A/K)$. ⌟

Proof: Let $\mathcal{L} \in \text{Pic}(A)$ be ample, then $\varphi_{\mathcal{L}} : A \to \widehat{A}$ is an isogeny, thus $\varphi_{\mathcal{L}} : A(K)/A(K)_{\text{tor}} \to \widehat{A}(K)/\widehat{A}(K)_{\text{tor}}$ is injective, and by(15.14.1.7), the image is a subgroup of $\widehat{A}(K)/\widehat{A}(K)_{\text{tor}}$ of the same rank, thus we are done by(15.13.1.8) item3 and(15.13.1.4). □

Cor. (15.13.1.10). Let A be an Abelian variety, $c \in \mathrm{Pic}(A)$ an even ample class, $c' \in \mathrm{Pic}(A)$, then $\widehat{h}_{c'} = O(\widehat{h}_c^{1/2})$. ⌟

Proof: By(15.7.4.15), φ_c is isogeny thus surjective, thus we can assume $c' = \varphi_c(a')$ for some $a' \in A(K)$. Then by(15.13.1.8), $\widehat{h}_{c'}(a) = b_c(a, a')$. Because b_c is positive semi-definite by(15.13.1.3), by Cauchy-Schwartz(3.1.3.7), $|\widehat{h}_{c'}(a)|^2 \leq b(a,a)b(a',a') = 4\widehat{h}_c(a)\widehat{h}_c(a')$. □

Hilbert's Irreducibility Theorem

Prop. (15.13.1.11) [Runge's Theorem]. ⌟

Prop. (15.13.1.12) [Hilbert's Irreducibility Theorem]. Let C be a smooth irreducible projective curve over a number field K and let $f : C \to \mathbb{P}^1$ be a surjective rational function on C over K, then for all $n \in \mathbb{N}$ except for a set of natural density 0, the divisor $f^*[n]$ is a prime divisor over K. ⌟

Proof: Cf.[Diophantine Geometry, P319]. □

Local Height Pairings

Cf.[Sil99]Chap6 or [Local Heights on Curves, Gross, in Arithmetic Geometry] and [B-G06] or [Introduction to Diophantine Geometry, Lang].

Canonical Heights on Semi-Abelian Varieties

Cf.[Points of small height on semiabelian varieties]Section3 or [Poonen, Bogomolov plus Mordell-Lang].

Def. (15.13.1.13) [Canonical Height on Semi-Abelian Varieties]. ⌟

2 Isogenies

Thm. (15.13.2.1) [Masser-Wüstholz/Pellarin]. Let $F \in \texttt{NField}, d = [F : \mathbb{Q}]$. If $E, E' \in \mathcal{E}\mathrm{ll}/F$ are isogenous, then there exists an isogeny $\psi : E \to E'$ over F with degree$\leq \kappa(d)(1 + h^+(j(E)))^2$, where $\kappa(d)$ depends only on d and is effective. ⌟

Proof: **?** □

Cor. (15.13.2.2) [Bounded on Rational Isogenies]. Let $F \in \texttt{NField}, d = [F : \mathbb{Q}]$ and $E \in \mathcal{E}\mathrm{ll}/F$ without CM, and there is a cyclic isogeny $\varphi : E \to E'$ over F with degree δ, then $\delta \leq \kappa(d)(1 + h^+(j(E)))^2$. ⌟

Proof: Let $\psi : E \to E'$ be an isogeny of degree$\leq \kappa(d)(1 + h^+(j(E)))^2$. In fact we can assume that ψ is cyclic. Then $\varphi^\vee \circ \psi \in \mathrm{End}(E) = \mathbb{Z}$. Thus $\varphi = \pm\psi$ has degree$\leq \kappa(d)(1 + h^+(j(E)))^2$. □

Tate's Hom Conjecture

References are [Fal86] and [Tat66].

Lemma (15.13.2.3). Let $k \in \texttt{Field}, A_1, A_2 \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/k$, and $\ell \in \mathbf{P}\backslash \mathrm{char}\, k$, then the natural map

$$\mathrm{Hom}(A_1, A_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(A_1), T_\ell(A_2))$$

is injective. ⌟

Proof: Same as the proof of the Elliptic case**?** Cf.[Silverman]. □

Thm. (15.13.2.4) [Tate's Hom Conjecture, Tate/Faltings]. Let $k \in \texttt{Field}^{\text{fin}}$ or $k \in \texttt{GField}$, $\ell \in \mathbf{P} \setminus \{\text{char}\, k\}$, $A_1, A_2 \in \mathcal{A}b\,\mathcal{V}ar\,/k$, then

$$\text{Hom}(A_1, A_2) \otimes \mathbb{Z}_\ell \to \text{Hom}_{\text{Gal}_k}(T_\ell(A_1), T_\ell(A_2))$$

is an isomorphism. ⌟

Proof: Firstly notice that

$$\text{Hom}(A_1, A_2)_{\mathbb{Q}_\ell} \to \text{Hom}_{\text{Gal}_k}(V_\ell(A_1), V_\ell(A_2))$$

is injective, and it suffices to show this is surjective: This follows from(15.13.2.3) and the fact $\mathbb{Q}_\ell$ is flat over $\mathbb{Z}_\ell$ and

$$\text{Coker}\Big(\text{Hom}(A_1, A_2) \otimes \mathbb{Z}_\ell \to \text{Hom}_{\text{Gal}_k}(T_\ell(A_1), T_\ell(A_2))\Big)$$

is torsion-free, because if $[f] \in \text{Hom}_{\text{Gal}_k}(T_\ell(A_1), T_\ell(A_2))$ satisfies $n[f] = [g]$ for $g \in \text{Hom}(A_1, A_2) \otimes \mathbb{Z}_\ell$, then we may assume $n \in \ell^{\mathbb{Z}_+}$, and then g vanishes on $A_1[n]$, then $g = nf$ for some $f \in \text{Hom}(A_1, A_2)$. **?** □

Cor. (15.13.2.5) [Faltings Isogeny Theorem]. Let $k \in \texttt{Field}^{\text{fin}}$ or $k \in \texttt{GField}$, $\ell \in \mathbf{P} \setminus \{\text{char}\, k\}$, $A_1, A_2 \in \mathcal{A}b\,\mathcal{V}ar\,/k$, then A_1, A_2 are isogenous iff $T_\ell(A_1) \cong T_\ell(A_2)$ as Gal_k-modules. ⌟

3 Heights of Abelian Varieties

Cf.[Milne, Abelian Varieties] and [Faltings Height].

Def. (15.13.3.1) [Faltings Heights]. Let $F \in \texttt{NField}$ and $A \in \mathcal{A}b\,\mathcal{V}ar\,/F$, take the Néron model $\mathcal{A}/\mathcal{O}_F$, then $\mathcal{K}_{\mathcal{A}/\mathcal{O}_F}$ is an invertible sheaf, and thus $\omega_{\mathcal{A}/\mathcal{O}_F}$ is an invertible $\mathcal{O}_F$-sheaf, represented by a fractional ideal $M \subset F$, and $M \otimes_R F = \Gamma(A, \mathcal{K}_{A/F})$ by(9.1.1.14).

We define a norm on $M \otimes_F F_v = \Gamma(A_v, \mathcal{K}_{A_v/F_v})$ for each $v \in \Sigma_F^\infty$:

$$||\omega||_v = \Big((\frac{i}{2})^g \int_{A(\overline{F}_v)} \omega \wedge \overline{\omega}\Big)^{1/2}.$$

This make $\widetilde{M}$ a metrized line bundle on $\mathcal{O}_F$(16.2.1.1).

Then we define the **Faltings height** of A:

$$H_{\text{Fal}}(A) = H((\widetilde{M}, |\cdot|))\text{(16.2.1.2)}, \quad h_{\text{Fal}}(A) = \frac{1}{[F:\mathbb{Q}]} \log H_{\text{Fal}}(A).$$

More explicitly, take a non-zero holomorphic g-form ω on A, and for $v \in \Sigma_F^0$, let ω_v be a Néron differential on A_v, then

$$h_{\text{Fal}}(A) = \frac{-1}{[F:\mathbb{Q}]}\Big(\sum_{v \in \Sigma_F^0} \log |\frac{\omega}{\omega_v}|_v + \sum_{v \in \Sigma_F^\infty} \frac{[F_v : \mathbb{Q}_v]}{2} \log \Big|(\frac{\mathrm{i}}{2})^g \int_{A(\overline{F}_v)} \omega \wedge \overline{\omega}\Big|\Big).$$

⌟

Def. (15.13.3.2) [Stable Faltings Height]. Let $F \in \mathtt{NField}$ and $A \in \mathcal{A}b\,\mathcal{V}ar\,/F$, then by**??** there exists a finite extension L/F s.t. A_L is semistable. Then the Néron model of A_L are stable under base change**?**. Then we can define the **stable Faltings height** $h_{\mathrm{st}}(A) = h(A_L)$, which is invariant of L chosen. ⌟

Prop. (15.13.3.3). Let $F \in \mathtt{NField}$ and $A \in \mathcal{A}b\,\mathcal{V}ar\,/F$, then $h_{\mathrm{Fal}}(A) = h_{\mathrm{Fal}}(A^\vee)$. ⌟

Proof: Cf.[Szpiro, La Conjecture de Mordell, Séminaire Bourbaki, 1983/84]. □

Prop. (15.13.3.4) [Colmez]. If A, A' are isogenous, then $h_{\mathrm{Fal}}(A) = h_{\mathrm{Fal}}(A')$. ⌟

Proof: □

Thm. (15.13.3.5) [Heights and Isogenies]. Let $F \in \mathtt{NField}$, $\mathcal{A}_1, \mathcal{A}_2$ be semi-Abelian schemes over $\mathcal{O}_F$ of relative dimension g with proper generic fiber $A_1, A_2 \in \mathcal{A}b\,\mathcal{V}ar\,/F$. Let $\varphi : \mathcal{A}_1 \to \mathcal{A}_2$ be an isogeny with kernel $\mathcal{G}/\mathcal{O}_F$, then

$$h_{\mathrm{st}}(A_2) = h_{\mathrm{st}}(A_1) + \frac{1}{2}\log\deg(\varphi) - [F : \mathbb{Q}]\log e^*\Omega^1_{\mathcal{G}/\mathcal{O}_F}.$$

⌟

Proof: Cf.[Faltings, Lemma5] or [Faltings height].**?** □

Thm. (15.13.3.6)[Finiteness of Heights in an Isogeny Class]. Let $F \in \mathtt{NField}$ and $A \in \mathcal{A}b\,\mathcal{V}ar\,/F$ be semistable, then the set of Faltings height of $B \in \mathcal{A}b\,\mathcal{V}ar\,/F$ isogenous to A is finite. ⌟

Proof: This is the hardest part of the proof.**?** Cf.[Conrad Seminar, L20]. □

Modular Heights

Def. (15.13.3.7) [Modular Heights]. Consider the Siegel modular varieties $\mathcal{M}_{g,d}/\mathbb{Q}$ parametrizing Abelian schemes(19.1.3.3), then for any $F \in \mathtt{NField}$, $(A, \lambda) \in \mathcal{A}b\,\mathcal{V}ar^{\dim=g,\mathrm{polar}=d}\,/F$ defines a F-point $j((A, \lambda))$ of $\mathcal{M}^{g,d}$. Then we can define the **modular height** $h_M(A, \lambda)$ to be $h(j((A, \lambda)))$, where h is the Weil height associated to the canonical ample divisor on $\mathcal{M}^{g,d}$(19.1.3.4), which is defined up to a bounded function on $\mathcal{M}^{g,d}$. ⌟

Prop. (15.13.3.8) [Comparison of Heights]. For $F \in \mathtt{NField}$, there are constants c_1, c_2, c_3 s.t. for any semistable $(A, \lambda) \in \mathcal{A}b\,\mathcal{V}ar^{\mathrm{polar}}\,/F$,

$$|h_{\mathrm{Fal}}(A) - c_1 h_M(A, \lambda)| < c_2 \log h_M(A, \lambda) + c_3.$$

⌟

Proof: **?** Hard. Cf. [Chai and Faltings, 1990]. □

Prop. (15.13.3.9) [Height I]. Let $F \in \mathtt{NField}$ and $g, d, C \in \mathbb{Z}_+$, then up to isomorphism, there are only f.m. semistable $(A, \lambda) \in \mathcal{A}b\,\mathcal{V}ar^{g,\mathrm{polar}=d}\,/k$ s.t. $h_M(A, \lambda) < C$. ⌟

Proof: By the definition of Siegel modular varieties, two objects in $(A, \lambda) \in \mathcal{A}b\,\mathcal{V}ar^{g,\mathrm{polar}=d}\,/F$ corresponds to the same point of $\mathcal{M}^{g,d}$(15.13.3.7) iff they are isomorphic over $\overline{F}$. And by Northcott's theorem(15.2.1.24) the image of polarized Abelian varieties with bounded modular heights is finite. Thus the assertion follows from(15.13.5.2). □

Cor. (15.13.3.10) [Height II]. Let $F \in \texttt{NField}$ and $g, C \in \mathbb{Z}_+$, then up to isomorphism, there are only f.m. semistable $A \in \mathcal{A}b\mathcal{V}ar^g/F$ s.t. $h_{\text{Fal}}(A) < C$, by(15.13.3.8).

(Is this true for non-semistable varieties**?**). ⌟

Proof: By the proposition(15.13.3.9) and(15.13.3.8), the set of isomorphism classes of semistable Abelian varieties $(B, \lambda) \in \mathcal{A}b\mathcal{V}ar^{g,\text{polar}=d}/F$ is finite. Now notice for any $A \in \mathcal{A}b\mathcal{V}ar/F$, $B = (A \times A^\vee)^4$ is principally polarized by(15.7.7.2), and $h(B) = 8h(A)$ by(15.13.3.3), so we are done. □

Elliptic Curve case

Prop. (15.13.3.11)[Heights of Elliptic Curves]. For $F \in \texttt{NField}$ and $E \in \mathcal{E}ll/F$. For each $v \in \Sigma_F^\infty$, let $\tau_v \in \mathcal{H}$ in the fundamental domain s.t. $E_{\overline{K}_v} \cong E_{\tau_v}$. Then

$$12[F:\mathbb{Q}]h_{\text{Fal}}(E/F) = \log\left|\operatorname{Nm}_{F/\mathbb{Q}} N_{E/F}\right| - \sum_{v \in \Sigma_F^\infty}[F_v:\mathbb{Q}_v]\log\left|\Delta(\tau_v)(\operatorname{Im}\tau_v)^6\right|.$$

⌟

Proof: Choose any Weierstrass model $W: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, and let Δ be its discriminant, and take

$$\omega = \Delta.\Big(\frac{\mathrm{d}x}{2y + a_1x + a_3}\Big)^{\otimes 12}.$$

Then notice this ω is invariant under change of variables, thus $-\sum_{v\in\Sigma_F^0}\log|\frac{\omega}{\omega_v}|_v = |\operatorname{Nm}_{F/\mathbb{Q}} N_{E/F}|$**?**. □

Prop. (15.13.3.12). For $F \in \texttt{NField}, E \in \mathcal{E}ll/F$,

$$O(1) \le h^+(j(E)) + \frac{1}{[F:\mathbb{Q}]}\log|\operatorname{Nm}_{F/\mathbb{Q}}\Upsilon_{E/F}| - 12h_{\text{Fal}}(E/F) \le 6\log(1 + h^+(j(E))) + O(1).$$

In particular, if E/F is semistable, then

$$|h^+(j(E)) - 12h_{\text{Fal}}(E/F)| \le 6\log(1 + h^+(j(E))) + O(1),$$

which is a special case of(15.13.3.8). ⌟

Proof: Cf.[Heights and Elliptic Curves, P258]**?**. □

Cor. (15.13.3.13). For any $\varepsilon \in \mathbb{R}_+$, we have: $E \in \mathcal{E}ll/\mathbb{Q}$,

$$h_{\text{Fal}}(E/\mathbb{Q}) + O(1) \le \frac{1}{12}\max(|j(E)|, |\Delta_E^{\min}j(E)|) \le (1+\varepsilon)h_{\text{Fal}}(E/\mathbb{Q}) + O_\varepsilon(1),$$

$$h_{\text{Fal}}(E/\mathbb{Q}) + O(1) \le \frac{1}{12}\max(|c_4(E)|^3, |c_6(E)|^2) \le (1+\varepsilon)h_{\text{Fal}}(E/\mathbb{Q}) + O_\varepsilon(1).$$

⌟

Proof: By definition, $h^+(j(E)) + \log|\Upsilon_E| = \log\max(|j\Delta_E^{\min}, |\Delta_E^{\min}|)$. So the first inequality follows from(15.13.3.12) and the fact $\log(1+h) < \varepsilon h + O_\varepsilon(1)$ for $h \in \mathbb{R}_+$.

The second inequality follows from the first by the definition of Δ and j(15.11.1.5). □

Cor. (15.13.3.14) [Northcott Property for Elliptic Curves]. For $d, C \in \mathbb{R}_+$, there exists only f.m. pairs (F, E) where $F \in \mathtt{NField}, E \in \mathcal{E}\mathrm{ll}/F$ s.t. $F = \mathbb{Q}(j(E))$, $\deg(F) \le d$ and $h_{\mathrm{Fal}}(E/F) \le C$. ⌟

Proof: It follows from(15.13.3.12) that for such pairs (F, E), $h^+(j(E))$ is bounded from above, so by Northcott, there are only f.m. possibilities for $j(E)$. Then it suffices to show that for any $E \in \mathcal{E}\mathrm{ll}/\overline{\mathbb{Q}}$, there are only f.m. $E' \in \mathcal{E}\mathrm{ll}/\mathbb{Q}(j(E))$ s.t. $j(E') = j(E)$ and $h(E'/\mathbb{Q}(j(E))) \le C$.

Denote $F = \mathbb{Q}(j(E))$, it follows from(15.13.3.12) that for any such E', $|\mathrm{Nm}_{F/\mathbb{Q}} \Upsilon_{E'/F}|$ is bounded. Choose $S \in \Sigma_F$ s.t. $S(6) \cup \Sigma_F^\infty \cup \mathrm{Ram}_{E/F} \subset S$ and $\mathrm{cl}(\mathcal{O}_{F,S}) = 1$, **?** □

4 Small Points

Notation (15.13.4.1).

- Let $F \in \mathtt{NField}$ and $G \in \mathrm{semi}\,\mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/F$ with maximal subtorus T of dimension t and quotient $A = G/T$ of dimension g.
- Let $\mathcal{L}$ be the canonical line bundle and h be a canonical height on A(15.13.1.13).
- For each $x \in G(\overline{\mathbb{Q}})$, use $\mathcal{O}(x)$ to denote the Galois orbit of x.
- A **torsion subvariety** is a subvariety $Y \subset G$ of the form $Y = x + B$ where x is a torsion point and $B \subset G$ is an semi-Abelian subvariety.

⌟

Def. (15.13.4.2) [Small Sequences]. A sequence $(x_n)_{n\in\mathbb{N}} \subset G(\overline{F})$ is called

- **strict** if no infinite subsequence is contained in a proper torsion subvariety of A.
- **generic** if no infinite subsequence is contained in a proper subvariety of A.
- **small** if $\lim_{n\to\infty} h(x_n) = 0$.

⌟

Prop. (15.13.4.3). If $X \in \mathcal{V}\mathrm{ar}/\overline{\mathbb{Q}}$ and $(x_n) \in X^{\mathbb{N}}$ is a Zariski dense sequence in X, then (x_n) has a generic sequence. ⌟

Proof: This follows from the fact that there are only countably many proper subvarieties of X. □

Thm. (15.13.4.4) [Strong Equidistribution Conjecture, Bilu/Szpiro-Ullmo-Zhang/Kuhne]. For any strict small sequence(15.13.4.2) $(x_i) \in A^{\mathbb{N}}$, there is a weak convergence of measures on $G_{\mathbb{C}_v}^{\mathrm{an}}$:

$$\frac{1}{\#\mathcal{O}_v(x_i)} \sum_{y\in\mathcal{O}_v(x_i)} \delta_y \rightharpoonup \frac{1}{\deg_{\mathcal{L}}(\overline{G})} c_1(\overline{\mathcal{L}_v})^{\wedge(g+t)}.$$

Notice for $v \in \inf \Sigma_F$, $c_1(\overline{\mathcal{L}_v})^{\wedge(g+t)}$ is a Haar measure on $G_{\mathbb{C}_v}^{\mathrm{an}}$. ⌟

Proof: Cf.[Points of small height on semiabelian varieties]P2078**?**. The proof is Arakelov, and is similar to that of the Abelian variety case. □

Cor. (15.13.4.5) [Mordell-Lang plus Bogomolov, Poonen/Remond]. Let $\Gamma \subset G(\overline{F})$ be a f.g. subgroup, with divisible hull Γ'. For $\varepsilon \in \mathbb{R}_+$, denote $\mathbb{D}(\Gamma', \varepsilon) \subset G(\overline{F})$ the metric nbhd in the metric defined by the canonical height**?**. Then for any closed subvariety $X \subset A$, there exists some $\varepsilon \in \mathbb{R}_+$ s.t. $X(\overline{F}) \cap \Gamma'_\varepsilon$ is contained in a finite union $\cup_j Z_j$ where each $Z_j \subset X_{\overline{F}}$ is a torsion subvariety(15.13.4.1). ⌟

Proof: ?. Cf.[Poonen]. □

Cor. (15.13.4.6) [Bogomolov Conjecture, Ullmo-Zhang]. If $X \subset A$ is subvariety but not a torsion subvariety, then there exists $\varepsilon \in \mathbb{R}_+$ s.t. $\{P \in X(\overline{F}) | h(P) \leq \varepsilon\}$ is not Zariski-dense in X. ⌟

Proof: ? □

Cor. (15.13.4.7) [Manin-Mumford-Lang Conjecture, Raynaud]. By Bogomolov conjecture(15.13.4.6) and(15.13.1.5), if $X \subset G$ is subvariety but not a torsion subvariety, then $X(\overline{\mathbb{Q}}) \cap G(\overline{\mathbb{Q}})_{\mathrm{tor}}$ is not Zariski-dense in X. ⌟

Thm. (15.13.4.8) [Equidistribution of Small Points, Zhang]. If $(x_n)_{n \in \mathbb{N}}$ is a small and strict sequence in A, then for any continuous function on A^{an},

$$\lim_{n \to \infty} \frac{1}{\#\mathcal{O}(x_n)} \sum_{y \in O(x_n)} f(y) = \int_{A^{\mathrm{an}}} f \mathrm{d}x.$$

⌟

Proof: Firstly (x_n) is generic: If there is an infinite subsequence with Zariski closure a proper subvariety $X \subset A$, then it follows from Bogomolov's conjecture(15.13.4.6) that X is a torsion subvariety. Then (x_n) is not strict, contradiction.

□

Cor. (15.13.4.9). Let $S \subset A^{\mathrm{an}}$ be a closed subset, then S contains only f.m. non-Galois-conjugate maximal torsion subvarieties. And if S' is the complement in S of all the Galois orbits of maximal torsion subvarieties contained in S, then there exists $\varepsilon \in \mathbb{R}_+$ s.t. for any $x \in A(\overline{\mathbb{Q}})$ s.t. $O(x) \subset S'$, $h(x) > \varepsilon$. ⌟

Proof: ? □

Thm. (15.13.4.10) [Theorem of Successive Minima]. Let $F \in \mathtt{NField}, X \in \mathcal{V}\mathrm{ar}^d/F$, and $\mathcal{L}$ an ample line bundle on X with a semipositive adelic metric $|| \cdot ||$. For $1 \leq i \leq d$, define

$$\lambda_i = \sup_{Y \subset X, \dim Y = i} \Big(\inf_{P \in X(\overline{\mathbb{Q}}) \setminus Y(\overline{\mathbb{Q}})} h_{\mathcal{L}}(P) \Big),$$

then

$$\lambda_d \geq h_{\mathcal{L}}(X) \geq \frac{1}{d}(\lambda_1 + \ldots + \lambda_d).$$

⌟

Proof: Cf.[Small Points and Adelic metric, Shouwu Zhang].? □

Small Points on $\mathbb{G}_m^n$

References are [Sch96] and [B-G06].

Small Points on Elliptic Curves

Conj. (15.13.4.11)[Lang's Height Conjecture]. For any $F \in \texttt{NField}$, there exists $c_1(F), c_2(F) \in \mathbb{R}_+$ s.t. for any $E \in \mathcal{E}\mathrm{ll}/F$ and $P \in E(F) \setminus E(F)_{\mathrm{tor}}$,

$$h_{\text{N-T}}(P) \geq c_1(F) \log |\operatorname{Nm}_{F/\mathbb{Q}} \Delta_{E/F}^{\min}| + c_2(F).(15.11.4.23)$$

⌟

Thm& Conj.Cor. (15.13.4.12) [Silverman]. This conjecture is true when we restrict to $E \in \mathcal{E}\mathrm{ll}/F$ with $j(E) \in \mathbb{Z}$. ⌟

Proof: Cf.[Sil86]P263. □

5 Finiteness Theorems(Faltings)

Prop. (15.13.5.1). Let $L/F \in \texttt{NField}$ be Galois, then for any $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/F$, there exists f.m. isomorphism classes of $B \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/F$ s.t. $A_L \cong B_L$. ⌟

Proof: Cf.[Conrad note, L14]**?** □

Prop. (15.13.5.2) [Weak Finiteness, Faltings]. Let $F \in \texttt{NField}$ and $(A, \lambda) \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}^{g,\mathrm{polar}=d}/F$, then there exists only f.m. isomorphism classes of $(B, \lambda') \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}^{g,\mathrm{polar}=d}/F$ s.t. $(A_{\overline{F}}, \lambda) \cong (B_{\overline{F}}, \mu)$. ⌟

Proof: Firstly, by(15.7.12.11), any such B is also semistable, so the set of good reductions are stable under base change, thus the set of good reductions of A and B in Σ_F are the same.

Then by(15.14.1.1) and(14.4.1.28), for $\ell \in \mathbf{P}\backslash\{2\}$, there is a finite extension L/F s.t. every ℓ-torsion points of such B are in $B(L)$.

Now any such B are isomorphic to A over L as above: Given any isomorphism $\alpha : (A_{\overline{F}}, \lambda) \cong (B_{\overline{F}}, \mu)$, for $\alpha \in \mathrm{Gal}_L$, α and $\sigma(\alpha)$ has the same action on ℓ-torsion points, as all these points are L-rational, so $\sigma(\alpha)^{-1} \circ \alpha$ acts trivially on $A[\ell]$, which implies by(15.7.7.6) that $\sigma = \alpha(\sigma)$, so σ is defined over L and we are done.

Finally we finish using(15.13.5.1) and(15.7.7.3). □

Thm. (15.13.5.3) [Finiteness I]. Let $F \in \texttt{NField}$ and $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/F$, then there are only f.m. isomorphism classes of Abelian varieties $B \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/F$ isogenous to A. ⌟

Proof: If A is semistable, then by(15.7.12.11), any $B \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/F$ isogenous to A is also semistable. Then we are done by(15.13.3.10) and(15.13.3.6).

For a general A, there exists a finite extension L/F s.t. A_L is semistable by**??**. Then the general case reduced to the semistable case by using(15.13.5.1). □

Thm. (15.13.5.4)[Finiteness II, Shafarevich/Faltings]. Let $F \in \texttt{NField}, 0 \subset_{\mathrm{fin}} S \subset \Sigma_F$, then there are only f.m. isomorphism classes of $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}^g/F$ having good reduction at all finite places outside S. ⌟

Proof: By(15.13.5.3), it suffices to show that there are only f.m. isogeny classes of $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}^g/F$ having good reduction at all finite places outside S. But then we can use(15.7.12.19) and the fact there are only f.m. such polynomials $P_\ell(A_v, t)$ because of Weil conjecture. □

Mordell-Lang Conjecture

Thm. (15.13.5.5) [Mordell-Lang Conjecture, Falting-Vojta/Hindry/Raynaud/McQuillan]. Let $F \in$ `NField` and G/F be a semi-Abelian variety. Suppose $X \subset A$ is a closed subvariety that is not a translate of a semi-Abelian subvariety of A, and $\Gamma \subset A(\overline{F})$ is a f.g. subgroup, with divisible hull Γ', then $X(\overline{F}) \cap \Gamma'$ is not Zariski dense in X. ⌟

Proof: ? □

Applications to Curves

Prop. (15.13.5.6) [Genus 0 Curves]. For $F \in$ `GField` of characteristic$\neq 2$ and any smooth complete curve C/F genus 0 is a conic in $\mathbb{P}^2$. Thus by(6.12.8.2), it is isomorphic to $\mathbb{P}^1$ iff it has a rational point. But by Hasse-Weil principle, this is equivalent to it having a rational point over each local field of F, and this can be understood via Hilbert symbol. ⌟

Thm. (15.13.5.7) [Shafarevich's Conjecture, Faltings]. Let $F \in$ `GField` and $S \subset \Sigma_F$ a finite set of places, $g \in \mathbb{Z}_+$, then there are only f.m. isomorphism classes of smooth curves over k of genus g having good reduction at all finite places outside S. ⌟

Proof: This follows from(15.7.10.16)(15.7.10.15) and(15.7.7.3)(15.13.5.4). □

Prop. (15.13.5.8) [Kodaira-Parshin]. Let $F \in$ `NField` and S is a finite set of places of F containing all places over 2, then for any complete non-singular curve C/F of genus≥ 1 having good reduction at non-Archimedean places outside S, there exists a finite extension L/F and a constant N, s.t.: For any $P \in C(F)$, there exists a complete smooth curve C^P over L and a finite map $\varphi^P : C^P \to C_L$, that satisfies

- C^P has good reduction at places not above S.
- $g(C^P) \leq N$.
- φ_P is ramified exactly at P.

⌟

Proof: Cf.[Mil08]P115, 145.? □

Thm. (15.13.5.9)[Uniform Mordell Conjeture1922, Faltings1983]. For $g \in \mathbb{Z}_{\geq 2}$ and $d \in \mathbb{Z}$, there exists $C(g, d) \in \mathbb{Z}_+$ s.t. for any $F \in$ `NField` with $\deg(F) = d$ and C/F be a complete non-singular curve of genus g, we have

$$\#C(F) \leq C(g, d).$$

⌟

Proof: We only prove that $\#C(F)$ is finite?.

Using the construction of Kodaira-Parshin(15.13.5.8), there is a finite extension L/F s.t. any $P \in C(F)$ corresponds to a curve C^P over L and a map $\varphi_P : C^P \to C_L$. By Shafarevich's conjecture applied to L(15.13.5.7), there are only f.m. isomorphism classes of C^P. But for different P, Q s.t. $C^P \cong C^Q$, the maps φ_P, φ_Q are non-isomorphic, as they are ramified at different places. So we are done by de Franchis' theorem(6.12.1.34). □

Prop. (15.13.5.10)[Manin-Mumford]. Let $F \in$ `NField` and C/F be a complete non-singular curve of genus $g \geq 2$, and J the Jacobian of C. Fix an embedding $C \hookrightarrow J$ over F, then $\#C(\overline{F}) \cap J(\overline{F})_{\text{tor}} < \infty$. ⌟

Proof: This follows from the Manin-Mumford-Lang conjecture(15.13.4.7), as C is a not a torsion subvariety. □

6 Galois Cohomologies of Abelian Varieties

Prop. (15.13.6.1) [Fundamental Exact Sequence]. Let $\varphi : X \to X'$ be an étale isogeny between Abelian varieties over a field k, then there is an exact sequence

$$0 \to \ker(\varphi)(k^s) \to X(k^s) \to X'(k^s) \to 0$$

by(9.1.5.5), thus taking Galois cohomology, there is an exact sequence

$$0 \to X'(k)/\varphi(X(k)) \xrightarrow{\delta} H^1(G_k, X[\varphi]) \to H^1(G_k, X)[\varphi] \to 0.$$

⌟

Cor. (15.13.6.2). By(15.7.6.14), if $n \in \mathbb{Z} \cap K^\times$, then there is an exact sequence

$$0 \to X(k^s)/nX(k^s) \xrightarrow{\delta} H^1(G_k, X[n]) \to H^1(G_k, X)[n] \to 0.$$

And the first map is described as follows: for $P \in X(k^s)$, let $[n]Q = P$ where $Q \in K(k^s)$, then P is mapped to the 1-cocycle $f(\sigma) = \sigma(Q) - Q$. ⌟

Prop. (15.13.6.3). Let F be a global field or the function field of a non-singular smooth curve over an alg.closed field k, $\varphi : X \to X' \in \mathcal{A}b\mathcal{V}ar/F$ an étale isogeny, then by restriction(8.7.1.10), there is an exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X'(F)/\varphi(X(F)) & \longrightarrow & H^1(\mathrm{Gal}_F, X[\varphi]) & \longrightarrow & H^1(\mathrm{Gal}_F, X)[\varphi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \mathrm{res} & & \downarrow \mathrm{res} & & \\ 0 & \longrightarrow & \prod_{v\in\Sigma_F^{\mathrm{fin}}} X'(F_v)/\varphi(X(F_v)) & \longrightarrow & \prod_{v\in\Sigma_F^{\mathrm{fin}}} H^1(\mathrm{Gal}_{F_v}, X[\varphi]) & \longrightarrow & \prod_{v\in\Sigma_F^{\mathrm{fin}}} H^1(\mathrm{Gal}_{F_v}, X)[\varphi] & \longrightarrow & 0 \end{array}.$$

Where v are extended to K^s arbitrarily. ⌟

Def. (15.13.6.4) [(Classical)Selmer Groups]. Let F be a global field or the function field of a non-singular smooth curve over an alg.closed field k, $\varphi : A \to A' \in \mathcal{A}b\mathcal{V}ar/F$ an étale isogeny, the φ-**Selmer group** of A/F is a subgroup of $H^1(\mathrm{Gal}_F, A[\varphi])$ defined by

$$\mathrm{Sel}^\varphi(A/F) = \ker\Big(H^1(\mathrm{Gal}_F, A[\varphi]) \to \prod_{v\in\Sigma_F} H^1(\mathrm{Gal}_{F_v}, A)[\varphi]\Big).$$

Notice the kernel is independent of the extension of v to F^s, because any two such extensions induce conjugate groups Gal_{F_v} in Gal_F and use(8.7.1.12). ⌟

Def. (15.13.6.5)[Shafarevich-Tate Group]. The **Shafarevich-Tate group** of $A \in \mathcal{A}b\mathcal{V}ar/F$ is the subgroup of $H^1(\mathrm{Gal}_F, A[\varphi])$ defined by

$$Ш(A/F) = \ker\Big(H^1(\mathrm{Gal}_F, A) \to \prod_{v\in\Sigma_F^{\mathrm{fin}}} H^1(\mathrm{Gal}_{F_v}, A)\Big).$$

Notice the kernel is independent of the extension of v to F^s, because any two such extensions induces conjugate groups Gal_{F_v} in Gal_F and use(8.7.1.12).

For $f : A \to B \in \mathcal{A}b\mathcal{V}ar/F$, there is a natural map $f_* : Ш(A/F) \to Ш(B/F)$. ⌟

Prop. (15.13.6.6) [Selmer Groups and Shafarevich-Tate Groups]. Let C be a proper Dedekind scheme or a non-singular curve over a field k with fraction field F, $\varphi : A \to A'$ an étale isogeny of Abelian varieties over F, then there is an exact sequence

$$0 \to A'(K)/\varphi(A(K)) \to \mathrm{Sel}^{\varphi}(A/K) \to Ш(A/K)[\varphi] \to 0.$$

⌟

Proof: This exact sequence is a consequence of (15.13.6.3) and (15.13.6.4)(15.13.6.5). □

Remark (15.13.6.7) [Computability]. It is difficult to characterize $A'(K)/\varphi(A(K)) \subset \mathrm{Sel}^{\varphi}(A/K)$. ⌟

Prop. (15.13.6.8) [$\mathrm{Sel}^{\varphi}(A)$ **is Finite].** Let F be a global field or the function field of a non-singular smooth curve over an alg.closed field k, $\varphi : A \to A'$ an étale isogeny of Abelian varieties over F, then if S is a finite set of places of F containing all the places dividing $\deg(\varphi)$, and the places that A has bad reductions, then any element in $\mathrm{Sel}^{\varphi}(A/F)$ is unramified at all finite places outside S. In particular, $\mathrm{Sel}^{\varphi}(A/F)$ is finite, by (8.7.3.11). ⌟

Proof: By definition of Sel^{φ} and (15.13.6.3), if $\xi \in \mathrm{Sel}^{\varphi}(A/F)$, then for any $v \in \Sigma_F^0$, there is some $P \in A(F_v^s)$ s.t. $\xi_\sigma = \sigma(P) - P \in A[\varphi]$ for any $\sigma \in G_v$. But if A has good reduction at v and $\sigma \in I_v$, then $\sigma(P) - P$ mapsto $\widetilde{O} \in \widetilde{A}_v$. But notice $A[\varphi] \subset A[m]$ which maps injectively into $\widetilde{A}_v(k_v)$ by (15.11.4.19) if v is not dividing $\deg(\varphi)$. Thus in this case, $\xi_\sigma = 0$ for any $\sigma \in I_v$. □

Cor. (15.13.6.9) [ℓ^∞**-Selmer Groups].** If $\ell \in \mathbf{P} \setminus \mathrm{char}\, F$, then the ℓ-primary part $Ш(A/F)[\ell^\infty] = \varinjlim_{n\geq 1} Ш(A/F)[\ell^n]$ is isomorphic to $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\delta_\ell} \times T_\ell$ for some $\delta_\ell \in \mathbb{N}$ and $T_\ell \in \mathcal{A}\mathrm{b}^{\mathrm{fin}}$. And define

$$\mathrm{Sel}^{\ell^\infty}(A/F) = \varinjlim_{n\geq 1} \mathrm{Sel}^{\ell^n}(A/F),$$

called the ℓ^∞**-Selmer group**. Then by taking limits of the exact sequence in (15.13.6.6), there is an exact sequence

$$0 \to A(F) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \to \mathrm{Sel}^{\ell^\infty}(A/F) \to Ш(A/F)[\ell^\infty] \to 0.$$

If we define the ℓ^∞**-Selmer rank** $\mathrm{rank}_\ell(A/F) = \mathrm{rank}(A/F) + \delta_\ell$, then

$$\mathrm{Sel}^{\ell^\infty}(A/F) = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\mathrm{rank}_\ell(A/F)} \cdot \widetilde{Ш}(A/F)[\ell^\infty],$$

where $\#\widetilde{Ш}(A/F)[\ell^\infty] < \infty$. Notice $\mathrm{rank}_\ell(A/F)$ is a cohomological number. ⌟

Conj. (15.13.6.10) [Tate-Shafarevich]. For $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/F$, $\#Ш(A/F) < \infty$. ⌟

Proof: □

Remark (15.13.6.11). There are still no $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ with $\mathrm{rank}_{\mathrm{an}}(E/\mathbb{Q}) \geq 2$ s.t. $Ш(E/\mathbb{Q})$ can be shown to be finite. ⌟

Prop. (15.13.6.12) [Cassels-Tate Pairing]. Let $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}/F$ and $\widehat{A}$ its dual, then there is a bilinear **Cassels-Tate pairing** $Ш(A/K) \times Ш(\widehat{A}/K) \to \mathbb{Q}/\mathbb{Z}$ and the kernel on both sides are the set of divisible elements. ⌟

Proof: Cf.[Birch and Swinnerton-Dyer Conjecture, P10].**?** □

Cor. (15.13.6.13) [Principally Polarized Case]. If $K \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/F$ has a principal polarization λ that comes from a rational divisor D, then the pullback pairing $Ш(A/K) \times Ш(A/K) \to \mathbb{Q}/\mathbb{Z}$ is alternating. In particular, if $\#Ш(A/F) < \infty$, then it is a perfect square, by(3.1.3.16).

In particular, if $E \in \mathcal{E}\mathrm{ll}/F$ and $\#Ш(E/F) < \infty$, then it is a perfect square. ⌟

Proof: □

Remark (15.13.6.14). This is not right for general Abelian varieties. ⌟

The discussion of Selmer groups and ranks are continued in B-S.D Conjecture21.6.

Elliptic Curves

Mazur's Control Theorem

Thm. (15.13.6.15) [Mazur]. For $F \in \mathtt{NField}, E \in \mathcal{E}\mathrm{ll}/F, p \in \mathbf{P}$, and E has good ordinary reduction over all primes lying over p. Assume $F_\infty = \cup_n F_n$ is a $\mathbb{Z}_p$-extension of F, then the natural map

$$\mathrm{Sel}(E/F_n)_p \to \mathrm{Sel}(E/F_\infty)_p^{\mathrm{Gal}(F_\infty/F_n)}$$

has finite kernels and cokernels of bounded orders as $n \to \infty$. ⌟

Proof: Cf.[Mazur's Control Theorem for Elliptic Curves]. □

15.14 Rational Points

Main references are [Sta], [Abelian Varieties notes Conrad], [Mil08], [B-G06], [Abelian Variety van der Geer], [BLR90], [Sil16] and [Sil99], [Sil11], http://www-personal.umich.edu/~asnowden/teaching/2013/679/index.html.

1 Mordell-Weil Theorem

Prop. (15.14.1.1)[Local Chevalley-Weil Theorem for Abelian Varieties]. Let S be a Dedekind scheme with function field F, Let A be an Abelian variety over F and $m \in \mathbb{Z} \cap F^*$. Let $s \in S$ be a closed point s,t. A has good reduction over $\mathcal{O}_{S,s}$ and $m \neq 0 \in \kappa(s)$, then for any $P \in A(\overline{F})$, the extension $\kappa(P)/\kappa([m]P)$ is unramified at all places over v. ⌟

Proof: By base change, we may assume $Q = [m]P$ is a rational point. Let w be a place of $\kappa(P)$ that $w|v_s$ with valuation ring R_w. As A has good reduction in v, A extends to an Abelian scheme $\overline{A}$ over $\mathcal{O}_{S,s}$, then the valuation criterion of properness shows P extends to a R_w-valued point of $\overline{A}$. Now the theorem follows from(15.7.6.14) and(6.6.5.16). □

Cor. (15.14.1.2). Let F be a global field, $X \in \mathcal{A}b\,\mathcal{V}ar\,/F$ and $n \in \mathbb{Z} \cap F^*$, $L = K(X[n](\overline{F}))$, i.e. the composite of all fields in $\overline{F}$ obtained by adjoining $[n]^{-1}x, x \in X(F)$, then L is a finite field extension of F. ⌟

Proof: This follows from the proposition and(14.4.1.28). □

Lemma (15.14.1.3)[Weak Mordell-Weil Theorem]. Let $F \in$ `GField` and $X \in \mathcal{A}b\,\mathcal{V}ar\,/F$, then for $n \in \mathbb{Z} \cap F^*$, $X(F)/nX(F)$ is finite. ⌟

Proof: This follows from the finiteness of the Selmer group(15.13.6.8) and(15.13.6.6). □

Prop. (15.14.1.4)[Mordell-Weil Theorem]. Let $F \in$ `GField`, then the group $X(F)$ of rational points of an Abelian variety X is f.g. ⌟

Proof: Because of(15.14.1.3) and(15.13.1.3), this follows from(3.1.3.15) applied to $M = X(K')$ and the symmetric bilinear form on $X(K')$ given by(15.13.1.3). □

Remark (15.14.1.5) [Computability]. The difficulty of computing $X(F)$ lies entirely at computing $X(F)/nX(F)$ for some n, for which, see(15.13.6.7). ⌟

Cor. (15.14.1.6) [Rank]. $X(F) \cong \mathbb{Z}^r \oplus X(F)_{\mathrm{tor}}$, where $X(F)_{\mathrm{tor}}$ is a finite group, and r is called the **rank of** X. ⌟

Cor. (15.14.1.7) [Isogenous Varieties have the same Rank]. Let $F \in$ `GField` and $X, X' \in \mathcal{A}b\,\mathcal{V}ar\,/F$ are isogenous, then $\mathrm{rank}(X) = \mathrm{rank}(X')$. In particular, $\mathrm{rank}(X) = \mathrm{rank}(\widehat{X})$. ⌟

Proof: The isogeny implies $X(F)/X(F)_{\mathrm{tor}} \to \widehat{X}(F)/\widehat{X}(F)_{\mathrm{tor}}$ is injective. Thus $\mathrm{rank}(X) \leq \mathrm{rank}(\widehat{X})$. The converse follows from(15.7.6.3). □

2 Lang-Néron Theorem

Main references are [Con06].

Def. (15.14.2.1) [Regular Extensions]. A field extension K/k is called **primary** if k is separably closed in K. It is called **regular** if it is separable and primary. ⌟

Prop. (15.14.2.2). Let K/k be a primary extension, then

- If $A \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/k$, then any Abelian subvariety of A_K is defined over k.
- If $A, B \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/k$, then any homomorphism $A_K \to B_K$ is defined over k.

⌟

Proof:

□

Prop. (15.14.2.3) [K/k-Images and K/k-Traces]. For a field extension K/k, the **K/k-image** is a functor $\mathrm{Im}_{K/k} : \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/K \to \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/k$ left adjoint to the base change functor, and **K/k-trace** is a functor $\mathrm{tr}_{K/k} : \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/K \to \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/k$ right adjoint to the base change functor.

Then for K/k primary, $\mathrm{Im}_{K/k}$ and $\mathrm{tr}_{K/k}$ exist, and are resp. left and right inverses to the base change functor. Also there is a natural isomorphism

$$\widehat{\mathrm{Im}_{K/k}(A)} \cong \mathrm{tr}_{K/k}(\widehat{A}).$$

The adjunction maps are denoted by

$$\tau_{A,K/k} : \mathrm{tr}_{K/k} A \to A, \quad \lambda_{A,K/k} A \to \mathrm{Im}_{K/k} A.$$

⌟

Proof: It suffices to prove for $\mathrm{Im}_{K/k}$, and $\mathrm{tr}_{K/k}$ follows by double duality theorem(15.7.4.18). For this, Cf.[Con06]P16**?**. □

Prop. (15.14.2.4). Let K/k be a primary extension and $A \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/K$, the unique map $\mathrm{tr}_{K/k} A \to \mathrm{Im}_{K/k} A$ descending $\lambda_{A,K/k} \circ \tau_{A,K/k}$ is an isogeny. ⌟

Proof: Cf.[Con06]P22**?**. □

Prop. (15.14.2.5). Let K/k be a regular extension, then for any $A \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/K$, the finite group $\ker(\tau_{A,K/k})$ is connected and coconnected. In particular, $\tau_{A,K/k}(K) : \mathrm{tr}_{K/k}(A)(K) \to A(K)$ is injective. ⌟

Prop. (15.14.2.6) [Lang-Néron]. Let K/k be a f.g. regular extension, then $A(K)/\mathrm{tr}_{K/k}(A)(k)$ is a f.g. Abelian group. ⌟

Proof: Cf.[Con06]P23**?**. □

Prop. (15.14.2.7) [Grothendieck]. Let $K \in \texttt{Field}, K = \overline{K}$, with prime field k, then any Abelian variety of CM-type over K is isogenous to an Abelian variety defined over a finite extension of k. ⌟

Proof: Cf.[Oort, The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field]. □

3 Elliptic Curve case

Torsion Points

Main references are [Maz78].

Prop. (15.14.3.1) [Controlling Torsion Points]. Let K be a number field, let E be given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in \mathcal{O}_K[X, Y].$$

Let $P = (x_0, y_0) \in E(K)$ be a torsion point of exact order m, then

- If m is not a p-power, then $x_0, y_0 \in \mathcal{O}_K$.
- If $m = p^n$, then for any place v of K, $v(x) \geq -2\lfloor\frac{v(p)}{p^n - p^{n-1}}\rfloor$, $v(y) \geq -3\lfloor\frac{v(p)}{p^n - p^{n-1}}\rfloor$.

⌟

Proof: This follows by base change E to each $\mathcal{O}_{K,v}$ and use(15.11.4.20). □

Cor. (15.14.3.2) [Integrality of Torsion Points in $\mathbb{Q}$]. Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ and $P = (x_0, y_0) \in E(\mathbb{Q})$ a torsion point of exact order m. then if m is not a p-power, $x_0, y_0 \in \mathbb{Z}$. If $m = p^n$, then $\lfloor\frac{v(p)}{p^n - p^{n-1}}\rfloor = 0$ unless $p = 2$ and $n = 1$. Thus $x_0 \in \frac{1}{4}\mathbb{Z}, x_0 \in \frac{1}{8}\mathbb{Z}$, and if $m \geq 3$, $x_0, y_0 \in \mathbb{Z}$.

The former case can occur, for example

$$E : y^2 + xy = x^3 + 4x + 1, \quad (-\frac{1}{4}, \frac{1}{8}) \in E(\mathbb{Q})[2].$$

⌟

Prop. (15.14.3.3) [Nagell–Lutz]. Let F be a number field and $E \in \mathcal{E}\mathrm{ll}/F$ be given by a Weierstrass equation

$$E : y^2 = x^3 + Ax + B \in \mathbb{Z}[x, y],$$

Let $P = (x_0, y_0) \in E(\mathbb{Q})_{\mathrm{tor}}$, then

- $x_0, y_0 \in \mathbb{Z}$.
- Either $y_0 = 0$, i.e. $[2](P) = O$ or y_0^2 divides $4A^3 + 27B^2$.

⌟

Proof: 1: Let P has exact order m. If $m = 2$, then $y_0 = 0$, and then $x_0 \in \mathbb{Z}$ as it is integral over $\mathbb{Z}$. If $m \geq 2$, the results follows from(15.14.3.1).

2: Suppose $[2](P) = (x_1, y_1) \neq O$, then $y_0 \neq 0$, and $x_0, y_0, x_1 \in \mathbb{Z}$. Now(15.11.1.9) shows $x_1 = \varphi(x_0)/4\psi(x_0)$ where

$$\varphi(X) = X^4 - 4AX^2 - 8BX + A^2, \quad \psi(X) = X^3 + AX + B.$$

And they satisfy a polynomial equation

$$f(X)\varphi(X) - g(X)\psi(X) = 4A^2 + 27B^2$$

where $f(X) = 3X^2 + 4A$, $g(X) = 3X^3 - 5AX - 27B$. Then because $y_0^2 = x_0^3 + Ax_0 + B$, we get

$$y_0^2(4f(x_0)x_1 - g(x_0)) = 4A^2 + 27B^2.$$

□

Prop. (15.14.3.4). If $p \in \mathbf{P}$ and $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ has a rational torsion point of order p, then E is isogenous to $E'/\mathbb{Q}$ with a rational point of order p and $\mathbb{Q}(E'[p])$ is a ramified extension of $\mathbb{Q}(\mu_p)$. ⌟

Proof: Cf.[Elliptic Curves, Group Schemes and Mazur's Theorem, P26]?. □

Prop. (15.14.3.5). If $p > 13 \in \mathbf{P}$ and $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ has a rational torsion point of order p, then $\mathbb{Q}(E[p])$ is an unramified extension of $\mathbb{Q}(\mu_p)$. ⌟

Proof: Cf.[Elliptic Curves, Group Schemes and Mazur's Theorem, P29]?. □

Lemma (15.14.3.6) [Mazur-Tate]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ and $p \in \mathbf{P}_{\geq 17} \cup \{11\}$, $E[p] = 0$. ⌟

Proof: Cf.`http://www-personal.umich.edu/~asnowden/teaching/2013/679/index.html`. □

Lemma (15.14.3.7). For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$, $E[13] = 0$. ⌟

Proof: Cf.`http://www-personal.umich.edu/~asnowden/teaching/2013/679/index.html`. □

Lemma (15.14.3.8) [Kubert]. If $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$, then

- E doesn't contain a rational torsion point of exact order N where $N \in \{14, 15, 16, 18, 20, 21, 24, 25, 27, 35, 49\}$.
- $E(\mathbb{Q})_{\mathrm{tor}}$ doesn't contain a subgroup isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(10)$ or $\mathbb{Z}/(2) \times \mathbb{Z}/(12)$.

⌟

Proof: Cf.[Kubert. Universal bounds on the torsion of elliptic curves.]?

Firstly, notice for $N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$, $X_0(N)$ has genus 1(20.2.3.18). And by taking the cusp as the origin, $X_0(N)$ is an elliptic curve. Then Kubert finds that $\mathrm{rank}(X_0(N)) = 0$, and can find all the rational points. Only for $N = 21$ or $N = 27$ there are non-cusp rational points. So it suffices to show that for $X_0(21)$ and $X_0(27)$, the quadratic twists of the elliptic curves corresponding to the rational non-cusp points of $X_0(N)$ don't have rational 21 torsion-points.

For $N = 21$, the non-cusp rational points of $X_0(N)$ are given by quadratic twists of

$$y^2 = x^3 + 45x - 18$$

$$y^2 = x^3 - 75x - 262$$

$$y^2 = x^3 - 1515x - 46106$$

$$y^2 = x^3 - 17235x - 870894.$$

For $N = 27$, the non-cuspidal rational points of $X_0(N)$ are given by quadratic twists of

$$y^2 + y = x^3 - 30x - 5.$$

For the second case, let P be a generator of $\mathbb{Z}/(2)$ and Q a generator of $\mathbb{Z}/(10)$ or $\mathbb{Z}/(12)$, then the dual map $E/P \to E \to E/Q$ is a cyclic isogeny, thus corresponds to a rational point on $Y_0(20)$ or $Y_0(24)$, which in fact has no rational point.

For $N = 16$, ?

For $N = 18$, ?

For $N = 25$, ?

For $N = 35$, let $E = X_0(35)/w_5$, where w_5 is the Atkin-Lehner involution. Then E is an elliptic curve, and $E(\mathbb{Q}) \cong \mathbb{Z}/(3)$. Then Kubert computed that the preimages of these points are cusps. □

Thm. (15.14.3.9) [Mazur]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$, $E(\mathbb{Q})_{\mathrm{tor}}$ can only be isomorphic to one of the following 15 groups:

- $\mathbb{Z}/(n)$ for $n \leq 10$ or $n = 12$, where $n \in \mathbb{Z}_+$.
- $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2n)$ for $n \leq 4$, where $n \in \mathbb{Z}_+$.

Moreover, each of these groups occur, by(15.14.3.11). ⌟

Proof: This follows from(15.14.3.6)(15.14.3.7) and(15.14.3.8). Notice the existence of elliptic curves with these torsion groups can also be shown using modular curves**?**. □

Thm. (15.14.3.10) [Uniform Boundedness of Torsion Groups, Merel]. For any $d \in \mathbb{Z}_+$ there is a constant $N(d)$ s.t. for any number field $F \in \mathtt{NField}$ of degree d and any $E \in \mathcal{E}\mathrm{ll}/F$,

$$\#E(F)_{\mathrm{tor}} \leq N(d).$$

⌟

Proof: **?** □

Prop. (15.14.3.11) [Bounding Torsion Points]. Proposition(15.11.4.19) is useful in controlling torsion points of E. For example: If $E/\mathbb{Q}$ is an elliptic curve with Weierstrass equation

- $E : y^2 + y = x^3 - x + 1$, then $\Delta = -13 \cdot 47$, so E has good reduction modulo 2. But it can be calculated that $\widetilde{E}(\mathbb{F}_2) = \widetilde{O}, E(\mathbb{Q})[2] = O$, thus $E(\mathbb{Q})_{\mathrm{tor}} = O$.
- $E : y^2 = x^3 + 3$, then $\Delta = -2^4 \cdot 3^5$, so E has good reduction modulo p for $p \geq 5$. But it can be calculated that $\#\widetilde{E}(\mathbb{F}_5) = 6, \#\widetilde{E}(\mathbb{F}_7) = 13$, so $E(\mathbb{Q})[p] = O$ for any prime p, and $E(\mathbb{Q})_{\mathrm{tor}} = O$. In particular, $(1, 2) \in E(\mathbb{Q})$ has infinite order.
- $E : y^2 = x^3 + x$, then $\Delta = -2^6$, so E has good reduction modulo p for $p \geq 3$. But it can be calculated that $\widetilde{E}(\mathbb{F}_3) \cong \mathbb{Z}/(4)$, $\widetilde{E}(\mathbb{F}_5) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$, thus $E(\mathbb{Q})_{\mathrm{tor}} \cong 0$ or $\mathbb{Z}/(2)$. The latter case is right, as $(0, 0) \in E(\mathbb{Q})$.
- $E : y^2 = x^3 + 2$.
- $E : y^2 = x^3 + 8$.
- $E : y^2 = x^3 + 4$.
- $E : y^2 = x^3 + 4x$.
- $E : y^2 - y = x^3 - x^2$.
- $E : y^2 = x^3 + 1$.
- $E : y^2 = x^3 - 43x + 166$. then $\Delta = -2^{19} \cdot 13$, thus E has good reduction modulo $3, 5$. But it can be calculated that $\#\widetilde{E}(\mathbb{F}_3) = 7 = \#\widetilde{E}(\mathbb{F}_3)$, thus $E(\mathbb{Q})_{\mathrm{tor}} \cong 0$ or $\mathbb{Z}/(7)$. By(15.14.3.3), for any torsion point (x, y), $y | 2^7$, thus we can find rational points

  $$\{(3, \pm 8), \quad (-5, \pm 16), \quad (11, \pm 32)\}.$$

  And using doubling formula(15.11.1.9) for $P = (3, 8)$,

  $$x([2](P)) = -5, \quad x([4](P)) = 11, \quad x([8](P)) = 3.$$

  Thus P must have order 7, and $E(\mathbb{Q})_{\mathrm{tor}} \cong \mathbb{Z}/(7)$.

- $E : y^2 + 7xy = x^3 + 16x$.
- $E : y^2 + xy + y = x^3 - x^2 - 14x + 29$.
- $E : y^2 + xy = x^3 - 45x + 81$.
- $E : y^2 + 43xy - 210y = x^3 - 210x^2$.
- $E : y^2 = x^3 - 4x$.
- $E : y^2 = x^3 + 2x^2 - 3x$.
- $E : y^2 + 5xy - 6y = x^3 - 3x^2$.
- $E : y^2 + 17xy - 120y = x^3 - 60x^2$.

⌟

Ranks

Conj. (15.14.3.12) [Unboundedness Conjecture]. For $F \in$ `GField`, the rank of elliptic curves over F can take arbitrary large values. ⌟

Proof: □

Remark (15.14.3.13). For function fields, this is proven by Tate-Shafarevich. For $F = \mathbb{Q}$, this is a consequence of the conjecture: for any $k \in \mathbb{Z}_+$, there exists a cube-free integer D s.t. D can be written as a sum of two positive cubes in at least k ways. Cf. [Silverman, Integral Points on Curves of Genus 1]. ⌟

Conj. (15.14.3.14) [Lang]. For any $\varepsilon > 0$, there exists a constant $C_\varepsilon > 0$ s.t. for any $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$, there exists a basis $\{P_1, \ldots, P_r\}$ of the free part of $E(\mathbb{Q})$ satisfying

$$\max_{i \leq i \leq r} \widehat{h}(P_i) \leq C_\varepsilon^{r^2} |D_{E/\mathbb{Q}}|^{\frac{1}{12}+\varepsilon}.$$

where $D_{E/\mathbb{Q}}$ is the minimal discriminant of $E/\mathbb{Q}$ and $\widehat{h}$ is the canonical height. ⌟

Proof: □

Conj. (15.14.3.15) [Rank Distribution]. The distribution of elliptic curves ordered by height(15.11.4.21) satisfies

$$\mathbf{P}_{\text{rank}}(r) = \begin{cases} 0.5 & r = 0 \\ 0.5 & r = 1 \\ 0 & r \geq 2 \end{cases}.$$

In particular, $\mathbb{E}(r) = 0.5$ ⌟

Prop. (15.14.3.16) [Bhargava-Shankar]. $\mathbb{E}(r) \leq 0.99$, if it exists. ⌟

Proof: □

4 Modular Curves

Main references are [Maz78], [Maz76] and [M-T73].

Thm. (15.14.4.1) [Mazur]. Let $p \in \mathbf{P}_{\geq 5}$, and n be the nominator of $\frac{N-1}{12}$, then $J_0(p)(\mathbb{Q})_{\mathrm{tor}}$ is a cyclic group of order n, generated by the class $[(0)-(\infty)]$. ⌟

Proof: Cf.[Maz78]Chap3.1.2.. □

Thm. (15.14.4.2) [Mazur]. Let $N \in \mathbb{Z}_+$ s.t. $g(X_1(N)) > 0$(i.e. $N = 11$ or $N \geq 13$), then $Y_1(N)(\mathbb{Q}) = \varnothing$. ⌟

Proof: Cf.[Maz78]Chap3.5.3. □

Thm. (15.14.4.3) [Mazur]. If $p \in \{11\} \cup \mathbf{P}_{\geq 17}$, then $\# X_{\mathrm{split}}(p)(\mathbb{Q}) < \infty$. ⌟

Proof: Cf.[Maz78]Chap3.6. □

Thm. (15.14.4.4) [Mazur/Momose/Merel]. If $p \in \{11\} \cup \mathbf{P}_{\geq 17}$, then for any $P \in Y_{\mathrm{split}}(p)(\mathbb{Q})$, $j(P) \in \mathbb{Z}$. ⌟

Proof: Cf.[Bilu-Parent]. □

Def. (15.14.4.5) [Modular Units on $X_{\mathrm{split}}(p)$]. As the ⌟

Prop. (15.14.4.6). Situation as in **?**, $\tau \in \mathbf{H}$ s.t. $|q(\tau)| \leq 1/p$, then

- If $p|c$, then
$$\Big|\log|U_c(\tau)| - (p-1)^2 \log|q(\tau)|\Big| \leq 4\pi^2 \frac{p^2}{\log|q(\tau)^{-1}|} + O(p\log p).$$
- If $p \nmid c$, then
$$\Big|\log|U_c(\tau)| + 2(p-1)\log|q(\tau)|\Big| \leq 8\pi^2 \frac{p^2}{\log|q(\tau)^{-1}|} + O(p).$$

⌟

Proof: □

Prop. (15.14.4.7). For any $p \in \mathbf{P}_{\geq 3}$ and $P \in Y_{\mathrm{split}}(\mathbb{C})$,
$$\log|j(P)| \leq 2\pi\sqrt{p} + \max\Big(6\log p, \frac{1}{2(p-1)}\Big|\log|U(P)|\Big| - 6\log p\Big) + O(1).$$

⌟

Proof:

□

Cor. (15.14.4.8). For any $p \in \mathbf{P}$ and $P \in Y_{\mathrm{split}}(p)(\mathbb{Z})$, $0 \leq \log|U(P)| \leq 24p\log p$.

In particular, by(15.14.4.7), there exists constant $C > 0$ s.t. for any $p \in \mathbf{P}$ and $P \in Y_{\mathrm{split}}(p)(\mathbb{Z})$, $\log|j(P)| \leq 2\pi p^{1/2} + 6\log p + C$. ⌟

Proof: □

Prop. (15.14.4.9). There exists an effective constant $\kappa > 0$ s.t. for any $p \in \mathbf{P}$ and an elliptic curve $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ without CM and endowed with a structure of normalizer of split Cartan subgroup in level p, then $h^+(j(E)) \geq \kappa p$. ⌟

Proof: For such an elliptic curve E with two p-isogenies $\varphi_1 : E \to E_1, \varphi_2 : E \to E_2$. Then $\varphi = \varphi_1^\vee \circ \varphi_2 : E_1 \to E_2$ is a cyclic p^2-isogeny. Then it follows from(15.13.2.2) that $h^+(j(E)) \geq \kappa_1 p$ for some constant κ_1 independent of p and E.

(15.13.3.5) shows that $h_{\mathrm{st}}(E_1) \leq h_{\mathrm{st}}(E) + \frac{1}{2}\log p$, and(15.13.3.12) shows that for any $X \in \mathcal{E}\mathrm{ll}/F$,

$$|h^+(j(X)) - 12h_{\mathrm{st}}(X/F)| \leq 6\log(1 + h^+(j(X))) + O(1).$$

Thus the assertion follows. □

Thm. (15.14.4.10) [Bilu-Parent/Bilu−Parent−Rebolledo/Balakrishnan-Dogra-Müller-Tuitman-Vonk]. For $p \in \mathbf{P}$, every point in $X_{\mathrm{split}}(p)(\mathbb{Q})$ is either a CM point or a cusp iff $p > 7$. ⌟

Proof: Firstly it follows from(15.14.4.4)(15.14.4.8) and(15.14.4.9) that this hols for p large. Then**?**
□

Lemma (15.14.4.11). $X_{\mathrm{split}}(13)(\mathbb{Q})$ consists of 6 CM-points and one cusp. Moreover, $X_{\mathrm{nonsplit}}(13)(\mathbb{Q})$ consists of 7 CM-points. ⌟

Proof: □

Conclusions

Prop. (15.14.4.12)[Rational Points of Modular Curves]. Situation as in(19.3.4.1), if $g(X_H(p)) > 0$, and $X_H(p)$ is defined over $\mathbb{Q}$, then

- $X_H(p) = X_0(p)$ has only f.m. $\mathbb{Q}$-points, and they can be calculated.
- $X_H(p) = X_{\mathrm{split}}(p)$ has only f.m. $\mathbb{Q}$-points for $p \neq 13$.
- For $X_H(p) = X_{\mathrm{nonsplit}}(p)$, nothing is known.**?**
- $X_H(p) = X_{S_4}(p)$ has no rational points for $p > 13$.

⌟

Proof: □

5 Effective Bounds on Rational Curves(Chabauty)

The idea is: By the embedding $X \to J(X)$, to calculate $X(\mathbb{Q})$, calculate $J(X)(\mathbb{Q})$ first, then determine which points are in $X(\mathbb{Q})$.

Coleman Integration

Prop. (15.14.5.1) [Coleman Integration]. For $J \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/\mathbb{Q}_p$, there is a **Coleman integration map**:

$$J(\mathbb{Q}_p) \times H^0(J/\mathbb{Q}_p, \Omega^1) \to \mathbb{Q}_p : (Q, \omega) \mapsto \int_0^Q \omega.$$

s.t. on an open subset $U \subset J$, the integration can be calculated locally by writing ω in power series. ⌟

Chabauty-Kim Method

Thm. (15.14.5.2) [Chabauty-Coleman]. Let $X \in \mathcal{C}ur^g/\mathbb{Q}$, and $p \in \mathbf{P}$ a good reduction of X. Suppose $r' < g$(e.g. $r < g$)**?**, then

-
- If $p > 2g$, then $\#X(\mathbb{Q}) \leq \#X(\mathbb{F}_p) + 2r' \leq \#X(\mathbb{F}_p) + (2g - 2)$.

⌟

6 Finite Fields

Prop. (15.14.6.1) [Esnault]. Let $p \in \mathbf{P}, q \in p^{\mathbb{Z}}, X \in \mathcal{S}m\mathcal{P}roj\mathcal{V}ar/\mathbb{F}_q$ s.t. $\mathrm{CH}_0(X_{\overline{R(X)}}) = \mathbb{Z}$, then $\#X(\mathbb{F}_q) \equiv 1 (\mathrm{mod}\ q)$. In particular, X has a rational point. ⌟

Proof: Cf.[Weil 1 Proof]. □

Cor. (15.14.6.2). Any rationally chain connected varieties over a finite field $k = \mathbb{F}_q$ s.t. $\mathrm{CH}_0(X_{\overline{R(X)}}) = \mathbb{Z}$, then $X(K) \equiv 1 \mod q$. In particular, X has a rational point. ⌟

Cor. (15.14.6.3)[Manin-Lang]. If $X/\mathbb{F}_q$ is a smooth projective Fano variety, then $X(\mathbb{F}_q) \equiv 1 \mod q$. ⌟

Proof: This is because by(6.11.4.4), any Fano variety is rationally chain connected. □

7 Vojta's Conjecture

8 Bombieri-Lang Conjecture

Conj. (15.14.8.1) [Bombieri-Lang]. Let $F \in \mathtt{NField}$ and X is a variety over F of general type(i.e. with maximal Kodaira dimension(6.11.3.5)), then there are f.m. subvarieties $X_i \subset X$ of lower dimensions s.t. $X(F) = \cup_i X_i(F)$. ⌟

Proof: □

Thm. (15.14.8.2) [Mordell Conjecture, Faltings]. By(15.13.5.9), for $F \in \mathtt{NField}$ and C/F be a complete non-singular curve of genus $g \geq 2$, then $\#C(F) < \infty$. ⌟

9 Uniform-Boundedness

Conj.Cor. (15.14.9.1) [Uniform-Boundedness for Torsion Points of Abelian Varieties]. The Morton-Silverman boundedness conjecture(15.17.4.1) implies that for any $D, g \in \mathbb{Z}_+$, there exists $\eta(D, g) \in \mathbb{Z}_+$ s.t. for any $F \in \mathtt{NField}$ with $[F : \mathbb{Q}] = D$ and $A \in \mathcal{A}b\mathcal{V}ar/F$, $\#A(F)_{\mathrm{tor}} \leq \eta(D, g)$. ⌟

Proof: Cf.[Fak03]P3.**?** □

10 Hilbert's 10-th Problem

Conj. (15.14.10.1)[Hilbert's 10-th Problem]. Let $F \in \mathtt{NField}$, X be a projective scheme over $\mathcal{O}_K$, it there an algorithm to determine in a finite number of operations whether $X(K) = \varnothing$. ⌟

Proof: □

Remark (15.14.10.2) [Mazur-Rubin]. If the BSD conjecture holds for all elliptic curves over any number fields, then Hilbert's 10-th problem has a negative answer for any number field. ⌟

Proof:

□

15.15 Tate Conjecture & Hodge Conjecture

Main references are [Tat91], [Tat65b], [RECENT PROGRESS ON THE TATE CONJECTURE, Totaro] and [Tate Conjecture over Finite Fields, Milne].

1 Statements

Prop. (15.15.1.1) [ℓ-adic Cycle Classes]. Let $k \in \texttt{Field}$ and $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}\mathcal{V}\mathrm{ar}/k$, $\overline{X} = X \otimes_k k^s$, $\ell \in \mathbf{P} \setminus \operatorname{char} k$, then there exists a cycle map

$$c^r : \mathrm{CH}^r(\overline{X}) \to \mathrm{H}^{2r}_{\text{ét}}(\overline{X}, \mathbb{Q}_\ell(r)),$$

as étale cohomology is a Weil cohomology theory**?**. Let $A^r_{\text{ét},\ell}(\overline{X})$ be the image, and $A^r_{\text{ét},\ell}(X)$ be the image of $\mathrm{CH}^r(X) \subset \mathrm{CH}^r(\overline{X})$ under this map. Then there are maps

$$A^r_{\text{ét},\ell}(\overline{X}) \otimes \mathbb{Q}_\ell \subset H^{2r}(\overline{X}, \mathbb{Q}_\ell(r)), \quad A^r_{\text{ét},\ell}(X) \otimes \mathbb{Q}_\ell \subset H^{2r}(\overline{X}, \mathbb{Q}_\ell(r))^{\mathrm{Gal}_k}.$$

⌟

Conj. (15.15.1.2) [Tate]. Situation as in(15.15.1.1), if k is f.g. over its prime field, then
$(T^r(X/k), \ell)$**:** $A^r_{\text{ét},\ell}(X) \otimes \mathbb{Q}_\ell = H^{2r}(\overline{X}, \mathbb{Q}_\ell(r))^{\mathrm{Gal}_k}$.
$(E^r(X/k), \ell)$**:** $A^r_{\text{ét},\ell}(\overline{X}) \cong GH^r(\overline{X})$. In particular, $A^r_{\text{ét},\ell}(\overline{X})$ doesn't depend on ℓ.
$(S^r(X/k), \ell)$**:** Fr_X acts semisimply on the 1-eigenpart $\mathrm{H}^{2r}_{\text{ét}}(X, \mathbb{Q}_\ell(r))_1$.

⌟

Proof: □

Conj. (15.15.1.3) [Integral Tate Conjecture]. Situation as in(15.15.1.1), if k is f.g. over its prime field, then we may ask if

$$A^r_{\text{ét},\ell}(X) \otimes \mathbb{Z}_\ell = H^{2r}(\overline{X}, \mathbb{Z}_\ell(r))^{\mathrm{Gal}_k}.$$

Cf.[Tate Conjecture, Milne, P3]. ⌟

Prop. (15.15.1.4) [(E^1) Holds]. The Kummer exact sequence of étale sheaves on $\overline{X}$: $0 \to \mu_{\ell^n} \to \mathbb{G}_m \xrightarrow{\ell^n} \mathbb{G}_m \to 0$ induces an injection $\mathrm{Pic}(\overline{X})/\ell^n \mathrm{Pic}(\overline{X}) \hookrightarrow H^2(\overline{X}, \mu_{\ell^n})$. Taking limits gives an injection $\mathrm{Pic}(\overline{X}) \otimes \mathbb{Q}_\ell \hookrightarrow H^2(\overline{X}, \mathbb{Q}_\ell(1))$. And c^1 is just

$$c^1 : Z^1(\overline{X}) \to \mathrm{Pic}(\overline{X}) \to \mathrm{Pic}(\overline{X}) \otimes \mathbb{Q}_\ell \hookrightarrow \mathrm{H}^2_{\text{ét}}(\overline{X}, \mathbb{Q}_\ell(1)).$$

Thus the kernel of c^1 is just the $\mathrm{Pic}(X)$ modulo ℓ^∞-divisible elements and torsion elements, but $\mathrm{Pic}^0(\overline{X})$ is ℓ^∞-divisible as it is the k^s-points of an Abelian variety over k^s. And also $\mathrm{Pic}(\overline{X})/\mathrm{Pic}_{\mathrm{num}=0}(\overline{X}) \to \mathrm{Pic}(X_{\overline{k}})/\mathrm{Pic}^\tau(X_{\overline{k}}) = N^1(X_{\overline{k}})$ is injective by[Sta]0CC5**?**, and $N^1(X_{\overline{k}})$ is finite free, so $\mathrm{Pic}_{\mathrm{num}=0}(\overline{X}) = \mathrm{Pic}(\overline{X})_{\mathrm{tor}}$, and $A^1_{\text{ét},\ell}(\overline{X}) = GH^1(X)$. ⌟

Remark (15.15.1.5) [Hodge & Tate Conjecture]. In characteristic 0, we can embed k into $\mathbb{C}$ and use étale-singular comparison to see the Hodge conjecture implies the Tate conjecture.**?** ⌟

Prop. (15.15.1.6). Situation as in(15.15.1.2), let $X, Y \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}\mathcal{V}\mathrm{ar}/k$, then $(T^1(X \times_k Y)) \iff (T^1(X)) + (T^1(Y))$. ⌟

Proof:

□

Prop. (15.15.1.7). Situation as in(15.15.1.2), let $f : X \to Y \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}\mathcal{V}\mathrm{ar}/k$ be a dominant rational map, then $(T^1(X/k)) \Rightarrow (T^1(Y/k))$. ⌟

Proof:

□

Cor. (15.15.1.8). The Fermat curve $S_n : z_0^n + z_1^n + z_2^n + z_3^n = 0$ is dominated by the product of two curves

$$C_1 : x_0^n + x_1^n = x_2^n, \quad C_2 : y_0^n + y_1^n = -y_2^n$$

by

$$C_1 \times C_2 \to S : ([x_0, x_1, x_2], [y_0, y_1, y_2]) \mapsto [x_0y_2, x_1y_2, y_0x_2, y_1x_2],$$

so $(T^1(S_n))$ holds. ⌟

2 over Finite Fields

Main references are [Milne, Tate Conjecture over Finite Fields], and [Endomorphisms of abelian varieties over finite fields, Tate, 1966].

Prop. (15.15.2.1) [(T^1)]. Let $\#k < \infty$ and $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}\mathcal{V}\mathrm{ar}/k$, Tate proved that $H^{2r}(\overline{X}, \mathbb{Q}_\ell(r))^{\mathrm{Gal}_k} \cong \mathrm{H}^{2r}_{\text{ét}}(X, \mathbb{Q}_\ell(r))$, and the Kummer sequence gives an exact sequence**?** ⌟

Proof: □

Connection with B-S.D

Prop. (15.15.2.2) [Tate]. Let $\#k < \infty, X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}\mathcal{V}\mathrm{ar}/k$, then $(T^r(X/k))$ and $(E^r(X/k))$ hold iff

$$\mathrm{ord}_{s=r}(Z(X, s)) = -\operatorname{rank} GH^r(X).$$

⌟

Proof: □

Prop. (15.15.2.3) [(T^1) and BSD]. Let $\#k < \infty$ and C a smooth complete curve over k with function field K, $\mathcal{E}/C$ is a regular elliptic surface with generic fiber $E \in \mathcal{E}\mathrm{ll}/K$, then $(T^1(\mathcal{E}/k))$ is equivalent to the BSD conjecture for E/K. ⌟

Proof: □

Prop. (15.15.2.4) [Grothendieck]. Let $\#k < \infty$ and C a smooth complete curve over k with function field K, $\mathcal{E}/C$ is a regular elliptic surface with generic fiber $E \in \mathcal{E}\mathrm{ll}/K$, then

$$\mathrm{Br}(\mathcal{E}/k) \cong Ш(E/K).$$

$\acute{k}$ ⌟

Proof: Cf.[Grothendieck, Alexander, Le groupe de Brauer. III. 1968]. □

3 K3 Surfaces

Main references are [The Tate Conjecture For K3 Surfaces In Odd Characteristic, Pera], [The Tate Conjecture For K3 Surfaces—A Survey Of Some Recent Progress], [2-adic integral canonical models and the Tate conjecture in characteristic 2].

Thm. (15.15.3.1) [Charles, Pera]. $(T^1(X))$ holds if X is a K3 surface. ⌟

Proof: Cf.[The Tate Conjecture For K3 Surfaces In Odd Characteristic, Pera] and [2-adic integral canonical models and the Tate conjecture in characteristic 2].? □

Cor. (15.15.3.2) [Lieblich-Maulik-Snowden]. There are only finitely many isomorphism classes of K3 surfaces over a finite field of characteristic ≥ 5. ⌟

Proof: [Finiteness of K3 surfaces and the Tate conjecture, Lieblich-Maulik-Snowden]. □

Kuga-Satake construction

4 Hodge Conjecture

Main references are [Hodge cycles on abelian varieties, Deligne].

Def. (15.15.4.1) [Hodge Classes]. For $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/\mathbb{C}$, define $\mathrm{Hdg}^{2k}(X) = H^{2k}_{\mathrm{Betti}}(X, \mathbb{Q}) \cap H^{k,k}_{\mathrm{Betti}}(X)$, called the **Hodge classes** of X of degree $2k$. ⌟

Prop. (15.15.4.2). If $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/\mathbb{C}$ and $Z \subset Z^r(X)$, then $[Z] \subset \mathrm{Hdg}^k(X)$. ⌟

Proof: ?? □

Conj. (15.15.4.3) [Hodge]. For $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/\mathbb{C}$, every Hodge class is algebraic. ⌟

Proof: □

Arithmetic Theory

Thm. (15.15.4.4) [Deligne]. Let $k \in \mathtt{Field}^0, k = \overline{k}$, $X \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}/k$, and let $t \in H^{2p}_{\mathbb{A}}(X)(p)$. Then if t is a Hodge cycle w.r.t. one embedding $\sigma : k \to \mathbb{C}$, then it is absolutely Hodge. ⌟

Proof: □

Def. (15.15.4.5) [Hodge Classes]. Let $k \in \mathtt{Field}^0, k = \overline{k}$, and $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/k$, then for any embedding $\sigma : k \hookrightarrow \mathbb{C}$, $H^n_{\mathrm{dR}}(X/k)$ satisfies

$$H^n_{\mathrm{dR}}(X/k) \otimes_{k,\sigma} \mathbb{C} \cong H^n_{\mathrm{dR}}(X, \mathbb{C}) \cong H^n_{\mathrm{Betti}}(X, \mathbb{C}).??$$

Thus we can define the space $\mathrm{Hdg}^{2k}(X)$ of **Hodge cycle** on X of degree $2k$ w.r.t. σ as the subspace of elements in $H^{2k}_{\mathrm{dR}}(X/k)$ that are mapped to $(2\pi\,\mathrm{i})^k$ times a Hodge class of σX of degree $2k$(15.15.4.1).

This notion is independent of the embedding σ. ⌟

Proof: ? □

15.16 Schemes over $\mathbb{F}_1$

References are [Connes, Schemes over $\mathbb{F}_1$ and Zeta-Functions], [Sou04].

1 Geometry of Monoids

Cf.[Toric Singularities, Kato].

Notation (15.16.1.1).
- In this section, monoids are assumed to be commutative and have a zero element and neutral element.

⌟

Def. (15.16.1.2) [Ideals in Monoids]. For $M \in \mathcal{CM}\mathrm{on}^{0,1}$, an **ideal(of monoids)** of M is a subset $I \subset M$ s.t.
- $0 \in I$.
- $x \in I, y \in M \implies xy \in I$.

And a **prime ideal(of monoids)** of M is an ideal $\mathfrak{p} \subset M$ s.t. $M \setminus \mathfrak{p}$ is a multiplicative subset of M. ⌟

Def. (15.16.1.3) [Spectrum of Monoids]. For $M \in \mathcal{CM}\mathrm{on}^{0,1}$ and $I \in \mathrm{Ideal}(M)$, let $D(I)$ be the the set of primes ideals of M not containing I. Then if $\mathrm{Spec}(M)$ is the set of prime ideals of M, $D(I)$ defines a the Zariski topology on $\mathrm{Spec}(M)$. ⌟

Prop. (15.16.1.4) [Abelian Groups and Monoids]. For $H \in \mathcal{A}\mathrm{b}$, denote $\mathbb{F}_1[H] = H \cup \{0\} \in \mathcal{CM}\mathrm{on}^{0,1}$. Then this defines $\mathcal{A}\mathrm{b}$ as a full subcategory of $\mathcal{CM}\mathrm{on}^{0,1}$, and the inclusion is left adjoint to taking invertible elements: For any $H \in \mathcal{A}\mathrm{b}, M \in \mathcal{CM}\mathrm{on}^{0,1}$,

$$\mathrm{Hom}_{\mathcal{CM}\mathrm{on}^{0,1}}(\mathbb{F}_1[H], M) = \mathrm{Hom}_{\mathcal{A}\mathrm{b}}(H, M^\times).$$

⌟

Mon-Functors

$\mathbb{F}_1$-Schemes

Def. (15.16.1.5) [$\mathbb{F}_1$-Schemes]. An **$\mathbb{F}_1$-scheme** is a topological space with a sheaf of monoids that is locally isomorphic to the spectrum of a commutative monoids. The category of $\mathbb{F}_1$-schemes is denoted by $\mathcal{S}\mathrm{ch}\,/\mathbb{F}_1$. ⌟

Def. (15.16.1.6). An **finitely generated $\mathbb{F}_1$-scheme** is a scheme that has a finite cover by affine schemes $U_i = \mathrm{Spec}\, A_i$ s.t. each A_i are f.g. monoids. ⌟

Def. (15.16.1.7) [Ascend Functor]. The functor $\mathcal{CM}\mathrm{on}^{0,1} \to \mathcal{CR}\mathrm{ing} : A \mapsto \mathbb{Z}[A]$ defines a functor

$$- \otimes \mathbb{Z} : \mathcal{S}\mathrm{ch}\,/\mathbb{F}_1 \to \mathcal{S}\mathrm{ch}\,.$$

⌟

Prop. (15.16.1.8). For $X \in \mathcal{S}\mathrm{ch}\,/\mathbb{F}_1$, X is f.g. iff $X_{\mathbb{Z}}$ is finitely generated. ⌟

Proof: ? □

Def. (15.16.1.9) [Ring Monoids]. For $R \in \mathcal{CR}\text{ing}$, define $\operatorname{Spec} R \in \mathcal{S}\text{ch}/\mathbb{F}_1$ to be the affine scheme corresponding to the multiplicative monoid $(R, \times)$.

Then we have $\operatorname{Hom}_{\mathbb{F}_1}(\operatorname{Spec} R, X) = \operatorname{Hom}_{\mathcal{S}\text{ch}}(\operatorname{Spec} R, X_{\mathbb{Z}})$ for any $X \in \mathcal{S}\text{ch}/\mathbb{F}_1$. ⌟

Prop. (15.16.1.10)[Zeta Polynomials]. For any $X \in \mathcal{S}\text{ch}^{\text{fg}}/\mathbb{F}_1$, there exists $e \in \mathbb{Z}_+$ and $N(T) \in \mathbb{Z}[T]$ s.t. for any $p \in \texttt{Prime}, q \in p^{\mathbb{Z}_+}$, if $(q-1, e) = 1$, then

$$\#X(\mathbb{F}_q) = N(q).$$

Such N is called the **zeta polynomial** of X. ⌟

Proof: This is quite easy, Cf.[Remarks on zeta functions and K-theory over F1, Dietmar]. □

Def. (15.16.1.11)[Zeta Functions of $\mathbb{F}_1$-Schemes]. For $X \in \mathcal{S}\text{ch}^{\text{fg}}/\mathbb{F}_1$, if $N_X(T) = a_0 + a_1 T + \ldots + a_n T^n$ is the zeta polynomial of X(15.16.1.10), then the **zeta function($\mathbb{F}_1$)** of X is defined to be

$$\zeta_X(s) = \lim_{q \to 1} Z_q(X, q^{-s})(q-1)^{N(1)} = s^{a_0}(s-1)^{a_1} \ldots (s-n)^{-a_n}.$$

And the **Euler characteristic($\mathbb{F}_1$)** of X is defined to be

$$\chi(X) = N_X(1) = \sum a_i.$$

⌟

Prop. (15.16.1.12). This zeta function so defined(15.16.1.11) fulfills the requirement of the motivic zeta function as in [Manin, Zeta functions].? ⌟

Prop. (15.16.1.13). Let $\underline{X}$ be a Mon-scheme and X its geometric realization, then the restriction of $\underline{X}$ to $\mathcal{A}\text{b}$ via $\mathbb{F}_1$ is:

$$\underline{X}(\mathbb{F}_1[H]) = \coprod_{x \in X} \operatorname{Hom}_{\mathcal{A}\text{b}}(\mathcal{O}_{X,x}^{\times}, H), \quad H \in \mathcal{A}\text{b}.$$

⌟

2 Zeta Functions

Conj. (15.16.2.1). For any $n \in \mathbb{Z}_+$, there should be a field $\mathbb{F}_{1^n}$, s.t.

- $\operatorname{Spec} Z$ is over $\mathbb{F}_1$, and
- $\mathbb{F}_{1^n} \otimes_{\mathbb{F}_1} \mathbb{Z} = \mathbb{Z}[T]/(T^n - 1)$.

⌟

Proof: □

Conj. (15.16.2.2). There exists a "curve" $C = \overline{\operatorname{Spec} \mathbb{Z}}$ over $\mathbb{F}_1$ whose zeta-function is $Z_C(s) = \Lambda(s)$. ⌟

Proof: □

Prop. (15.16.2.3). One expects $\overline{\operatorname{Spec} Z}$ to be of infinite genus. ⌟

Proof: [Manin, Zeta Functions and Motives]. □

3 Absolute Motives via Zeta Functions

Remark (15.16.3.1) [Absence of Absolute Motives]. Because of the absence of direct products of $\mathbb{Z}$-schemes, we cannot use correspondence to define morphisms between absolute motives. As a result, we can only observe them through the zeta function, and observe the imaginary morphisms between by their induced morphisms on zeta functions. ⌟

4 K-Theory of $\mathbb{F}_1$-Schemes

Def. (15.16.4.1) [$K_n^+(A)$]. For $A \in \mathcal{CM}\mathrm{on}$, define $\mathrm{GL}(n; A)$ to be the set of group of $n \times n$ matrices s.t. each row and column has exactly one non-zero element which lies in $A^\times$. Then $\mathrm{GL}(n; A) \cong A^\times \rtimes \mathrm{Sym}_n$, and there are natural embeddings $\mathrm{GL}(n; A) \hookrightarrow \mathrm{GL}(n+1; A)$.

Then we can define $\mathrm{GL}(A) = \varinjlim_n \mathrm{GL}(n; A)$, and define the **K-group of monoids** as $K_j^+(A) = \pi_j(\mathrm{BGL}(A)^+)$, where $+$ is the Quillen's plus construction. ⌟

Cor. (15.16.4.2). $K_j(\mathbb{F}_1) = \pi_j^{\mathrm{st}}(\mathbb{S})$. ⌟

Proof: **?** □

Def. (15.16.4.3) [$K_n^Q(A)$]. For $A \in \mathcal{CM}\mathrm{on}$, let $\mathcal{P}$ be the category of f.g. pointed projective A-modules, and $\mathcal{E}$ be the class of split exact sequences in $\mathcal{P}$, then $(\mathcal{P}, \mathcal{E})$ is a quasi-exact category, and we can define the **K-group of monoids** as $K_i^Q(A) = K_i(\mathcal{P}, \mathcal{E})$(10.1.2.5). ⌟

Prop. (15.16.4.4). For $A \in \mathcal{A}\mathrm{b}$, $K_n^+(A) = K_n^Q(A)$(15.16.4.1)(15.16.4.3) for any $n \in \mathbb{N}$.

In particular,

$$K_i^+(A) = K_i(A^\times) = \begin{cases} Z \times A^\times & , i = 0 \\ \pi_i^{\mathrm{st}}(\mathbb{S}) & , i > 0 \end{cases}.$$

And there are maps $K_i^+(A) = K_i(A^\times) \to K_i^Q(A)$. ⌟

Proof: Any projective pointed A-module is free**?**, so the usual proof for $A \in \mathcal{CR}\mathrm{ing}$ pass through(**?**Cf. Higher K-theory, 2).

And then $\mathcal{P}$ is just the product of the category of pointed sets and $\{A\}$. Thus $\mathbb{B}Q(\mathcal{P}) = \mathbb{B}Q(\mathcal{S}\mathrm{et}_{\mathrm{pt}}) \times \mathbb{B}A$, and the assertion follows.

The map $K_i(A^\times) \to K_i^Q(A)$ comes from the fact any projective $A^\times$-modules are free. □

15.17 Arithmetic Dynamical Systems

References are [Sil07] and [Fak03].

Def. (15.17.0.1) [Rational Maps]. A map $\varphi : \mathbb{P}^N \to \mathbb{P}^M$ is called a **rational map of degree** d if ⌟

Prop. (15.17.0.2) [Fakhruddin's Trick]. Let $k \in \texttt{Field}, \#k = \infty$, X a projective variety over k, $\varphi : X \to X$ a morphism, $\mathcal{L} \in \mathrm{Pic}(X)$ a very ample line bundle and $d \in \mathbb{Z}_+$ s.t. $\varphi^*(\mathcal{L}) \cong \mathcal{L}^{\otimes d}$, then there exists $N \in \mathbb{Z}_+$ and an embedding $\iota : X \to \mathbb{P}^N_k$ with a morphism $\psi : P^N_k \to P^N_k$ s.t. $\psi \circ \iota = \iota \circ \psi$. ⌟

Proof: Cf.[Fak03]P2. □

Thm. (15.17.0.3). For $k \in \texttt{Field}, k = \overline{k}$, $A \in \mathcal{A}b\mathcal{V}ar/k$ with a group G acting freely, then $X = A/G$ has a line bundle $\mathcal{L}$ and a morphism $\varphi : X \to X$ s.t. $\varphi^*(\mathcal{L}) \cong \mathcal{L}^{\otimes d}$ for some $d \in \mathbb{Z}_{\geq 2}$. And if $\mathrm{char}\, k = 0$, then for any $X \in \mathcal{S}m\mathcal{P}roj/k$ with $\mathrm{Kod}(X) \geq 0$ and a line bundle $\mathcal{L}$ and a morphism $\varphi : X \to X$ s.t. $\varphi^*(\mathcal{L}) \cong \mathcal{L}^{\otimes d}$ for some $d \in \mathbb{Z}_{\geq 2}$ is of the form $X = A/G$ for $A \in \mathcal{A}b\mathcal{V}ar/k$ with a group G acting freely. ⌟

Proof: Cf.[Fak03]P8. □

1 over Finite Fields

2 over Local Fields

3 over Global Fields

Heights

Canonical Heights

Def. (15.17.3.1) [Quasi-Homogenous Functions]. Let $N \subset \mathbb{R}$ be a multiplicatively-closed subset of $\mathbb{R}$ acting on a set $S \in \mathcal{S}et$. Then a function $h : S \to \mathbb{R}$ is called a **quasi-homogenous function** of degree $d \in \mathbb{R}_+$ iff for any $n \in N$, there exists $C(n) \in \mathbb{R}_+$ s.t.

$$|h(nx) - n^d h(x)| \leq C(n), \forall x \in S.$$

⌟

Prop. (15.17.3.2) [Tate's Limiting Argument]. Situation as in(15.17.3.1), there exists a unique homogenous function $\widehat{h} : S \to \mathbb{R}$ of degree d s.t. $\widehat{h} - h$ is bounded, which is given by

$$\widehat{h}(x) = \lim_{|n| \to \infty} \frac{h(nx)}{n^d}.$$

⌟

Proof: Cf.[B-G06]P285. □

Prop. (15.17.3.3). For $F \in \texttt{NField}$ and $f : \mathbb{P}^1_F \to \mathbb{P}^1_F$ of degree> 1, then the canonical height

$$\widehat{h}_f : \alpha \mapsto \lim_{n \to \infty} \frac{h(f^{(n)}(\alpha))}{d^n}$$

is the unique function s.t. $\widehat{h}_f \circ f = d\widehat{h}_f$, and $\widehat{h}_f \sim h$. ⌟

Prop. (15.17.3.4). For $F \in \texttt{NField}, E \in \mathcal{E}ll/F$ and $f = \varphi_{E,2}$, $\widehat{h}_f(\mathrm{pr}(P)) = 2\widehat{h}_E(P)$ for any $P \in E(F)$. ⌟

4 Uniform-Boundeness

Conj. (15.17.4.1) [Uniform-Boundedness Conjecture, Morton-Silverman]. For $D, N, d \in \mathbb{Z}_+$ and $d \geq 3$, there exists $\kappa(D, N, d) \in \mathbb{Z}_+$ s.t. for any $F \in \texttt{NField}$ with $[F : \mathbb{Q}] = D$ and each morphism $\psi : \mathbb{P}^N_F \to \mathbb{P}^N_F$ defined by homogenous polynomials of degree d, $\# \operatorname{PrePer}(\psi; F) \leq \kappa(D, N, d)$. ⌟

Proof: □

Remark (15.17.4.2). By[Fak03]P4, by restriction of scalars, it suffice to consider the case $F = \mathbb{Q}$. ⌟

Conj. (15.17.4.3). For $F \in \texttt{NField}$ and $N \in \mathbb{Z}_+, d \in \mathbb{Z}_{\geq 2}$, there exists a finite set $S(d, N, F) \subset \mathbb{P}^N(F)$ s.t. for any morphism $f : \mathbb{P}^N_F \to \mathbb{P}^N_F$ defined by homogenous polynomials of degree d, $S(d, N, F) \nsubseteq f(\mathbb{P}^N(F))$. ⌟

Proof: □

Prop. (15.17.4.4). This conjecture is a consequence of the Bombieri-Lang conjecture(15.14.8.1), by[Fak03]P4. ⌟

Proof: □

5 Arithmetic Dynamical Mordell-Lang Conjecture

References are [Poo14].

Prop. (15.17.5.1)[p-adic Interpolation of Iterates, Poonen]. Let K be a valued field s.t. $|p| = 1/p$, and $f \in \mathcal{O}_K\langle X_1, \ldots, X_d\rangle^d$ satisfies $f(\underline{X}) \equiv \underline{X} (\operatorname{mod}\ p^c)$ for some $c > 1/(p-1)$. Then there exists $g \in \mathcal{O}_K\langle X_1, \ldots, X_d, T\rangle$ s.t. $g(\underline{X}, n) = f^{\circ n}(n) \in \mathcal{O}_K\langle \underline{X}\rangle^d$ for any $n \in \mathbb{N}$. Moreover, $g(\underline{X}, T+1) = f(g(\underline{X}, T))$ holds. ⌟

Proof: The hypothesis implies that $h(f(\underline{X})) \equiv f(\underline{X}) (\operatorname{mod}\ p^c)$ for any $h(\underline{X}) \in \mathcal{O}_K[\underline{X}]^d$, and by taking limits this is also true for any $h \in \mathcal{O}_K\langle \underline{X}\rangle^d$. Thus if we define the linear operator

$$\Delta(h)(\underline{X}) = h(f(\underline{X})) - f(\underline{X}),$$

then for any $m \in \mathbb{N}$, Δ^m maps $\mathcal{O}_K\langle \underline{X}\rangle^d$ into $p^{mc}\mathcal{O}_K\langle \underline{X}\rangle^d$. Then because $|m!| > p^{-m/(p-1)}$(2.6.3.28), so the Mahler series

$$g(\underline{X}, T) = \sum_{m \in \mathbb{N}} \binom{T}{m} \Delta^m(\underline{X})$$

converges in $\mathcal{O}_K\langle \underline{X}\rangle^d$. And

$$g(\underline{X}, n) = \sum_{m=0}^{n} \binom{n}{m} \Delta^n(\underline{X}) = (\Delta + \mathrm{id})^n(\underline{X}) = f^{\circ n}(\underline{X}).$$

For the last assertion, the equation clearly holds for $T \in \mathbb{N}$, so by comparing coefficients, it holds for any T. □

6 Dynamics Associated to Algebraic Groups

Power Maps

Chebyshev Maps

Lattès Maps

References are [On Lattès Maps, Milnor].

Def. (15.17.6.1)[Lattès Maps]. A rational function $f : \mathbb{P}^1 \to \mathbb{P}^1$ is called a **Latte map** if there exists $E \in \mathcal{E}\mathrm{ll}/\mathbb{C}$ s.t. it is a quotient of an endomorphism $\varphi \in \mathrm{End}(E)$ through a finite map $\mathrm{pr} : E \to \mathbb{P}^1$. ⌟

Prop. (15.17.6.2). For any Lattès map $f : \mathbb{P}^1 \to \mathbb{P}^1$ corresponding to an endomorphism $\varphi \in \mathrm{End}(E)$ of degree≥ 2?, $\mathrm{Jul}(f) = \mathbb{P}^1(\mathbb{C})$. ⌟

Proof: This is because the Julia set is the closure of repelling periodic points, and the set of periods of $E \in \mathcal{E}\mathrm{ll}/\mathbb{C}$ are dense and it is expanding everywhere. □

7 Equidistributions

15.18 Arithmetic Topology

Main references are [Knots and Primes, an Introduction to Arithmetic Topology, Masanori-Morishita], [Knots and Primes, Chao Li], [Kapranov, M.: Analogies between number fields and 3-manifolds. Unpublished Note (1996)], [Kapranov, M.: Analogies between the Langlands correspondence and topological quan- tum field theory. In: Progress in Math., vol. 131, pp. 119–151. Birkhäuser, Basel (1995)], [Manin, Y., Marcolli, M.: Holography principle and arithmetic of algebraic curves. Adv. Theor. Math. Phys. 5(3), 617–650 (2001)], [Reznikov, A.: Three-manifolds class field theory (Homology of coverings for a nonvir- tually b1-positive manifold). Sel. Math. New Ser. 3, 361–399 (1997)], [Reznikov, A.: Embedded incompressible surfaces and homology of ramified coverings of three-manifolds. Sel. Math. New Ser. 6, 1–39 (2000)].

1 Knots and Primes

16 Arakelov Geometry

16.1 Arithmetic Intersection Theory

1 Arithmetic Intersection

References are [Points of small height on semiabelian varieties, Kuhne].

2 Arithmetic Riemann-Roch

16.2 Arakelov Geometry

1 Metrized Line Bundles

Def. (16.2.1.1)[Metrized Line Bundles]. Let F be a number field, a **metrized line bundle** $(\mathcal{L}, |\cdot|)$ is a line bundle on $\mathcal{O}_F$ together with norms $||\cdot||_v$ on the free F_v-module $M \otimes_R F_v$ of rank 1 for $v \in \Sigma_F^\infty$. ⌟

Def. (16.2.1.2) [Heights and Degree of Metrized Line Bundles]. Let F be a number field and $(\mathcal{L}, |\cdot|)$ be a metrized line bundle on $\mathcal{O}_F$(16.2.1.1), for each $v \in \Sigma_F^0$, $\mathcal{L}_v = \mathcal{O}_{F,v} m_v$ for some $m_v \in \mathcal{L}_v$, so we define $||m||_v = |m/m_v|_v$ for $m \in \mathcal{L}_v$, and define the **height of** $\mathcal{L}$ to be

$$H((\mathcal{L}, |\cdot|)) = \prod_{v \in \Sigma_F} ||m||_v^{-1}, \quad m \neq 0 \in M$$

which is independent of m by product formula. Also we define

$$h(M) = \frac{1}{[F:\mathbb{Q}]} \log H(M),$$

called the **degree of** $\mathcal{L}$. $h((\mathcal{L}, |\cdot|))$ is invariant under change of number fields. ⌟

17 p-Adic Geometry

17.1 $\mathbb{F}_p$-Schemes

1 Perfect Schemes

Def. (17.1.1.1)[Perfect Schemes]. An $\mathbb{F}_p$-scheme is called **perfect** if the Frobenius is an isomorphism on it. Equivalently, this means every affine subscheme is the spectrum of a perfect scheme.

Let Perf be the category of perfect qcqs $\mathbb{F}_p$-schemes endowed with the V-topology(6.1.4.43). ⌟

Def. (17.1.1.2)[Perfection]. There is a **perfection** functor $X \mapsto X_{perf}$ from the category of schemes to the category of perfect schemes, it is defined as the glueing of the perfection $R \to R_{perf}$(5.5.1.3) as it commutes with colimits. ⌟

Prop. (17.1.1.3)[Perfection and Properties]. Let $f : X \to Y$ be a morphism of $\mathbb{F}_p$-schemes, then the following properties holds true for f iff it holds true for f_{perf}:

1. Qco.
2. Quasiseparated.
3. Affine.
4. Separated.
5. Integral.
6. Universally closed.
7. Universal homeomorphism.

The following properties holds for f_{perf} if it holds for f:

1. Closed immersion.
2. Open immersion.
3. immersion
4. Étale
5. (Faithfully)Flat.

⌟

Proof: Cf.[Projectivity of Witt Vectors Affine Grassmannian, 3.4]. □

Prop. (17.1.1.4). If X is an $\mathbb{F}_p$-scheme and $\mathcal{L}$ is a line bundle on X, then $\mathcal{L}$ is ample iff the pullback to X_{perf} is ample. ⌟

Proof: Cf.[Projectivity of Witt Vectors Affine Grassmannian, 3.6]. □

Prop. (17.1.1.5). If X is an $\mathbb{F}_p$-scheme, then $X_{ét} \to X_{perf,ét} : Y \to Y_{perf}$ is an equivalence of sites. ⌟

Proof: □

Prop. (17.1.1.6) [Perfectly Finitely Presented Morphisms]. Let $f : X \to Y$ be a morphism in Perf(17.1.1.1), then f is called a **perfectly finitely presented morphism** if it satisfies the following equivalent conditions:

- Any open affine subscheme $\operatorname{Spec} B \subset X$ mapping to an open affine subscheme $\operatorname{Spec} A \subset Y$, $A \to B$ is perfectly f.p.(5.5.1.5).
- There is an open affine covering $\operatorname{Spec} A_i \to X$ mapping to an open affine covering $\operatorname{Spec} B_i \to Y$ that $B_i \to A_i$ are all perfectly f.p.
- For any cofiltered system $\{Z_i\} \in \mathrm{Perf}_{/Y}$ with affine transition maps, there is a bijection $\operatorname{colim} \operatorname{Hom}_Y(Z_i, X) \cong \operatorname{Hom}_Y(\lim Z_i, X)$.

In particular, perfectly finitely presented is local on the base and target. ⌟

Proof: Cf.[Projectivity of Witt Vectors Affine Grassmannian, 3.11]. □

Prop. (17.1.1.7) [Perfect Base Change]. If

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ \downarrow{f'} & & \downarrow{f} \\ Y' & \xrightarrow{g} & Y \end{array}$$

is a pullback diagram of perfect $\mathbb{F}_p$-schemes, then for any complex $K^\bullet$ of Qco sheaves on X, the base change map(6.3.3.18)

$$Lg^* Rf_* K \to Rf'_* Lg' K$$

is an isomorphism. ⌟

Proof: It is clearly we need only check for the affine case, then let $X = \operatorname{Spec} B, Y = \operatorname{Spec} A, Y' = \operatorname{Spec} A'$, and $X' = \operatorname{Spec} B \otimes_A A'$, then it suffices to prove that

$$K \otimes^L_A A' \cong K \otimes^L_B B'.$$

This follows from the fact $B \otimes_A A' = B \otimes^L_A A'$, by(5.5.1.7). □

Prop. (17.1.1.8) [Cartier Isomorphism]. If ⌟

Proof: □

Cor. (17.1.1.9) [Affine Line case]. Let R be an $\mathbb{F}_p$-algebra and ⌟

17.2 ℓ-adic Étale Cohomologies over Finite Fields

Basic References are [Conrad Seminar note in Stanford], [Seminar on Gross-Zagier over Function Fields, Lei Fu], [Seminar notes on Weil 2 Bhatt], [K-W01], [Etale Cohomology and Weil Conjecture], [A course on Weil Conjectures, Szamuely], [Deligne's proof of the Weil Conjecture, Jannsen].

Notation (17.2.0.1).

- $p \in \mathbf{P}, r \in \mathbb{Z}_+, q = p^r$, $k \cong \mathbb{F}_q$. Denote k_n the unique extension of k of degree n in $\overline{k}$.
- $\ell \in \mathbf{P} \backslash p$.
- $X_0 \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}}/k$, $X = X_0 \otimes_k \overline{k}$ is its base change.
- If $\mathcal{F}_0$ is a sheaf on X_0, then $\mathcal{F} = \mathcal{F}_0 \otimes_k \overline{k}$.
- If $x_0 \in X_0(\overline{k})$, $x = x_0 \otimes_{\kappa(x)} \overline{k}$, and $\overline{x} \in x$ is a point over x_0.
- Fix a CDVR $(\Lambda, K, \mathfrak{m}, k)$ of characteristic $(0, \ell)$.
- For a Noetherian ring A with a distinguished ideal $I \subset A$, let $A_n = A/I^n$.

⌟

1 Weil Sheaves

Weil Sheaves

Def. (17.2.1.1) [Weil Groups]. Cf.[Conrad, L19].**?** ⌟

Def. (17.2.1.2) [Weil Sheaves]. By Galois descent, the pullback induces an equivalence of categories between the category of constructible $\overline{\mathbb{Q}}_\ell$-sheaves on X_0 to the category of constructible $\overline{\mathbb{Q}}_\ell$-sheaves on X with an specified $G(X/X_0) = G_k \cong \widehat{\mathbb{Z}}$-actions. In practice, sometimes it is hard to verify the action of $\mathbb{Z} \subset \widehat{\mathbb{Z}}$ is continuous, which leads to the following definition:

The category $\mathrm{W}\mathcal{S}\mathrm{h}_\ell(X_0)$ of **Weil-sheaves** on X_0 consists of pairs $\mathcal{G}_0 = (\mathcal{G}, F_\mathcal{G})$ where $\mathcal{G}$ is a constructible $\overline{\mathbb{Q}}_\ell$-sheaf on X and an isomorphism $F_\mathcal{G} : F_X^*\mathcal{G} \to \mathcal{G}$(6.2.10.1). Notice F_X^* is not $\overline{k}$-linear! There are natural definition of morphisms of Weil-sheaves. A **lisse Weil-sheaf** is a Weil-sheaf $\mathcal{G}_0$ s.t. $\mathcal{G}$ is lisse. ⌟

Prop. (17.2.1.3) [Constructible $\overline{\mathbb{Q}}_\ell$-Sheaves as Weil Sheaves]. For any constructible $\overline{\mathbb{Q}}_\ell$-sheaf $\mathcal{F}_0$ on X_0, the canonical $F_X^* \operatorname{pr}^* \mathcal{F}_0 \cong (\operatorname{pr} \circ F_X)^* \mathcal{F}_0 = \operatorname{pr}^* \mathcal{F}_0$ makes $\mathcal{F}$ into a Weil-sheaf. ⌟

Prop. (17.2.1.4).

- $\mathrm{W}\mathcal{S}\mathrm{h}_\ell(X_0)$ is an Abelian category, and contains the category of lisse $\overline{\mathbb{Q}}_\ell$-sheaves as an Abelian subcategory.
- The constructions like $R^i f_*, R^i f_!, f^*$ is functorial thus is definable on $\mathrm{W}\mathcal{S}\mathrm{h}_\ell(X)$ by(8.4.2.19).
- The specified isomorphism $F_\mathcal{G} : F_X^*\mathcal{G} \to \mathcal{G}$ gives us an action F_X^* of F_X on $H^i_{\text{ét},c}(X, \mathcal{G})$, just like in(8.4.1.36).
- (Frobenius Actions on Stalks)Let $x_0 \in X_0(\overline{k}), x = x_0 \otimes_{\kappa(x)} \overline{k}, \overline{x} \in x$, there is an Frobenius action $F_{x_0}^*$ of x_0 on $\mathcal{G}_{\overline{x}}$ given as follows: Pulling back $\mathcal{G}_0$ to a Weil-sheaf on x_0, then $F_x^*\mathcal{G}_x \cong \mathcal{G}_x$ gives an isomorphism $\mathcal{G}_{F^{i+1}(\overline{x})} \cong \mathcal{G}_{F^i(\overline{x})}$, whose $\deg(x_0)$-th iterate gives the action $\mathcal{G}_{\overline{x}} \cong \mathcal{G}_{F^{\deg(x_0)-1}(\overline{x})} \cong \ldots \cong G_{F(\overline{x})} \cong \mathcal{G}_{\overline{x}}$. For different choice of $\overline{x}$, the actions are conjugate.

  And if $\mathcal{G}_0$ is a constructible sheaf on X_0, then $F_{x_0}^*$ acts via $\varphi_{x_0}^{-1}$**?**.

⌟

Prop. (17.2.1.5) [Weil Sheaves and Representation]. When X_0 is geo.connected, there is an equivalence of categories

$$\mathrm{W}\mathcal{S}\mathrm{h}_\ell(X_0)\cong \mathrm{Rep}_\ell(W(X_0,\overline{x})):\mathcal{G}_0\mapsto(\mathcal{G}_0)_{\overline{x}},$$

and the correspondence defined in(8.4.7.27) is a sub-correspondence of this.

Thus the notion of **geometric irreducible/semisimple** is definable for Weil-sheaves. ⌟

Proof: Because by the correspondence(8.4.7.27), $\mathcal{G}$ corresponds to a representation of $\pi_1(X,\overline{x})$, and $\pi_1(X,\overline{x})$ acts trivially on the Galois cover X/X_0. Now a representation of $W(X_0,\overline{x})$ is equivalent to an automorphism $\rho(\sigma)$(where $\sigma\in W(X_0,\overline{x})$ satisfies $\deg(\sigma)$ corresponds to the geometric Frobenius) that $\rho(\sigma)\rho(\pi_1(X,\overline{x}))\rho(\sigma^{-1})=\rho(\sigma\pi_1(X,\overline{x})\sigma^{-1})$, which is equivalent to an isomorphism $F_X^*\mathcal{G}\to\mathcal{G}$. □

Prop. (17.2.1.6) [Weil Sheaves and Eigenvalues]. If X_0 is geo.connected, a lisse Weil-sheaf $\mathcal{G}_0$ on X_0 is a usual $\overline{\mathbb{Q}}_\ell$-sheaf iff some deg1 element σ in $W(X,\overline{x})$ acts on $\mathcal{G}_{0\overline{x}}$ with eigenvalues which are ℓ-adic units. ⌟

Proof: This is purely a Galois representation problem, concerning whether the representation of $W(X_0,\overline{x})$ can be extended to a representation of $\pi_1(X_0,\overline{x})$, and it is a continuity problem.

Firstly the representation of $\pi_1(X,\overline{x})$ stabilizes a lattice O_E^n for some $E/\mathbb{Q}_\ell$ finite, and then extends E to contain coefficients of $\rho(\sigma)$ and even its rational form. Then notice $\pi_1(X_0,\overline{x})$ is the profinite completion of $W(X_0,\overline{x})$, thus it suffices to see if the image $\rho(W(X_0,\overline{x}))$ is compact, and this is equivalent to eigenvalues of $\rho(\sigma)$ are units. □

Prop. (17.2.1.7) [Determinential Criterion]. If X_0 is a normal variety, then a irreducible lisse Weil-sheaf on X_0 is an actual $\overline{\mathbb{Q}}_\ell$-sheaf iff its determinant bundle is. ⌟

Proof: Use geometric monodromy group. Cf.[Conrad L19 P7].

First assume that $\mathcal{G}_0$ is geometrically irreducible, then(17.2.4.4) shows that there is a nonzero power $\sigma^m=gz$ where $g\in G_{geo}(\overline{\mathbb{Q}}_\ell)$ and $z\in Z(G(\overline{\mathbb{Q}}_\ell))$. Now G_{geo} is a semisimple algebraic group(17.2.4.4), so the determinential character maps $G_{geo}(G(\overline{\mathbb{Q}}_\ell))$ to a finite group, because connected semisimple algebraic group has no nontrivial character as $[G,G]=G$**?**. So the determinant of g is an l-unit, and $\det(\sigma^m)=\det(z)$ is a unit. But z is a scalar by Schur's lemma, thus z is an l-adic unit. Now it suffices to show the eigenvalue of g are all l-units.

Now consider $\rho(\pi_1(X,\overline{x}))$ is a compact group in $\mathrm{End}(V)$, thus it generates a finite $\mathcal{O}_E$-submodule A , which is full-rank lattice in $\mathrm{End}(V)$ by Jacobson density theorem**?** and the fact ρ is absolutely irreducible. g normalized A, because σ and z both normalizes $\rho(\pi_1(X,\overline{x}))$, so the eigenvalue of the conjugate action of g are all l-units, but its eigenvalue are of the form $\lambda_i\lambda_j^{-1}$ where λ_k are eigenvalues of g, so this together with the fact $\det(g)$ is l-units shows that all λ_i are l-units.

For the general case, Cf.[Conrad L19 P7].**?** □

Cor. (17.2.1.8) [Filtration of Weil Sheaf]. If X_0 is a normal variety, then for any irreducible lisse Weil-sheaf $\mathcal{G}_0$, there is some $b\in\overline{\mathbb{Q}}_\ell^\times$ and a lisse Weil-sheaf $\mathcal{F}_0$ that $\mathcal{G}_0\cong\mathcal{F}_0\otimes\mathcal{L}_b$, where $\mathcal{L}_b$ is the Weil-sheaf corresponding to the character $W(X_0,\overline{x})\to\overline{\mathbb{Q}}_\ell^\times:x\mapsto b^{\deg(x)}$, which is a pull back from $\operatorname{Spec}\mathbb{F}_q$.

More generally, for any lisse Weil-sheaf, there is a filtration that each quotient is of the form $\mathcal{F}_0^{(i)}\otimes\mathcal{L}_{b_i}$ for some $b_i\in\overline{\mathbb{Q}}_\ell^\times$ and $\mathcal{F}_0^{(i)}$ lisse $\overline{\mathbb{Q}}_\ell$-sheaves. ⌟

Proof: Just choose $b = \chi_{\det}(\sigma)^{1/n}$, where $\deg(\sigma) = 1$, then

$$\wedge(\mathcal{G}_0 \otimes \mathcal{L}_{b^{-1}}) \cong \wedge(\mathcal{G}_0) \otimes \mathcal{L}^{-1}_{\chi_{\det}(\sigma)}$$

which has unit eigenvalues thus is a lisse $\overline{\mathbb{Q}}_\ell$-sheaf. □

2 Trace Formulae

Def. (17.2.2.1) [Zeta-Functions]. For $\mathcal{F} \in \mathrm{W}\mathcal{S}\mathrm{h}(X_0)$, the **zeta-function** associated to $\mathcal{F}_0$ is defined to be

$$Z(X_0, \mathcal{F}_0; T) = \prod_{x_0 \in |X_0|_0} \det(1 - F^*_{x_0} T^{\deg(x)} | \mathcal{F}_{\overline{x}})^{-1} \in 1 + T\Lambda[[T]],$$

where $F^*_{x_0}$ is defined in(17.2.1.4). Notice if $\mathcal{F}_0 \in \mathcal{S}\mathrm{h}((X_0)_{\text{ét}})$, then $F^*_{x_0} = \varphi^{-1}_{\kappa(x_0)}$ by(17.2.1.4). ⌟

Prop. (17.2.2.2). Situation as in(17.2.2.1),

$$Z(X_0, \mathcal{F}_0; T) = \exp(\sum_{n \geq 1} \sum_{x \in X_0(k_n)} \mathrm{tr}(F^*_x | \mathcal{F}_{\overline{x}}) \frac{T^n}{n})$$

⌟

Proof: By(3.5.7.26),

$$\begin{aligned} Z(X_0, \mathcal{F}_0; T) &= \prod_{x_0 \in X(\overline{k})} \exp(\sum_{n \geq 1} \mathrm{tr}((F^*_{x_0})^n | \mathcal{F}_{\overline{x}}) \frac{T^{n \deg(x)}}{n}) \\ &= \exp(\sum_{n \geq 1} \sum_{x_0 \in X_0(\overline{k})} \deg(x) \, \mathrm{tr}((F^*_{x_0})^n | \mathcal{F}_{\overline{x}}) \frac{T^n}{n}) \\ &= \exp(\sum_{n \geq 1} \sum_{x_0 \in X_0(k_n)} \mathrm{tr}(F^*_{x_0} | \mathcal{F}_{\overline{x}}) \frac{T^n}{n}) \end{aligned}$$

where in the last equality, notice there are exactly $\deg(x_0)$ many points in $X_0(\overline{k})$ over $x_0 \in X_0(k_n)$. □

Cor. (17.2.2.3). If $\mathcal{F} = \mathbb{Q}_\ell$, then

$$Z(X_0, \mathbb{Q}_\ell; T) = \prod_{x_0 \in |X_0|_0} \frac{1}{1 - T^{\deg(x_0)}}$$

is just the Z-function defined in(21.2.3.1). ⌟

Lemma (17.2.2.4) [Weil Trace Formula]. Let $X_0 \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,ft}}/k$, A be a Noetherian $\mathbb{Z}/(\ell^n)$-algebra, $\mathcal{F}_0 \in D^b_{ctf}(X_0, A)$, then

$$\sum_{x_0 \in X_0(k)} \mathrm{tr}(F^*_{x_0} | \mathcal{F}_{\overline{x}}) = \mathrm{tr}(F^*_X | [R\Gamma_c(X, \mathcal{F})])$$

⌟

Proof: Cf.[Fu11]P596**?**. □

Prop. (17.2.2.5) [General Trace Formula for Frobenius]. Let $X_0 \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,ft}}/k, \mathcal{F}_0 \in D^b_{\mathrm{const}}(X_0, \overline{\mathbb{Q}}_\ell)$, then

$$\sum_{x_0 \in X_0(k)} \mathrm{tr}(F^*_{x_0}|\mathcal{F}_{\overline{x}}) = \mathrm{tr}(F^*_X|[R\Gamma_c(X,\mathcal{F})]).$$

⌟

Proof: Cf.[Fu11]P596**?**. □

Prop. (17.2.2.6) [Grothendieck-Lefschetz Trace Formula for Weil Sheaves]. For $S_0 \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}}/k, f_0 : X_0 \to S_0 \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,ft}}/S, \mathcal{F}_0 = (\mathcal{F}, F_{\mathcal{F}}) \in \mathrm{W}\mathcal{S}\mathrm{h}(X_0)$(17.2.1.2),

$$Z(X_0,\mathcal{F}_0;T) = \prod_{n=0}^{2\dim X_0} Z(S_0, R^n f_{0!}\mathcal{F}_0; T)^{(-1)^n}.$$

In particular, for $S = \operatorname{Spec} k, X_0 \in \mathcal{S}\mathrm{ch}^{\mathrm{sep,ft}}/k$, by base change and(17.2.1.4),

$$Z(X_0,\mathcal{F}_0;T) = \prod_{n=0}^{2\dim X_0} \det(1 - F^*_X T|H^n_{\text{ét},c}(X,\mathcal{F}))^{(-1)^{n+1}}$$

Notice by(8.4.5.7), the higher proper pushforwards just vanish. ⌟

Proof: Use the filtration in(17.2.1.8), notice that the trace is additive for a filtration, so we can reduce to the case $\mathcal{G}_0 = \mathcal{F}_0 \otimes \mathcal{L}_b$ and $\mathcal{G}_{\overline{x}} = \mathcal{F}_{\overline{x}} \otimes \mathcal{L}_{b,\overline{x}}$, then the Euler factors are

$$\det(1 - b^{\deg(x)}\varphi^{-1}_{\kappa(x)} T^{\deg(x)}|\mathcal{F}_{\overline{x}})$$

and the cohomology factor is

$$\det(1 - F^*_X T|H^i_{\text{ét},c}(X,\mathcal{F}\otimes\mathcal{L}_b)) = \det(1 - bF^*_X T|H^i_{\text{ét},c}(X,\mathcal{F}))$$

where the projection formula(8.4.5.8) is used, noticing the $\mathcal{L}_b$ is pulled back from $\operatorname{Spec}\mathbb{F}_q$. Then the assertion is clear from(17.2.2.5) and(17.2.2.2)(17.2.1.4). □

Cor. (17.2.2.7). $Z(X_0,\mathcal{F}_0;T)$ is a rational function in T. ⌟

3 Weights and Purity

Determinantial Weights

Prop. (17.2.3.1) [Structure of Weil Group of Curves]. If X_0 is a smooth curve over $\mathbb{F}_q$, then the image of $\pi_1(X,\overline{x})$ in $W(X_0,\overline{x})^{ab}$ is a product of a finite group and a pro-p group. ⌟

Proof: Let K be the function field of X_0, $\overline{X_0}$ be the regular completion of X_0, with $S_0 = \overline{X_0} - X_0$, then we have an isomorphism $\pi_1(\overline{X_0},\overline{x}) \cong G_K$ Cf.[Étale Cohomology Lei Fu P136]**?**. So we can use global class field theory:

$$\begin{array}{ccccccccc}
 & & \pi_1(\overline{X},\overline{x})^{ab} & \longrightarrow & \pi_1(\overline{X_0},\overline{x})^{ab} & \longrightarrow & G_k \cong \widehat{\mathbb{Z}} & \longrightarrow & 0 \\
 & & \downarrow & \searrow & \uparrow & & \uparrow & & \\
0 & \longrightarrow & I_K & \longrightarrow & W(\overline{X_0},\overline{x})^{ab} \cong W(K,k) & \longrightarrow & W(k) \cong \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow\cong & & \downarrow\cong & & \downarrow\cong & & \\
0 & \longrightarrow & K^*\backslash(A^*_K)^1/\prod_v \mathcal{O}^*_v & \longrightarrow & K^*\backslash A^*_K/\prod_v \mathcal{O}^*_v & \longrightarrow & q^{\mathbb{Z}} & \longrightarrow & 0
\end{array}$$

So the image of $\pi_1(\overline{X},\overline{x})$ factors through $\pi_1(\overline{X},\overline{x})\to\pi_1(\overline{X},\overline{x})^{ab}\to K^*\backslash A_K^*/\prod_v\mathcal{O}_v^*$ which is the class number of K, is finite.

In this diagram, $W(X_0,\overline{x})$ corresponds to $K^*\backslash A_K^*/\prod_{v\notin S_0}\mathcal{O}_v^*$, so

$$0\to\ker(W(X_0,\overline{x})\to W(\overline{X_0},\overline{x}))\to\mathrm{Im}(\pi_1(X_0,\overline{x}))\to\mathrm{Im}(\pi_1(\overline{X_0},\overline{x}))\to 0$$

But the kernel is a quotient of $\prod_{v\in S_0}\mathcal{O}_v^*$, which is a pro$-p$ group times a finite group, so finally $\mathrm{Im}(\pi_1(X_0,\overline{x}))$ is a product of a pro-p-group times a finite group. □

Lemma (17.2.3.2) [Curve Rank 1 case]. If X_0/k is a smooth curve and $\chi: W(X_0,\overline{x})\to\overline{\mathbb{Q}}_\ell^\times$ be a continuous character, then there exists a $c\in\overline{\mathbb{Q}}_\ell^\times$ that χ is a product of a character of finite order and the character $\sigma\mapsto c^{\deg(\sigma)}$.

In particular, the Weil-sheaf corresponding to χ is punctually ι-pure of weight $2\log_q|\iota(c)|$. ⌟

Proof: By(18.3.1.3), the image of χ is in $\mathcal{O}_E^*$ for some $E\in\ell$-`LField`, so by(17.2.3.1), it has an open subgroup which is pro-p and pro-ℓ so trivial, thus $\pi_1(X_0,\overline{x})$ is mapped to a finite group.

In particular there is an n that $\chi^n=\mathrm{id}$ on $\pi_1(X_0,\overline{x})$, so there is some b that $\chi^n=b^{\deg(\sigma)}$, hence if c is an n-th roots of b and we let $\chi'=\chi/c^{\deg(\sigma)}$, then $(\chi')^n=1$. □

Cor. (17.2.3.3) [Rank 1 Lisse Sheaf is Pure]. If X_0/k is a smooth curve, then any lisse Weil-sheaf of rank 1 is pure. ⌟

Def. (17.2.3.4) [Determinential Weight]. Let $\mathcal{F}_0$ be a lisse Weil-sheaf on a geometrically connected smooth scheme X_0, and $0=\mathcal{F}_n\subset\mathcal{F}_{n-1}\subset\ldots\subset\mathcal{F}_0$ be a filtration of lisse sheaves that the quotients are irreducible, we define the **determinential ι-weights** of $\mathcal{F}_0$ to be that of the ι-weights of the top wedge products of the successive quotients divided by their ranks, which exists by(17.2.3.3).

Notice that the determinential ι-weights are unchanged when $\mathcal{F}_0$ is replaced by its semisimplification $\mathcal{F}_0^s=\oplus_{i\geq 0}(\mathcal{F}_i/\mathcal{F}_{i-1})$. ⌟

Purity

Def. (17.2.3.5) [Purity]. For an embedding $\iota:\overline{\mathbb{Q}}_\ell\to\mathbb{C}$, $\mathcal{F}_0\in\mathcal{W}\mathrm{Sh}(X_0)$ is called **ι-pure** of weight w if for any closed point $x\in X$, the $\overline{\mathbb{Q}}_\ell$-eigenvalues of $F_{x_0}^*$ on the stalks $\mathcal{F}_x$(17.2.1.4) are algebraic and satisfy $|\iota(\alpha_i)|=(q^{\deg(x)})^{w/2}$.

It is called **pure of weight** w iff for any closed point $x\in X$, the $\overline{\mathbb{Q}}_\ell$-eigenvalues are $q^{\deg(x)}$-Weil numbers of weight w(14.4.1.13), i.e. ι-pure for any embedding $\iota:\overline{\mathbb{Q}}_\ell\to\mathbb{C}$.

It is said to be **(ι-)mixed** with weights $w_1,\ldots,w_n$ if it has a filtration of constructible $\overline{\mathbb{Q}}_\ell$-sheaves that each quotient is pure of weight w_i respectively. ⌟

Example (17.2.3.6). $\mathbb{Q}_\ell(r)$ is pure of weight $-2r$. ⌟

Proof: This is because the geometric Frobenius $\varphi_{\kappa(x)}^{-1}$ acts by $1/q^{d_x}$-th power, which is additively multiplying by $(q^{d_x})^{-2/2}$. □

Prop. (17.2.3.7) [Permanence Properties].

- $f_0:X_0\to Y_0$ is a morphism, and $\mathcal{G}_0$ is a Weil-sheaf on Y_0, then if $\mathcal{G}_0$ is ι-pure, then $f_0^*\mathcal{G}_0$ is also ι-pure, and the converse is also true if f is surjective.
- If $f_0:X_0\to Y_0$ is finite, and $\mathcal{G}_0$ is a Weil-sheaf on X_0, then if $j_0^*(\mathcal{G}_0)$ is ι-pure, then $\mathcal{G}_0$ is ι-pure.

- Let k'/k be a finite field extension, then a Weil-sheaf $\mathcal{G}_0$ on X_0 is pure of weight β iff $(\mathcal{G}_0)_{k'}$ is on $(X_0)_{k'}$.

⌟

Proof: 1 is because the stalk corresponds.
2: This is because the stalks can be calculated, by**?**.
3: **?** □

Semicontinuity of Weights

Def. (17.2.3.8) [Maximal Weight]. For a general Weil-sheaf $\mathcal{G}_0$ on X_0, we can also define the **maximal ι-weight** of $\mathcal{G}_0$ as

$$w(\mathcal{G}_0)=\sup_{x\in|X_0|}\sup_{\alpha_i}2\log_{N(x)}(|\iota(\alpha_i)|).$$

⌟

Lemma (17.2.3.9). $|X_0(k_n)|=O(q^{n\dim X})$ ⌟

Proof: We can pass to the reduced structure of X_0, then we can use excision to pass to the integral case. Then choose an open affine dense subset U_0 of X_0, then by Noetherian normalization, it factors through a finite map $f:U_0\to\mathbb{A}^{\dim X_0}_{k_n}$, so

$$|U(k_n)|\leq(\deg f)q^{n\dim X_0}$$

Then we can use induction on dimension, because $\dim(X_0-U_0)<\dim X_0$. □

Lemma (17.2.3.10). Let $\mathcal{G}_0$ be a Weil-sheaf on X_0 and β be a real number that $\beta\geq w(\mathcal{G}_0)$, then the L-function

$$\iota(L(X_0,\mathcal{G}_0,t))=\prod_{x\in|X_0|}\iota(\det(1-t^{d_x}F_x,\mathcal{G}_{0,\overline{x}})^{-1})$$

converges for $|t|<q^{-\beta/2-\dim X_0}$ and has no zero or pole there. ⌟

Proof: We can show that it has no zero or pole using the fact that the logarithmic derivative has no poles(when it is convergent). We suppress the isomorphism $\iota:\overline{\mathbb{Q}}_\ell\to\mathbb{C}$ and calculate:

$$\frac{d\log}{dt}L(X_0,\mathcal{G}_0,t)=\sum_{x\in|X_0|}\sum_{n\geq1}d_x(\mathrm{tr}(F_x^n))t^{d_xn-1}\mathbf{??}=\sum_{n\geq1}\sum_{x\in|X_0|,d_x|n}d_x(\mathrm{tr}(F_x^{n/d_x}))t^{n-1}$$

Notice by assumption on β, $|\mathrm{tr}(F_x^{n/d_x})|\leq rq^{n\beta/2}$, where $r=\max_{x\in|X_0|}\dim_{\overline{\mathbb{Q}}_\ell}\mathcal{G}_{0,x}$ is finite because it has a stratification by(8.4.7.15), so

$$|\frac{d\log}{dt}L(X_0,\mathcal{G}_0,t)|\leq\sum_{n\geq1}\sum_{x\in|X_0|,d_x|n}d_xrq^{n\beta/2}t^{n-1}=\sum_{n\geq1}|X_0(k_n)|rq^{n\beta/2}t^{n-1}$$

converges for $|t|<q^{-\beta/2-\dim X_0}$ by(17.2.3.9). □

Lemma (17.2.3.11) [Semicontinuity of Weights for Curves]. If X_0/k be a smooth curve and $U_0\xrightarrow{j_0}X_0$ be a nonempty open with $S_0=X_0-U_0$. Let $\mathcal{G}_0$ be a Weil-sheaf on X_0 s.t. the restriction $j_0^*\mathcal{G}_0$ is lisse and $H^0_S(X,\mathcal{G})=0$, then $w(j_0^*(\mathcal{G}_0))\leq\beta$ implies $w(\mathcal{G}_0)\leq\beta$. ⌟

Proof: For any point x, consider an affine open subset of X_0, then reduce to the affine case, and because $H^0_S(X,\mathcal{G})=0$ and the excision sequence(8.4.5.5), we have $\mathcal{G}\hookrightarrow j_*j^*\mathcal{G}$, so the weights of $\mathcal{G}_0$ are no more than that of $j_*j^*\mathcal{G}$, and replacing $\mathcal{G}_0$ with $j_{0*}j_0^*\mathcal{G}_0$, we can assume $\mathcal{G}_0=j_{0*}j_0^*\mathcal{G}_0$. Then

$$H^0_c(X,\mathcal{G})=H^0_c(X,j_*j^*\mathcal{G})=H^0_c(U,j^*\mathcal{G})=0$$

by Poincare duality and the fact j_* is exact because it is finite.

Now by Grothendieck-Lefschetz trace formula,

$$L(X_0,\mathcal{G}_0,t)=L(U_0,j_0^*(\mathcal{G}_0),t)\cdot\prod_{s\in|S_0|}\det(1-t^{d_s}F_s,\mathcal{G}_{\overline{s}})^{-1}=\frac{\det(1-F_Xt|H^1_{\text{ét},c}(X,\mathcal{G}))}{\det(1-F_Xt|H^2_c(X,\mathcal{G}))}$$

Denote $\mathcal{F}_0=j_0^*\mathcal{G}_0$, then

$$H^2_c(X,\mathcal{G})=H^2_c(U,\mathcal{F})=(\mathcal{F}_{\overline{x}})_{\pi_1(U,\overline{x})}(-1)$$

So the weights of eigenvalues of F_X on $H^2_c(X,\mathcal{G})\leq$ weights of $\mathcal{F}+2$, hence the L-function converges for $|t|<q^{-\beta/2-1}$. Now the LHS has $L(U_0,j_0^*(\mathcal{G}_0),t)$ converges for $|t|<q^{-\beta/2-1}$ because $w(\mathcal{F}_0)\leq\beta$, and so for the points in S_0, we also have $\det(1-t^{d_s}F_s,\mathcal{G}_{\overline{s}})$ has no zero there, which means they have weights$\leq\beta+1$. Now consider replacing $\mathcal{G}_0$ with $\mathcal{G}_0^{\otimes k}$ and let $k\to\infty$, then their weights$\leq\beta$. □

Prop. (17.2.3.12) [Semicontinuity of Weights]. Let X_0 be geo.normal, $\mathcal{G}_0$ be a lisse sheaf on X_0 and $j_0:U_0\to X_0$ be an open dense subscheme, then

- $w(\mathcal{G}_0)=w(j_0^*\mathcal{G}_0)$.
- If $j_0^*(\mathcal{G}_0)$ is ι-pure of weights β, then $\mathcal{G}_0$ is also ι-pure of weights β.
- Let X_0 be irreducible and normal, and $\mathcal{G}_0$ is irreducible, then if $j_0^*\mathcal{G}_0$ is ι-mixed, then $\mathcal{G}_0$ is ι-pure.

⌟

Proof: 1: The weights is local so we may assume X_0 is irreducible, and then for any closed point x, we can connect it with U_0 with a curve(choose an affine open and use Noetherian Normalization to choose an irreducible component of an arbitrary curve in $\mathbb{A}^n$). Notice $H^0_S(X,\mathcal{G})=0$ because it is lisse thus $H^0(X,\mathcal{G})$ is determined by stalk thus $H^0(X,\mathcal{G})\to H^0(U,\mathcal{G}|_U)$ is injective. So we finish by the curve case(17.2.3.11).

2: Apply item1 to $\mathcal{G}_0$ and $\mathcal{G}_0^\vee$.

3: It is ι-mixed so it has ι-pure Weil-sheaf constituents. Now by(8.4.7.15) we can find an open dense U_0 that restriction to U_0 has constituents ι-pure lisse sheaves. But it is also irreducible because $\pi_1(U_0,\overline{a})\to\pi_1(X_0,\overline{a})$ is surjective?, so it is ι-pure and item2 shows $\mathcal{G}_0$ is ι-pure. □

L^2-Norms and Maximal Weights

Def. (17.2.3.13). As in(17.2.8.1), for any $\mathcal{G}_0\in D^b_{cons}(X_0,\overline{\mathbb{Q}}_\ell)$, we have a a function

$$f^{\mathcal{G}_0}:X_0(\mathbb{F}_{q^n})\to\overline{\mathbb{Q}}_\ell:x\mapsto\sum_i(-1)^i\operatorname{tr}(F_x^{n/d_x}|(H^i(\mathcal{G}_0))_{\overline{x}}),$$

Fix an arbitrary isomorphism $\overline{\mathbb{Q}}_\ell\cong\mathbb{C}$, we can consider the usual L^2-norm for functions on $X_0(k_n)$, denoted by $(f,g)_n$. ⌟

Def. (17.2.3.14). Notice the equation form(17.2.3.10) can be rewritten as

$$\frac{d\log}{dt}L(X_0,\mathcal{G}_0,t)=\sum_{n\geq 1}\sum_{x\in|X_0|,d_x|n}d_x(\mathrm{tr}(F_x^{n/d_x}))t^{n-1}=\sum_n(f^{\mathcal{G}_0},1)_n t^{n-1}.$$

Now we define another closed related function

$$\varphi^{\mathcal{G}_0}(t)=\sum_n||f^{\mathcal{G}_0}||_n^2t^{n-1},$$

which works better with Fourier transform we are about to define later. ⌟

Lemma (17.2.3.15). There is a constant C that $||f^{\mathcal{G}_0}(x)||^2\leq Cq^{n(w(\mathcal{G}_0)+\dim X_0)}$, so $\varphi^{\mathcal{G}_0}(t)$ converges for $|t|\leq q^{-w(\mathcal{G}_0)-\dim X_0}$. ⌟

Proof: The proof is similar to that of(17.2.3.10) thus omitted. □

Def. (17.2.3.16) [Norm of a Weil Sheaf]. Define the Norm of a Weil-sheaf as

$$||\mathcal{G}_0||=\sup\{\rho|\limsup_n\frac{||f^{\mathcal{G}_0}||_n^2}{q^{n(\rho+\dim X_0)}}>0\}$$

Then $q^{-||\mathcal{G}_0||-\dim X_0}$ is just the radius of convergence of the function $\varphi^{\mathcal{G}_0}(t)$, and $||\mathcal{G}_0||\leq w(\mathcal{G}_0)$ by lemma(17.2.3.15) above. ⌟

Prop. (17.2.3.17) [Radius of Convergence]. Let $\mathcal{G}_0$ be a ι-mixed sheaf on a smooth curve X_0 over k, and $H^0_{\text{ét},c}(X,\mathcal{G})=0$, then $||\mathcal{G}_0||=w(\mathcal{G}_0)=\beta$. ⌟

Proof: It suffices to show $w(\mathcal{G}_0)\leq||\mathcal{G}_0||$. First notice we can assume X_0 is reduced because the nilpotents corredsponds to zero Frobenius eigenvalues, and also it is connected, because the function $f^{\mathcal{G}_0}$ is additive in X. Now we study by cases:

1: If $\mathcal{G}_0$ is a lisse ι-pure sheaf on a smooth affine curve X_0, we may assume $\mathcal{G}_0\neq 0$, then $\mathcal{G}_0\otimes\overline{\mathcal{G}_0}$(17.2.5.2) is ι-real of weight 2β and $(f^{\mathcal{G}_0\otimes\overline{\mathcal{G}_0}},1)_n=||f^{\mathcal{G}_0}||_n^2$, so $\varphi^{\mathcal{G}_0}(t)$ is just the logarithmic derivative of the L-function $L(X_0,\mathcal{G}_0\otimes\overline{\mathcal{G}_0},t)$, thus(17.2.3.10) shows its convergence radius$\geq q^{-\beta-1}$. And notice the H^0_c terms vanish so the poles can only appear as the zeros of H^2_c term, so(17.2.5.3) shows the poles of the $L(X_0,\mathcal{G}_0\otimes\overline{\mathcal{G}_0},t)$ has weight $2\beta+2$, thus the poles can only appear on $|t|=q^{-\beta-1}$.

Now consider each local Euler factor $\det(1-F_xt^{d_x}|(\mathcal{G}_0\otimes\overline{\mathcal{G}_0})_x)^{-1}$ has non-negative coefficients, they have poles because $\mathcal{G}_0\neq 0$, and their poles have weight β because of purity, thus their product also has (real)poles, by previous argument, the pole has weight $\beta+1$, thus it has convergence radius at most $q^{-\beta-1}$, so we are done.

2: If $\mathcal{G}_0$ is a ι-mixed, consider its semisimplification $\mathcal{G}_0^{ss}=\mathcal{F}_0\oplus\mathcal{H}_0$, where $\mathcal{F}_0$ is ι-pure of weight $w(\mathcal{G}_0)$, and $w(\mathcal{H}_0)\leq w(\mathcal{F}_0)$.

Then $f^{\mathcal{G}_0}=f^{\mathcal{F}_0}+f^{\mathcal{H}_0}$, and

$$\varphi^{\mathcal{G}_0}(t)=\varphi^{\mathcal{F}_0}(t)+\sum_{n\geq 1}2\,\mathrm{Re}(f^{\mathcal{F}_0},f^{\mathcal{H}_0})_nt^{n-1}+\varphi^{\mathcal{H}_0}(t)$$

then by item1 $\varphi^{\mathcal{F}_0}(t)$ has convergence radius $q^{-w(\mathcal{G}_0)-1}$, and by(17.2.3.15) $\varphi^{\mathcal{H}_0}(t)$ has radius at least $q^{-w(\mathcal{H}_0)-1}>q^{-w(\mathcal{G}_0)-1}$, and by Cauchy inequality the middle term satisfies

$$|2\,\mathrm{Re}(f^{\mathcal{F}_0},f^{\mathcal{H}_0})_n|\leq 2||f^{\mathcal{F}_0}||_n||f^{\mathcal{H}_0}||_n\leq Cq^{n(w(\mathcal{F}_0)+w(\mathcal{H}_0)/2+1)}$$

So the middle term has convergence radius$>$ $q^{-w(\mathcal{G}_0)-1}$, so their sum has convergence radius $q^{-w(\mathcal{G}_0)-1}$. □

4 Geometric Monodromy

Def. (17.2.4.1) [Notations]. Let X_0 be a geometrically connected normal scheme over $k = \mathbb{F}_q$ in this subsection. ⌟

Def. (17.2.4.2) [Geometric Monodromy Group]. Let $\mathcal{G}_0$ be a Weil-sheaf associated to a representation $(V,\rho) = GL(\mathcal{G}_{\overline{x}})$ of $W(X_0,\overline{x})$, the **geometric monodromy group** G_{geo} associated to $\mathcal{G}_0$ is the Zariski Closure of $\rho(\pi_1(X,\overline{x})) \subset GL(V)$.

Every element in $\rho(W(X_0,\overline{x}))$ normalizes G_{geo} by continuity, so choosing an arbitrary generator $\sigma \in W(\overline{k}/k)$, we have an action of $W(\overline{k}/k)$ on G_{geo}. Define $G = W(\overline{k}/k) \ltimes G_{geo}$ the **arithmetic monodromy group** of $\mathcal{G}_0$. ⌟

Lemma (17.2.4.3). If G_{geo} is connected, then there is a positive integer N that the semidirect sequence

$$1 \to G_{geo} \to \deg^{-1}(N\mathbb{Z}) \xrightarrow{\deg} N\mathbb{Z} \to 1$$

is direct, i.e. $\deg^{-1}(N\mathbb{Z}) \cong G_{geo} \times \mathbb{Z}$. ⌟

Proof: Choose a $\deg(g) = 1$. The representation G_{geo} splits as a characters of $Z(G)$, and then some g^n stablizes these characters, hence stablizes $Z(G)$, which then it descends to an action on G_{adj}, whose automorphism is the automorphism of the Dynkin diagram**?**, so finite, so some g^m fixes G_{adj} after changing a semidirect product, thus induces a map $\mathrm{Hom}(G_{adj}, Z(G))$, but G_{adj} is semisimple(9.3.3.19), so the connected component is mapped to 1 in $Z(G)$(9.3.3.17), so there are only f.m. such homomorphism, showing g^k is 1, so the product is exact for $N = k$. □

Prop. (17.2.4.4) [Geometric Monodromy Group is Semisimple]. Let $\mathcal{G}_0$ be a geometrically semisimple lisse Weil-sheaf(17.2.1.5), then

- G_{geo} and G^0_{geo} are semisimple algebraic group.
- Let $Z = Z(G(\overline{\mathbb{Q}}_\ell))$, then the map $\psi : Z \to W(\overline{k}/k)$ has finite kernel and cokernel. In particular, Z contains an element of finite degree, and it is surjective after a finite base change of fields.

And notice in fact if $\mathcal{G}_0$ is semisimple, then it is automatically geometrically semisimple by(18.1.2.10). ⌟

Proof: 1: L G_{geo} is semisimple iff G^0_{geo} is semisimple. Pass to a finite étale covering, we may assume $G_{geo} = G^0_{geo}$. Let $R(G^0_{geo})$ be the radical and $R_u(G^0_{geo})$ be the unipotent radical, then R is normal in G^0 and G^0 is normal in G, so by(18.1.2.10) $V = GL(\mathcal{G}_{\overline{x}})$ is irreducible $R(G^0_{geo})$ representation, but it is solvable, so V is a direct sum of 1-dimensional representations, and $R_u(G^0_{geo})$ is trivial, in particular G^0_{geo} is reductive. So it is semisimple if the maximal Abelian quotient G^{ab}_{geo} is finite(9.3.3.17).

let T_1 be the maximal central torus of G^0_{geo}, then lemma(17.2.4.3) shows after a finite base change of fields, we may assume $G = G_{geo} \times \mathbb{Z}$, consider the composite $W(X_0,\overline{x}) \to G_{geo} \times \mathbb{Z} \to G_{geo} \to G^{ab}_{geo}$, then $\pi_1(X,\overline{x})$ is Zariski dense in G^{ab}_{geo}, and (17.2.3.3) shows clearly G^{ab}_{geo} has no maximal torus thus finite.

2: $\ker\psi \subset Z(G_{geo}(\overline{\mathbb{Q}}_\ell))$ is finite since G_{geo} is semisimple. To find an element in $Z(G)$ of positive degree, we may use the same method as before to find an element ζ that commutes with G^0_{geo}, and pass to a power, we may assume it acts trivially on G_{geo}/G^0_{geo}.

For any $g \in G_{geo}$, consider $vp_g(n) = g\zeta^n g^{-1}\zeta^{-n} \in G^0_{geo}$, so $\varphi_g(m+n) = \varphi_g(n)\zeta^n\varphi_g(m)\zeta^{-n} = \varphi_g(n)\varphi_g(m)$, thus it is a homomorphism, and if $g' \in G^0_{geo}$, then

$$\varphi_g = \varphi_{g(g^{-1}g'g)} = \varphi_{g'g} = g'\varphi_g(g')^{-1}$$

so φ_g has image in $Z(G^0_{geo})$, which is finite, so $\varphi_g(n)=1$ for some n, then ζ^n commutes with G_{geo} so $\zeta^n\in Z(G)$. □

Cor. (17.2.4.5) [Weights and Center Element Actions]. Let $\mathcal{G}_0$ be a semisimple lisse Weil-sheaf on X_0, if $z\in Z(G(\overline{\mathbb{Q}}_\ell))$ satisfies $\deg(z)=n\neq 0$, which exists by(17.2.4.4), then if z acts on V with eigenvalues α_i, then $\frac{2}{n}\log_q(|\iota(\alpha_i)|)$ is just the determinential ι-weights of $\mathcal{G}_0$. ⌟

Proof: z is in the center, thus by Shur's lemma, it acts on each irreducible part of $\mathcal{G}_0$ by a constant. Thus the determinential weights are clear, by definition. □

Cor. (17.2.4.6) [Properties of Determinential Weights]. Let X_0/k be a smooth curve, $\mathcal{F}_0,\mathcal{G}_0$ be lisse Weil-sheaves on X_0, then

- If α_i are the determinential ι-weights of $\mathcal{F}_0$ and β_j be that of $\mathcal{G}_0$, then $\alpha_i+\beta_j$ are those of $\mathcal{F}_0\otimes\mathcal{G}_0$ with multiplicity.
- For $\gamma\in\mathbb{R}$, let $r(\gamma)$ be the sum of ranks of all irreducible constituents of $\mathcal{F}_0$ which have determinential weight γ w.r.t ι, then the determinential weights of $\wedge^r\mathcal{F}_0$ are the numbers $\sum_\gamma n(\gamma)\gamma$ with $\sum n(\gamma)=r$ and $0\leq n(\gamma)\leq r(\gamma)$, $n(\gamma)\in\mathbb{Z}$ with multiplicity.

⌟

Proof: Firstly notice the determinential weight is unchanged when we change $\mathcal{F}_0,\mathcal{G}_0$ to their semisimplification $\mathcal{F}_0^{ss},\mathcal{G}_0^{ss}$(17.2.3.4). And notice $(\mathcal{F}_0\otimes\mathcal{G}_0)^{ss}=((\mathcal{F}_0)^{ss}\otimes(\mathcal{G}_0)^{ss})^{ss}$, thus the determinential weights of $\mathcal{F}_0\otimes\mathcal{G}_0$ are also unchanged. Similarly for the wedge product.

2: We may assume $\mathcal{F}_0,\mathcal{G}_0$ are irreducible, and let $\mathcal{H}_0=(\mathcal{F}_0\otimes\mathcal{G}_0)^{ss}$, $G^{\oplus}_{geo},G^{ss}_{geo}$ be the geometric monodromy group of $\pi_1(X,\overline{x})$ in $GL(\mathcal{F}_{\overline{x}}\oplus\mathcal{G}_{\overline{x}})$ and $GL(\mathcal{H}_{\overline{x}})$ correspondingly, then $G^{\oplus}_{geo}\to G^{ss}_{geo}$ is surjective because they are both the geometric monodromy group of $\mathcal{H}_{\overline{x}}$. So also $G^{\oplus}\to G^{ss}$ is surjective. So if g be an element in the center of $G^{\oplus}$ that has nonzero degree, then it maps to the center of G^{ss} of nonzero degree. And the action of g on each factor $\mathcal{F}_x,\mathcal{G}_x$ is a constant, so action on H_x is also a constant, so we are done.

3: Easy from2. □

5 Real Sheaves

Def. (17.2.5.1) [ι-Real Sheaf]. Let $\mathcal{F}_0$ be a Weil-sheaf on X_0, then $\mathcal{F}_0$ is called **ι-real** if for any $x\in|X_0|$, the characteristic polynomial $\iota(\det(1-F_xt;\mathcal{F}_{\overline{x}}))$ of F_x real coefficients. ⌟

Prop. (17.2.5.2). Any ι-pure Weil-sheaf of weight w is a direct sum of a ι-real ι-pure Weil-sheaf. In fact, $\mathcal{F}_0\oplus\mathcal{F}_0^\vee(-w)=\mathcal{F}_0\oplus\overline{\mathcal{F}_0}$ is ι-real. ⌟

Lemma (17.2.5.3) [Eigenvalue of Cohomology and Stalk in Curve case]. Let X_0/k be a smooth curve, $\mathcal{F}_0\in\mathrm{W\mathcal{S}h}(X_0)$ is lisse, then the eigenvalues of F_X on $H^0(X,\mathcal{F})$ or $H^2_{\text{ét},c}(X,\mathcal{F})$ is related to the determinential weights of $\mathcal{F}_0$ and the eigenvalue of F_x on $\mathcal{F}_{\overline{x}}$. ⌟

Proof: Let $V=\mathcal{F}_{\overline{x}}$, then

$$H^0(X,\mathcal{F})=V^{\pi_1(X,\overline{x})},\quad H^2_c(X,\mathcal{F})=V_{\pi_1(X,\overline{x})}(-1).$$

Then the base change sheaf of the sheaf $V^{\pi_1(X,\overline{x})}$ or $V_{\pi_1(X,\overline{x})}(-1)$ on $\operatorname{Spec}k$ is the maximal subsheaf/quotient lisse sheaf of $\mathcal{F}_0$ that is constant on X. Then it has determinential weights just the action of F_X on the stalk by(17.2.4.5), which are also determinential weights of $\mathcal{F}_0$ by(17.2.4.6). □

Lemma (17.2.5.4) [Rankin-Selberg Method]. Let X_0/k be a smooth curve, $\mathcal{F}_0 \in \mathrm{W}\mathcal{S}\mathrm{h}(X_0)$ is lisse, and w be the largest determinential weight of $\mathcal{F}_0$, then for any $x \in |X_0|$, $w_{N(x)}(\alpha) \le w$. ⌟

Proof: By the arbitraryness of x, we can replace X_0 by an affine open nbhd of x. Then $H^0_c(X, \mathcal{G}) = 0$ by Artin vanishing(8.4.2.12). By Grothendieck trace formula,

$$\prod_{x\in|X_0|} \iota\det(1 - t^{d_x}F_x| \otimes^{2k} \mathcal{F}_{\overline{x}})^{-1} = \frac{\iota\det(1 - tF_X^*|H^1_c(X, \otimes^{2k}\mathcal{F}))}{\iota\det(1 - tF_X^*|H^2_c(X, \otimes^{2k}\mathcal{F}))}$$

Now the weight of root t_0 of $\det(1-tF_X^*|H^2_c(X, \otimes^{2k}\mathcal{F}))$ has weight$\le$(determinential weight of $\mathcal{G}_0^{\otimes 2k}$)$+$ 2(17.2.5.3) $\le 2kw + 1$(17.2.4.6), so $|t_0| \ge q^{-k\beta-1}$.

Now by the formula**??** and noticing $\mathrm{tr}(F_x^n, \otimes^{2k}\mathcal{F}_{\overline{x}}) = (\mathrm{tr}(F_x, \mathcal{F}_{\overline{x}}))^{2k}$, so $(1 - t^{d_x}F_x| \otimes^{2k} \mathcal{F}_{\overline{x}})^{-1}$ has non-negative coefficients, which means their convergence radius are no less than $q^{-k\beta-1}$, equivalently, $(1 - t^{d_x}F_x| \otimes^{2k} \mathcal{F}_{\overline{x}})$ has no zeros with eigenvalue$< q^{-k\beta-1}$.

So for any eigenvalue α of F_x acting on $\mathcal{F}_{\overline{x}}$, $|\iota(\alpha^{-2k/d_x})| \le q^{-k\beta-1}$, or equivalently,

$$|\iota(\alpha)|^2 \le N(x)^{\beta+1/k}.$$

Now let $k \to \infty$, we are done. □

Lemma (17.2.5.5) [Real Sheaf Mixed Curve case]. Let X_0/k be smooth curve and $\mathcal{F}_0 \in \mathrm{W}\mathcal{S}\mathrm{h}(X_0)$ is ι-lisse, then all irreducible constituents of $\mathcal{F}_0$ is ι-pure, and their ι-weights coincides with their determinential weights. ⌟

Proof: For $\beta \in \mathbb{R}$, let $\mathcal{F}_0(\beta)$ be the sum of constituents of $\mathcal{F}_0$ of determinential weight β, and let $n(\beta) = \mathrm{rank}(\mathcal{F}_0(\beta))$, then we need to show that $w_{N(x)}(\alpha_i(\beta)) = \beta$ for any eigenvalue of $\mathcal{F}_x$ on $\mathcal{F}(\beta)_{\overline{x}}$.

By definition of determinential weight, for each γ, we have $\sum w_{N(x)}(\alpha_j(\gamma)) = n(\gamma)\gamma$. Now let $N = \sum_{\gamma>\beta} n(\gamma)$, then any determinential weight of $\wedge^{N+1}\mathcal{F}_0$ has weight$\le \beta + \sum_{\gamma>\beta} n(\gamma)\gamma$: This is clear by(17.2.4.6) as the determinential weights of $\wedge^{N+1}\mathcal{F}_0$ is of the form $\sum_\gamma a(\gamma)\gamma$ that $0 \le a(\gamma) \le \gamma$ and $\sum_\gamma a(\gamma) = N + 1$.

But now $\alpha_i(\beta)\prod_{\gamma>\beta}\prod_{i=1}^{n(\gamma)} \alpha_j(\gamma)$ is an eigenvalue of $(\wedge^{N+1}\mathcal{F}_0)_{\overline{x}}$, but by lemma(17.2.5.4), $w_{N(x)}(\alpha_i(t)) \le t$. Thus we must have equality $w_{N(x)}(\alpha_i(\beta)) = \beta$. □

Prop. (17.2.5.6) [Real Sheaf is Mixed]. Let X_0 be an algebraic scheme over $\mathbb{F}_q$, then

- Any ι-real Weil-sheaf on X_0 is ι-mixed.
- If X_0 is irreducible and normal, any irreducible constituent of a lisse of an ι-real sheaf is ι-pure.

⌟

Proof: Cf.[Bhatt P28], [KW, P36].

We have the following devissages:

- Choose an open subset $j_0 : U_0 \hookrightarrow X_0, S_0 = X_0 - U_0$ and consider the fundamental excision sequence(8.4.5.4), we can reduce to an open affine subscheme $U_0 \subset X_0$.
- We may base change to a finite field extension.**?**
- So we may reduce to the case X_0 is smooth, irreducible affine, and $\mathcal{G}_0$ is lisse, with all the irreducible constituents geometrically irreducible(by base change, because they are geometrically semisimple(17.2.4.4)). And we may assume $\dim X_0 > 1$ because the curve case is proven.
- Change k to the alg.closure of k in the function field of X_0, we can assume X_0 is geometrically irreducible by(6.4.3.16).

Embed X_0 in some projective space $\mathbb{P}_0^N$, then by a suitable Bertini theorem, the linear subspaces of codimension $\dim X - 1$ that intersects X with a non-empty smooth irreducible curve C_L is dense in the Grassmannian. Now the closed points in any C_L is a pure-point for the any irreducible component $\mathcal{F}_0$ of $\mathcal{G}_0$ of the same weights. Now let L vary, then there is a dense subset of a finite extension of X_0 that $\mathcal{F}_0$ is pure. So we are done. □

6 Deligne's Purity Theorem

Thm. (17.2.6.1) [Deligne's Purity Theorem]. If $f : X_0 \to Y_0$ is a separated morphism of algebraic scheme over k, and $\mathcal{F}_0$ is a lisse $\overline{\mathbb{Q}}_\ell$-sheaf on X that is mixed weights$\leq n$, then for any integer $i \geq 0$, the sheaf $R^i f_{0!}\mathcal{F}_0$ is also ι-mixed of weights$\leq n + i$.

Moreover, each ι-weight of of $R^i f_! \mathcal{F}$ is equivalent modulo $\mathbb{Z}$ to an ι-weight of $\mathcal{F}$. In particular, if all ι-weights of $\mathcal{F}$ is integral, then so is $R^i f_! \mathcal{F}$. ⌟

Proof: This follows from(17.2.6.6). □

Cor. (17.2.6.2). If X_0 is a smooth separated algebraic scheme over k, $\mathcal{F}_0$ is mixed of weight $\geq n$, then $\mathrm{H}^i_{\text{ét}}(X, \mathcal{F})$ is mixed of weights $\geq n + i$. ⌟

Proof: By Poincaré duality(8.4.7.51), $H^{2d-n}_{\text{ét},c}(X, \mathcal{F}^\vee(d)) = (\mathrm{H}^n_{\text{ét}}(X, \mathcal{F}))^\vee$ as Galois representation, and $\mathcal{F}^\vee(d)$ is still a lisse sheaf pure of weight $-w - 2d$, thus Deligne's purity theorem(17.2.6.1) shows that $H^{2d-n}_{\text{ét},c}(X_{\overline{k}}, \mathcal{F}^\vee(d))$ has weight $\leq (-w - 2d) + (2d - n) = -w - n$, thus we are done. □

Cor. (17.2.6.3) [Weil's Conjecture]. Let X_0 be a smooth separated algebraic k-scheme, and $\mathcal{F}_0$ is a lisse $\overline{\mathbb{Q}}_\ell$-sheaf which is pure of weight w, then the image of $H^n_{\text{ét},c}(X, \mathcal{F})$ in $\mathrm{H}^n_{\text{ét}}(X, \mathcal{F})$ is pure of weight $w + n$. ⌟

Proof: The morphism $H^n_{\text{ét},c}(X, \mathcal{F}) \to \mathrm{H}^n_{\text{ét}}(X, \mathcal{F})$ defined in(8.4.5.6) is compatible with Frobenius, so from(17.2.6.2) we know the image has weights$\geq w + n$, so combined with Deligne's purity theorem(17.2.6.1), we know it is pure of weight $w + n$. □

Cor. (17.2.6.4). If $f_0 : X_0 \to Y_0$ is a smooth proper map of algebraic schemes and $\mathcal{F}_0$ is ι-pure of weight β, then $R^i f_{0,*}\mathcal{F}_0$ is ι-pure of weight $\beta + i$. ⌟

Proof: Use proper base change of(8.4.5.5) to reduce to the case of(17.2.6.3). Notice in the proper case, $Rf_* = Rf_!$. □

Cor. (17.2.6.5) [Riemann Hypothesis]. If $X_0 \in \mathcal{S}m\mathcal{P}rpr/k$, then $\mathrm{H}^n_{\text{ét}}(X; \mathbb{Q}_\ell)$ as a Weil-sheaf over $\operatorname{Spec} k$, is pure of weight n. ⌟

Reduction to Curve case

Prop. (17.2.6.6). Deligne's purity theorem(17.2.6.1) can be reduced to case that X_0 is a smooth geometrically connected affine curve$\subset \mathbb{A}^1_{\mathbb{F}_q}$ and $\mathcal{F}_0$ a lisse $\overline{\mathbb{Q}}_\ell$-sheaf. ⌟

Proof: We have the following dévissages about the Deligne's :

1. It is trivial in case f_0 is quasi-finite. This is because of(8.4.5.7), as the fiber has dimension 0.
2. We can replace X_0 by an affine open $U_0 \subset X_0$ by Noetherian induction and excision sequence(8.4.5.5), which commutes with Frobenius action.
3. If the conclusion is true for g_0, h_0, then it is true for $f_0 = g_0 \circ h_0$, this follows from the Leray spectral sequence(8.4.5.5), which is Frobenius equivariant by(8.4.1.35).

4. We can replace Y_0 with an affine open $U_0 \subset Y_0$: If the image f_0 is not dense, then trivial, if it is dense, then choose any affine open U_0, then it suffices to prove for $f_0 : f_0^{-1}(U_0) \to Y_0$ by item2, then then by item3 it suffice to prove for $f_0 : f_0^{-1}(U_0) \to U_0$, because $U_0 \hookrightarrow Y_0$ is quasi-finite and use item1.

Now we claim we can reduce to the case of $f_0 : X_0 \to Y_0$ surjective affine smooth with the fibers being geometrically irreducible curves: By devissage2 and 4, we may assume X_0, Y_0 is affine, thus f_0 is affine. Take a generic point η of Y_0(How to pass to the reduced case**?**), then $(X_0)_\eta \to \operatorname{Spec} k(\eta)$ is affine hence by Noetherian normalization(5.2.4.22) there is a finite map $X_\eta \to \mathbb{A}^n_{k(\eta)}$, and this spread out to a finite morphism $f_0^{-1}(U_0) \to U_0$ for some affine open $U_0 \subset Y_0$ because f_0 is of f.t.. Then by Devissage1 and 3 we are reduced to the case $A^1_{Y_0} \to Y_0$. Now by(8.4.7.15), there is an affine open $U_0 \subset A^1_{Y_0}$ that $\mathcal{F}_0|_{U_0}$ is lisse, so by Devissage2 we may change X_0 to U_0.

That is we reduced to the case that $\mathcal{F}_0$ is lisse and X_0 is open in $\mathbb{A}^1_{Y_0}$ so f_0 is smooth affine, in particular open(6.6.4.4), so we can replace Y_0 by $f(X_0)$ and assume f_0 is surjective. Then the fiber are all geometrically irreducible curves.

Then the assertion about weights are clear from proper base change(8.4.5.5) and the curve case.

For the ι-mixedness, we may use(17.2.5.2) and(17.2.5.6) to reduce to showing that $R^i f_!$ maps ι-real sheaves to ι-real sheaves.

for a geometric point $\overline{x} \to x \to X_0$, let $C \to C_0$ be the fiber, which is affine irreducible, so $H^0_c(X, \mathcal{F}) = 0$ by Poincaré duality(8.4.7.51) and Artin vanishing theorem(8.4.2.12), so

$$\iota L(C_0, \mathcal{G}_0, t) = \frac{\iota \det(1 - tF_X^*|H^1_c(C, \mathcal{G}|_C))}{\iota \det(1 - tF_X^*|H^2_c(C, \mathcal{G}|_C))}$$

by Grothendieck-Lefschetz formula(17.2.2.6). Now we can use Poincare duality and the definition that $\mathcal{G}_0$ is pure of weight β, we know $H^2_c(C, \mathcal{G}|_C)$ is pure of weight $\beta+2$, by(17.2.5.3). And $H^2_c(C, \mathcal{G}|_C)$ has weights smaller than $\beta + 1$ by the curve case, so the two polynomial is coprime, and both has constant coefficient 1, which shows they are both real. And then by proper base change(8.4.5.5), this just says $R^i f_{0!}\mathcal{G}_0$ is ι-real. □

Third Reduction

Prop. (17.2.6.7). If $X_0 \subset \mathbb{A}^1_{\mathbb{F}_q}$ is a smooth affine curve and $\mathcal{F}_0$ a lisse $\overline{\mathbb{Q}}_\ell$-sheaf, the Deligne's purity theorem is true. ⌟

Proof: We have the following devissages:

- We only need to check for $H^1_c(X, \mathcal{F})$, because H^0_c vanish by Poincaré duality(8.4.7.51) and Artin vanishing theorem(8.4.2.12) and , $H^2_c(X, \mathcal{F})$ is dealt with in(17.2.5.3).
- We are free to pass to finite base change.
- We may assume $\mathcal{F}_0$ is geometrically irreducible: By(17.2.4.4), all the irreducible constituents of $\mathcal{F}_0$ are geometrically semisimple, so pass to a finite base change, we may assume that its irreducible filtration is just the geometric irreducible filtration, then because $H^0_c = 0$, H^1_c is left exact.
- We can assume that $\mathcal{F}_0$ can be extended to a lisse sheaf on ∞. This is because we can choose a closed point and move it to ∞ by using Möbius transform, after a finite base change.

- We can assume $\mathcal{F}_0$ is not geometrically constant: if $\mathcal{F}_0 \cong \underline{\overline{\mathbb{Q}}_\ell}$, then let $i : U_0 \to P^1_{\mathbb{F}_q}$ and $Z_0 = P^1_{\mathbb{F}_q} - U_0$, then there is a short exact sequence

$$0 \to j_{0!}(\underline{\overline{\mathbb{Q}}_\ell}) \to j_*(\underline{\overline{\mathbb{Q}}_\ell}) \to \mathcal{Q} \to 0$$

where $\mathcal{Q}$ is supported at S, so its higher compact cohomology vanish, and weights of $H^0(\mathcal{Q}) = \prod_{s\in S}(j_{0*}(\mathcal{F}_0))_{\overline{s}}$ is no more than the maximal weight of $\underline{\overline{\mathbb{Q}}_\ell}$ on X_0, which is 0, by semicontinuity of weights for curves(17.2.3.11). And $j_*(\underline{\overline{\mathbb{Q}}_\ell})$ is also geometrically constant, thus its cohomology is $\mathrm{Pic}(\mathbb{P}^1)[n] = 0$ by(8.4.7.42), so $H^1(P^1, j_{0!}(X_0))$ has weights zero.

The actual proof will use the following lemma(17.2.6.8). After that, notice by(17.2.8.6)

$$(T_\psi(G_0))|_{\{0\}} = R\Gamma_c(\mathbb{A}^1, \mathcal{G})[1] = R\Gamma_c(U, \mathcal{F})[1] = H^1_c(U, \mathcal{F})$$

Then to understand the Frobenius eigenvalues of $H^1_c(U, \mathcal{F})$, it suffices to understand the weights of $T_\psi(\mathcal{G}_0)$, i.e.

$$w(T_\psi(\mathcal{G}_0)) \le w + 1$$

Then we use(17.2.3.17), notice the condition is satisfied by lemma(17.2.6.8), so $w(T_\psi(\mathcal{G}_0)) = ||T_\psi(\mathcal{G}_0)||$, and also $w(G_0) = ||G_0||$ for the same reason as $H^0_c(\mathbb{A}^1, \mathcal{G}) = H^0_c(U, \mathcal{F}) = 0$ by Poincare duality. Now(17.2.8.10) gives the result.

□

Lemma (17.2.6.8) [Key Assertions of Weil Proof]. If $\mathcal{G}_0 = j_{0!}(\mathcal{F}_0)$ where $j_0 : U_0 \hookrightarrow A^1_{\mathbb{F}_q}$, $\psi : \mathbb{F}_q \to \overline{\mathbb{Q}}_\ell$ is a fixed non-trivial additive character, then

- $T_\psi(\mathcal{G}_0)$ is a sheaf placed at degree 0.
- $H^0_c(\mathbb{A}^1, T_\psi(\mathcal{G}_0)) = 0$.
- $T_\psi(\mathcal{G}_0)$ is ι-mixed.

┘

Proof: 1: By(17.2.8.6), we need to show $H^i_c(\mathbb{A}^1, \mathcal{G}_0 \otimes \mathcal{L}(\psi_a)) = 0$ for $i \neq 1$, and this is equivalent to

$$H^i_c(\mathbb{A}^1, j_!\mathcal{F} \otimes \mathcal{L}(\psi_a)) = H^i_c(U, F \otimes \mathcal{L}(\psi_a)) = 0.$$

Notice by vanishing result(8.4.5.6), only need to show $i = 0, i = 2$, $i = 0$ case is done by Poincare duality(8.4.7.51) and Artin vanishing(8.4.2.12) because it is smooth and $\mathcal{F}$ is lisse.

$H^2_c(\mathcal{G}_0 \otimes \mathcal{L}(\psi_a)) = V_{\rho\otimes\chi_a}|_{\pi_1(U,\overline{x})}(-1)$ by(17.2.5.3), and $\rho \otimes \chi_a$ irreducible as ρ does, so if $V_{\rho\otimes\chi_a}|_{\pi_1(U,\overline{x})} \neq 0$, then $\rho \otimes \psi_a$ is trivial representation. Then $\mathcal{G} \cong \mathcal{L}_{\psi_{-a}}$ on $\mathbb{P}^1_{\overline{k}}$ as an étale sheaf on $\mathbb{A}^1 \cup \{\infty\} = \mathbb{P}^1$ by our reduction, so we have the character ψ_{-a} factors through $\pi_1(\mathbb{P}^1, \overline{x})$, i.e.

$$\begin{array}{ccccc} \pi_1(\mathbb{A}^1, \overline{x}) & \longrightarrow & \pi_1(\mathbb{P}^1, \overline{x}) = 0 & & \\ \downarrow & & \downarrow & & \\ \pi_1(\mathbb{A}^1_0, \overline{x}) & \longrightarrow & \pi_1(\mathbb{P}^1_0, \overline{x}) & \xrightarrow{\psi_{-a}} & \overline{\mathbb{Q}}_\ell \end{array}.$$

But this is in contradiction with the fact the Artin-Schreier cover is geometrically irreducible**?**.

2: Denote $T_\psi(\mathcal{G}_0) = \mathcal{K}_0$, then by(17.2.8.5) and Fourier inversion(17.2.8.8):

$$H^0_c(\mathbb{A}^1, \mathcal{K}) = \mathcal{H}^{-1}((T_{\psi^{-1}}(\mathcal{K}_0))_0) = \mathcal{H}^{-1}(T_{\psi^{-1}} \circ T_\psi(j_{0!}(\mathcal{F}_0))_0) = \mathcal{H}^{-1}(j_{0!}(\mathcal{F}_0)(-1))_0 = 0$$

because $\mathcal{F}_0$ is placed at degree 0.

3: To show ι-mixed, the only thing we can do it show it is embedded in a ι-real sheaf: Consider the ι-real sheaf

$$\mathcal{H}_0 = \mathrm{pr}_2^*(j_{0!}\mathcal{F}_0) \otimes m^*(\mathcal{L}(\psi)) \oplus \mathrm{pr}_2^*(j_{0!}\mathcal{F}_0^\vee) \otimes m^*(\mathcal{L}(\psi^{-1}))(-w)$$

Then

$$(R^i\pi_!^1(\mathcal{H}_0))_{\overline{x}} = H^i(\{\overline{x}\} \times \mathbb{A}^1, \mathcal{H}_0) = H^i(j_{0!}\mathcal{F}_0 \otimes \mathcal{L}(\psi_x)) \oplus H^i(j_{0!}\mathcal{F}_0^\vee \otimes \mathcal{L}(\psi_{x^{-1}}^{-1}))(-w)$$

which we proved to vanish for $i \neq 1$. So using Poincare duality on $\{\overline{x}\} \times \mathbb{A}^1$,

$$\det(1-tF_x^{d_x}|(R^1\pi_!^1(\mathcal{H}_0)_{\overline{x}})) = \det(1-tF_X|H_c^1(\{\overline{x}\}\times\mathbb{A}^1, H_0|_{\{\overline{x}\}\times\mathbb{A}^1})) = \prod_{y\in\mathbb{F}_{q^n}} \det(1-tF_y^{d_y}|(\mathcal{H}_0)_{\overline{(x,y)}})^{-1}$$

which is real, so by(17.2.5.5), the direct summand $T_\psi(\mathcal{G}_0)$ is ι-mixed. □

Remark (17.2.6.9). If we use the machinery of perverse sheaf and show that Fourier transform preserves perversity, then item1, 2 will be a direct consequence, Cf.[Bhatt notes, P39]. In fact, this is just the bigger picture, given in [Weil conjectures Perverse Sheaves and l-adic Fourier Transform Kiehl/Weissauer]. ⌟

7 Semisimplicity and Hard Lefschetz

Prop. (17.2.7.1) [Semisimplicity Theorem]. If X_0 is smooth and $\mathcal{F}_0$ is a lisse and ι-pure $\overline{\mathbb{Q}}_\ell$-sheaf, then $\mathcal{F}_0$ is semisimple, thus geometrically semisimple by(17.2.4.4) . ⌟

Proof: Let $\mathcal{F}'$ be the sum of irreducible lisse subsheaves of $\mathcal{F}$, then it is the largest semisimple subsheaf of $\mathcal{F}$. It is stable under $G(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, thus can be descended to a lisse subsheaf $\mathcal{F}_0'$ of $\mathcal{F}_0$, and let $\mathcal{F}'' = \mathcal{F}_0/\mathcal{F}_0'$, we want to show the exact sequence

$$0 \to \mathcal{F}_0' \to \mathcal{F}_0 \to \mathcal{F}_0'' \to 0$$

splits geometrically. Notice this exact sequence defines an element in $\mathrm{Ext}_X^1(\mathcal{F}'', \mathcal{F}') = H^1(X, (\mathcal{F}'')^\vee \otimes \mathcal{F}')$**?**. $\mathcal{F}_0$ is pure, hence so does $(\mathcal{F}_0'')^\vee \otimes \mathcal{F}_0'$, thus $H^1(X, (\mathcal{F}'')^\vee \otimes \mathcal{F}')$ is ι-mixed of weights≥ 1. But the exact sequence is compatible with Frobenius action, it defines a Frobenius fixed element, which then must vanish. □

Cor. (17.2.7.2). If $f : X \to Y$ is proper between smooth algebraic schemes, then the sheaves $R^i f_* \mathbb{Q}_\ell$ are semisimple. ⌟

<u>Hard Lefschetz</u>

Def. (17.2.7.3). The setup is k is a finite field, $F \in \mathtt{Field}^0$ and $\mathscr{H}$ is a cohomology theory $\mathcal{S}m\mathcal{P}roj/k \to \mathcal{CR}ing^{gr}/F$ which satisfies

- (Poincaré duality)$\mathscr{H}^i(X) \otimes_F \mathscr{H}^{2n-i}(X) \to \mathscr{H}^{2n}(X)$ is a perfect pairing, and the Frobenius $F_X^* = q^n$ on $\mathscr{H}^{2n}(X)$.
- (Weak Lefschetz)If $\mathcal{L}$ is an ample line bundle on X and $H \subset X$ is a smooth divisor in $|\mathcal{L}|$, then

$$f^* : \mathscr{H}^i(X) \to \mathscr{H}^i(Y)$$

  is an isomorphism for $i = n-2$ and injective for $i = n-1$.

- (Zeta Function)Let $\mathscr{P}^i(X;T)=\det(1-F_X^*T|\mathscr{H}^i(X))$, then the Hasse-Weil zeta function

$$Z(X;T)=\prod_{i=0}^{2n}\mathscr{P}(X;T)^{(-1)^{i+1}}.$$

⌟

Prop. (17.2.7.4). Crystalline and ℓ-adic cohomologies satisfy the hypothesis(17.2.7.3). ⌟

Proof: □

Prop. (17.2.7.5). Situation as in(17.2.7.3), then $\mathscr{P}^i(X;T)=P^i_{\text{ét}}(X;T)$. ⌟

Proof: ? □

Cor. (17.2.7.6).

- The characteristic polynomial $P_{\text{ét}}(X;T)$ is independent of ℓ chosen.
- $\dim_F\mathscr{H}^i(X)=\dim_{\mathbb{Q}_\ell}\mathrm{H}^i_{\text{ét}}(X)$.
- (Hard Lefschetz)If $\mathcal{L}$ is an ample line bundle on X, then

$$\mathscr{H}^{n-i}(X)\xrightarrow{c_1(\mathcal{L})^i}\mathscr{H}^{n+i}(X)$$

is an isomorphism.

⌟

Cor. (17.2.7.7).

$$b_d\geq b_{d-2}\geq\ldots,\quad b_{d-1}\geq b_{d-3}\geq\ldots$$

⌟

Prop. (17.2.7.8) [Hard-Lefschetz]. Cf.[Bhatt P42]. ⌟

8 Deligne-Fourier Transformation

Sheaf to Functions Correspondence

Def. (17.2.8.1) [Sheaf to Functions Correspondence]. For a complex $K_0\in D^b_{cons}(X_0,\overline{\mathbb{Q}}_\ell)$, we can associate a function

$$f^{K_0}:X_0(\mathbb{F}_{q^n})\to\overline{\mathbb{Q}}_\ell:x_0\mapsto\mathrm{tr}((F_{x_0}^*)^{n/d_x}|(K_0)_{\overline{x}})=\mathrm{tr}((\varphi_{x_0}^{-1})^{n/\deg(x_0)}|(K_0)_{\overline{x}})(17.2.1.4).$$

⌟

Prop. (17.2.8.2). We can use Grothendieck formula for a constructible sheaf(17.2.2.6) to relate the function f^{K_0} to the compact cohomologies of $\mathcal{H}^iK_0$, and we can translate many know theorems:

- $f^{f^*K_0}=f^{K_0}\circ f$.
- $$f^{K_0}\cdot f^{T_0}=f^{K_0\otimes^L T_0}?$$

- (Base Change)(8.4.5.5) asserts that given a Cartesian diagram

$$\begin{array}{ccc} X' & \xrightarrow{g'} & X \\ \downarrow{f'} & & \downarrow{f} \\ Y' & \xrightarrow{g} & Y \end{array}$$

  then it says in case Y' is a closed point of Y,

$$f^{Rf_!K_0}(y) = \sum_{x\in X_y(\mathbb{F}_{q^n})} f^{K_0}(x)$$

  where $y \in Y(\mathbb{F}_{q^n})$, and more generally

$$\sum_{x'\in X'_{y'}} f^{K_0}(g'(x')) = \sum_{x\in X_{g(y')}} f^{K_0}(x)$$

- The projection formula(8.4.5.8) turns out to say something trivial:

$$\sum_{x\in X_y} (f^{K_0}(f(x)) \cdot f^{T_0}(x)) = f^{K_0}(y) \cdot (\sum_{x\in X_y} f^{T_0}(x))$$

⌟

Prop. (17.2.8.3). $f^{\mathcal{L}_0(\psi)}(x) = \psi(-x)$, by(8.4.7.32). ⌟

Deligne-Fourier Transforms on $\mathbb{A}^1$

Use notations as in Artin-Schreier Theory.

Def. (17.2.8.4) [Deligne-Fourier Transform]. Consider the multiplication map $m : \mathbb{A}_0 \times \mathbb{A}'_0 \to \mathbb{A}_0$, let the sheaf $\mathcal{L}(\psi)$ be placed at A_0, and $K_0 \in D^b_c(\mathbb{A}'_0, \overline{\mathbb{Q}}_\ell)$ be placed at $\mathbb{A}'_0$, then define the **Deligne-Fourier transform**

$$T_\psi : D^b_c(\mathbb{A}'_0, \overline{\mathbb{Q}}_\ell) \to D^b_c(\mathbb{A}_0, \overline{\mathbb{Q}}_\ell) : K_0 \mapsto R\pi^1_!(\mathrm{pr}_2^* K_0 \otimes^L m^*\mathcal{L}_0(\psi))[1]$$

⌟

Lemma (17.2.8.5). $f^{T_\psi K_0}(x) = -\sum_{y\in\mathbb{F}_{q^n}} f^{K_0}(y)\psi^{-1}(xy)$ for any $x \in \mathbb{F}_{q^n}$. ⌟

Proof: By(17.2.8.2),

$$\begin{aligned} f^{T_\psi K_0}(x) &= \sum_{y\in\mathbb{F}_{q^n}} f^{(\mathrm{pr}_2^* K_0\otimes^L m^*\mathcal{L}_0(\psi))[1]}((x,y)) \\ &= -\sum_{y\in\mathbb{F}_{q^n}} f^{\mathrm{pr}_2^* K_0}((x,y)) \cdot f^{m^*\mathcal{L}_0(\psi)}((x,y)) \\ (17.2.8.3) &= -\sum_{y\in\mathbb{F}_{q^n}} f^{K_0}(y)\psi(-xy). \end{aligned}$$

□

Prop. (17.2.8.6). For $a \in \mathbb{A}^1(\mathbb{F}_{q^n})$,

$$(T_\psi(K_0))_a = R\Gamma_c(K \otimes^{\mathrm{L}} \mathcal{L}(\psi_a))[1]$$

where $\psi_a : \mathbb{F}_{q^n} \to \overline{\mathbb{Q}}_\ell^\times$ maps $x \mapsto \psi(ax)$. In particular, $\mathcal{H}^i((T_\psi(K_0))_0) = H^i_{\text{ét},c}(\mathbb{A}^1, K)$, so we placed the complex into a family of deformations. ⌟

Proof: By base change(8.4.5.5),

$$(T_\psi(K_0))_a = R\Gamma_c((\mathrm{pr}_2^* K_0 \otimes^L m^*\mathcal{L}_0(\psi)|_{\{a\}\times\mathbb{A}^1})[1] = R\Gamma_c(K \otimes^L \mathcal{L}(\psi_a))[1].$$

□

Lemma (17.2.8.7). If $\delta_0 = i_{0*}\overline{\mathbb{Q}}_\ell$ is the skyscraper sheaf where $i_0 : \{0\} \hookrightarrow \mathbb{A}^1$, then

$$T_\psi(\overline{\mathbb{Q}}_\ell[1]) = \delta_0(-1).$$

⌟

Proof: For the Artin-Schreier cover $\wp : x \mapsto x^q - x$, by(8.4.7.31),

$$\wp_*\overline{\mathbb{Q}}_\ell \cong \bigoplus_{x\in\mathbb{F}_q} \mathcal{L}(\psi_x).$$

As $\wp$ is finite, $\wp_*$ is exact(8.4.1.18), so using the Leray spectral sequence(8.4.5.5), we can calculate

$$H^1_c(\mathbb{A}^1, \mathcal{L}(\psi_x)) = 0 = H^1_c(\mathbb{A}^1, \overline{\mathbb{Q}}_\ell), \quad H^2_c(\mathbb{A}^1, \mathcal{L}(\psi_x)) = 0\text{(8.4.5.7)}, \quad H^2_c(\mathbb{A}^1, \mathcal{L}(\psi_x)) = \delta_0(x)\overline{\mathbb{Q}}_\ell(-1)\text{(17.2.5.3)}$$

So

$$(R\pi^1_!(m^*\mathcal{L}_0(\psi)[1])[1])_x = R\Gamma_c(\mathcal{L}(\psi_x))[2] = \delta_0(-1).$$

□

Prop. (17.2.8.8) [Fourier Inversion]. For $K_0 \in D^b_c(\mathbb{A}_0, \overline{\mathbb{Q}}_\ell)$, $T_{\psi^{-1}}T_\psi(K_0) = K_0(-1)$. ⌟

Proof: Consider

$$\begin{array}{ccccc}
\mathbb{A}^1_0 \times \mathbb{A}^1_0 \times \mathbb{A}^1_0 & \xrightarrow{\mathrm{pr}_{23}} & \mathbb{A}^1_0 \times \mathbb{A}^1_0 & \xrightarrow{\mathrm{pr}_2} & \mathbb{A}^1_0 \\
\downarrow \mathrm{pr}_{12} & & \downarrow \mathrm{pr}_1 & & \\
\mathbb{A}^1_0 \times \mathbb{A}^1_0 & \xrightarrow{\mathrm{pr}_2} & \mathbb{A}^1_0 & & \\
\downarrow \mathrm{pr}_1 & & & & \\
\mathbb{A}^1_0 & & & &
\end{array}$$

And we will use the following Cartesian diagrams:

$$\begin{array}{ccc}
\mathbb{A}^3_0 & \xrightarrow{\alpha:(x,y,z)\mapsto(y,z-x)} & \mathbb{A}^2_0 \\
\downarrow \pi^{13} & & \downarrow \mathrm{pr}_2 \\
A^2_0 & \xrightarrow{\beta:(x,z)\mapsto z-x} & A^1_0
\end{array}, \qquad
\begin{array}{ccc}
A^1_0 & \longrightarrow & * \\
\downarrow \Delta & & \downarrow i_0 \\
A^2_0 & \xrightarrow{\beta} & A^1_0
\end{array}$$

Then

$T_{\psi^{-1}}T_\psi K_0$ $\qquad$ $(T_{\psi^{-1}}T_\psi f)(x)$

$= R\pi^1_!(\mathrm{pr}_2^* R\pi^1_!(\mathrm{pr}_2^* K_0 \otimes m^*\mathcal{L}_0(\psi)) \otimes m^*\mathcal{L}_0(\psi^{-1}))[2]$ $\qquad = \sum_y (\sum_z f(z)\psi(-yz))\psi(xy)$

By base change(8.4.5.5) :

$= R\pi^1_!(R\pi^{12}_! \mathrm{pr}_{23}^*(\mathrm{pr}_2^* K_0 \otimes m^*\mathcal{L}_0(\psi)) \otimes m^*\mathcal{L}_0(\psi^{-1}))[2]$

By projection formula(8.4.5.5) :

$= R\pi^1_! R\pi^{12}_!(\mathrm{pr}_{23}^*(\mathrm{pr}_2^* K_0 \otimes m^*\mathcal{L}_0(\psi) \otimes \mathrm{pr}_{12}^* m^*\mathcal{L}_0(\psi^{-1})))[2]$ $\qquad = \sum_y \sum_z f(z)\psi(-yz)\psi(xy)$

Combine the character:

$= R\pi^1_! R\pi^{12}_!(\mathrm{pr}_{23}^* \mathrm{pr}_2^* K_0 \otimes \alpha^* m^*\mathcal{L}_0(\psi))[2]$ $\qquad = \sum_y \sum_z f(z)\psi(-y(z-x))$

Change order of summation:

$= R\pi^1_! R\pi^{13}_!(\pi^{13*} \mathrm{pr}_2^* K_0 \otimes \alpha^* m^*\mathcal{L}_0(\psi))[2]$ $\qquad = \sum_z \sum_y f(z)\psi(-y(z-x))$

By projection formula:

$= R\pi^1_!(\mathrm{pr}_2^* K_0 \otimes R\pi^{13}_1 \alpha^* m^*\mathcal{L}_0(\psi))[2]$ $\qquad = \sum_z f(z) \sum_y \psi(-y(z-x))$

By base change:

$= R\pi^1_!(\mathrm{pr}_2^* K_0 \otimes \beta^* R\pi^2_!(m^*\mathcal{L}_0(\psi))[2] = R\pi^1_!(\mathrm{pr}_2^* K_0 \otimes \beta^* T_\psi \overline{\mathbb{Q}}_\ell[-1])[2]$

By(17.2.8.7) :

$= R\pi^1_!(\mathrm{pr}_2^* K_0 \otimes \beta^* \delta_0[-2])[2] = R\pi^1_!(\mathrm{pr}_2^* K_0 \otimes \beta^* \delta_0(-1))$ $\qquad = \sum_z f(z) q^n \delta_0(z-x)$

Use base change and noticing$i_0$is finite thus proper and exact:

$= R\pi^1_!(\mathrm{pr}_2^* K_0 \otimes R\Delta_! \overline{\mathbb{Q}}_\ell(-1))$ $\qquad = \sum_z \sum_{x=z} q^n$

By projection formula:

$= R\pi^1_! R\Delta_!(\Delta^* \mathrm{pr}_2^* K_0 \otimes \overline{\mathbb{Q}_\ell})(-1)$ $\qquad = q^n \sum_{\{z|z=x\}} f(z)$

$= K_0(-1)$ $\qquad = q^n f(x)$

□

Prop. (17.2.8.9) [Plancherel Formula].

$$||f^{T_\psi(K_0)}||_n = q^{n/2}||f^{K_0}||_n.$$

⌟

Proof: By definition and using(17.2.8.5),

$$\begin{aligned} ||f^{T_\psi(K_0)}||_n^2 &= \sum_{x\in\mathbb{F}_{q^n}} f^{T_\psi(K_0)}(x)\overline{f^{T_\psi(K_0)}(x)} \\ &= \sum_{x,y,z} f^{K_0}(y)\overline{f^{K_0}(z)}\psi(-xy)\psi(xz) \\ &= q^n \sum_{z=y} f^{K_0}(y)\overline{f^{K_0}(z)} \end{aligned}$$

$$= q^n (f, f)_n$$

□

Cor. (17.2.8.10). Notice by the definition of norm of a Weil-sheaf $\mathcal{G}_0$, we have

$$||T_\psi(K_0)|| \leq ||K_0|| + 1$$

⌟

9 Integrality Problems

Def. (17.2.9.1) [Integral Sheaves]. Let X_0 be a separated algebraic scheme over k and $\mathcal{F}_0$ a lisse constructible sheaf on X_0, then $\mathcal{F}_0$ is called an **integral lisse sheaf** if for all $x_0 \in X_0$, all the eigenvalues of F_x^* acting on $\mathcal{F}_{\overline{x}}$ are algebraic integers. ⌟

Prop. (17.2.9.2) [Deligne]. If $\mathcal{F}_0$ is an integral lisse sheaf(17.2.9.1) on X_0, then all coefficients of $H^i_{\text{ét},c}(X, \mathcal{F})$ are integral. ⌟

Proof: Cf.[Weil 1 Proof, P21]. □

Cor. (17.2.9.3). All eigenvalues of $H^i_{\text{ét},c}(X, \mathcal{F})$ are algebraic integers. ⌟

17.3 Trigonometric Sums

References are [Kats's work] and [Weil conjectures and Fourier transform].

1 Katz's Trigonometric Sums

Def. (17.3.1.1) [Generalized Trigonometric Sums]. For $p \in \mathbf{P}, q \in p^{\mathbb{Z}}$, $\psi \neq 1 \in \chi(\mathbb{F}_q)$, and $h : X \to \mathbb{A}^1_{\mathbb{F}_q} \in \mathcal{S}\mathrm{ch}^{\mathrm{fg}}/\mathbb{A}^1_{\mathbb{F}_q}$, the generalized **trigonometric sum** is defined to be the exponential sum

$$\sum_{x \in X(\mathbb{F}_q)} \psi(h(x)).$$

⌟

Thm. (17.3.1.2) [Katz]. Let $h : X \to \mathbb{A}^1 \in \mathcal{S}\mathrm{ch}^{\mathrm{fg}}/\mathbb{A}^1$, then there exists $C \in \mathbb{R}_+$ s.t. for any $p \in \mathbf{P}$ and $q \in p^{\mathbb{Z}_+}, \psi \neq 1 \in \chi(\mathbb{F}_q)$,

$$|\sum_{x \in A(\mathbb{F}_q)} \psi(h(x))| \leq C q^{N + \frac{1}{2}},$$

where N is the supremum of the dimension of the fiber of $h_{\mathbb{C}}$.

And if moreover the generic fiber $h_{\overline{\eta}}$ is geo.irreducible or has dimension$< N$, then for any $p \in \mathbf{P}$ and $q \in p^{\mathbb{Z}_+}, \psi \neq 1 \in \chi(\mathbb{F}_q)$,

$$|\sum_{x \in A(\mathbb{F}_q)} \psi(h(x))| \leq C q^{N}.$$

⌟

Proof: Cf.[K-W01]P228. □

2 Gauss Sums

Def. (17.3.2.1) [Gauss Sums and Heilbronn Sums]. For $p \in \mathbf{P}$ and $f(X) \in \mathbb{Z}[X]$, a **Gauss sum** is a summation

$$G_p(f) = \sum_{n=1}^{p} e^{2\pi\,\mathrm{i}\, f(n)/p}.$$

A special case is the summation

$$G_p(a,k) = G_p(aX^k) = \sum_{n=1}^{p} e^{2\pi\,\mathrm{i}\, an^k/p}$$

where $k \in \mathbb{Z}_+, a \in \mathbb{Z} \setminus (p)$.

And a **Heilbronn sum** is the summation

$$H_p(a) = e^{2\pi\,\mathrm{i}\, an^p/p^2}.$$

Notice if $k_0 = \gcd(k, p-1)$, then $G_p(a,k) = G_p(a,k_0)$. Thus for $G_p(a,k)$, we always assume $k|p-1$. ⌟

Prop. (17.3.2.2). For $p \in \mathbf{P}_{\geq 3}, a, b, c \in \mathbb{Z}$ and $(a,p) = 1$,

$$|\sum_{t=0}^{p-1} e^{2\pi\,\mathrm{i}\, \frac{at^2+bt+c}{p}}| = \sqrt{p}.$$

⌟

Proof: It is easy to reduce to the case $b=c=0$. Then

$$\Big|\sum_{t=0}^{p-1} e^{2\pi\,\mathrm{i}\,\frac{at^2}{p}}\Big|^2 = \sum_{t=0}^{p-1}\sum_{s=0}^{p-1} e^{2\pi\,\mathrm{i}\,\frac{a(t^2-s^2)}{p}} = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} e^{2\pi\,\mathrm{i}\,\frac{axy}{p}} = p.$$

□

Prop. (17.3.2.3). For $p\in\mathbf{P}_{\geq 3}, n\in\mathbb{Z}_+, a\in\mathbb{Z}$,

$$\Big|\sum_{t=1}^{p^{n+1}} e^{2\pi\,\mathrm{i}[\frac{at^2}{p}+\frac{ht}{p^{n+1}}]}\Big| = \begin{cases} p^{n+\frac{1}{2}} & ,p^n|h, p\nmid a\\ 0 & ,p^n\nmid h\end{cases}.$$

⌟

Proof:

$$\sum_{t=1}^{p^{n+1}} e^{2\pi\,\mathrm{i}[\frac{at^2}{p}+\frac{ht}{p^{n+1}}]} = \sum_{t=1}^{p} e^{2\pi\,\mathrm{i}[\frac{at^2}{p}+\frac{ht}{p^{n+1}}]}\Big(\sum_{r=1}^{p^n} e^{2\pi\,\mathrm{i}\,\frac{hr}{p^n}}\Big).$$

Then the assertion follows from(17.3.2.2). □

Prop. (17.3.2.4) [Burgess]. For $p\in\texttt{Prime}, s\in\mathbb{Z}_+$ and $b_1,\ldots,b_s\in\mathbb{F}_p$,

$$\Big|\sum_{x\in\mathbb{F}_p}\Big(\frac{\prod_i(x+b_i)}{p}\Big)\Big|\leq s^2\sqrt{p},$$

unless $s\in 2\mathbb{Z}_+$ and up to permutation $b_1=b_2, b_3=b_4,\ldots,b_{s-1}=b_s$. ⌟

Proof: This is clear for $s=1$, and for $s\geq 2$, use Weil conjecture on the the hyperelliptic curve

$$y^2=\prod_i(x+b_i).$$

□

Prop. (17.3.2.5) [Burgess Multiplicative Character Bound]. For any $\beta\in\mathbb{R}_{>1/4}$, there exists $C(\beta), e(\beta)\in\mathbb{R}_+$ s.t. for any $\chi:\mathbb{F}_p^\times\to\mathbb{C}^\times$ and $x_0\in\mathbb{Z}$,

$$\Big|\sum_{x=x_0}^{x_0+N-1}\chi(x)\Big|\leq C(\beta)N^{1-e(\beta)}.$$

⌟

Proof: ? □

Cor. (17.3.2.6). For any $\varepsilon\in\mathbb{R}_+$, there exists $C(\varepsilon)\in\mathbb{R}_+$ s.t. for any $p\in\texttt{Prime}$, any interval of length $C(\varepsilon)p^{1/4+\varepsilon}$ contains a square and a non-square. ⌟

Thm. (17.3.2.7) [Weil]. For $p\in\mathbf{P}$ and $f(X)\in\mathbb{F}_p[X]$ with $\deg(f)=k$,

$$|G_p(f)|\leq k\sqrt{p}.$$

⌟

Proof: Cf.[Larry Guth]P56, and a weaker bound is found in [Larry Guth]P62. □

Monomial Gauss Sums and Heilbronn Sums

Conj. (17.3.2.8).

$$|G_p(a,k)| \le \min\Big((k-1)\sqrt{p}, (1+\eta)\sqrt{2kp\log(kp)}\Big),$$

where $\eta \to 0$ as k and p/k both tend to infty. ⌟

Proof: □

Prop. (17.3.2.9).

$$|G_p(a,k)| \le \min(p, (k-1)\sqrt{p}).$$

⌟

Proof: $|G_p(a,k)| \le p$ is trivial. For the second assertion, notice

$$G_p(a,k) = \sum_{\chi \in \mathrm{Diri}(p), \chi^k = \mathbf{1}, \chi \neq \mathbf{1}} \chi^{-1}(a)\tau(\chi)(17.3.3.3),$$

and use the fact $|\tau(\chi)| = \sqrt{p}$ for each χ. □

Thm. (17.3.2.10) [Heath.Brown-Konyagin]. Situation as in(17.3.2.1),

$$G_p(a,k) = O(\min(k^{5/8}p^{5/8}, k^{3/8}p^{3/4})).$$

⌟

Proof: Cf.[B-K20]P223. □

Lemma (17.3.2.11). Situation as in(17.3.2.1), if $h = (p-1)/k$, and

$$A(h) = \{(x_1, \ldots, x_4) \in \mu_h(\mathbb{Z}_p)^4 | x_1 + x_2 = x_3 + x_4\},$$

then

$$|G_p(a,k)| \le \min(k^{4/5}, p^{1/8})(\#A(h))^{1/4}.$$

⌟

Proof: Cf.[B-K20]P224. □

Lemma (17.3.2.12). Situation as in(17.3.2.11), if $h < p^{2/3}$, then $\#A(h) = O(h^{5/2})$. ⌟

Proof: Cf.[B-K20]P225. □

Thm. (17.3.2.13) [Heath.Brown-Konyagin]. Situation as in(17.3.2.1),

$$\sum_{r=1}^{p} |H_p(a+rp)|^4 = O(p^{7/2}),$$

in particular,

$$H_p(a) = O(p^{7/8}).$$

⌟

Proof: □

Lemma (17.3.2.14). Situation as in(17.3.2.1), if

$$f(X) = X + \frac{X^2}{2} + \ldots + \frac{X^{p-1}}{p-1} \in \mathbb{Z}_p[X],$$

and

$$B = \{(x_1, x_2) \in \mathbb{Z}_p^2 | f(x_1) = f(x_2)\},$$

then

$$\sum_{r=1}^{p} |H_p(a+rp)|^4 = O(p^3 + p^2 \# B).$$

⌟

Proof: Cf.[B-K20]P224. □

Lemma (17.3.2.15). Situation as in(17.3.2.14), then $\# B = O(p^{3/2})$. ⌟

Proof: Cf.[B-K20]P225. □

3 Dirichlet Characters

Def. (17.3.3.1) [Dirichlet Character]. For $F \in \mathtt{NField}$ and a modulus $\mathfrak{m}$ for F, a **Dirichlet character modulo** $\mathfrak{m}$ is a functor $\mathrm{Cl}_{\mathfrak{m}}(F) = J^{\mathfrak{m}}/P^{\mathfrak{m}} \to \mathbb{C}^\times$.

A **primitive Dirichlet character** modulo $\mathfrak{m}$ is a Dirichlet character modulo $\mathfrak{m}$ that is injective. The set of Dirichlet characters modulo $\mathfrak{m}$ is denoted by $\mathrm{Diri}(\mathfrak{m})$, and the set of primitive Dirichlet characters modulo $\mathfrak{m}$ is denoted by $\mathrm{Diri}'(\mathfrak{m})$.

Usually we consider the case $F = \mathbb{Q}$ and $\mathfrak{m} = m \cdot \infty$. In which case, a Dirichlet character is just a homomorphism $(\mathbb{Z}/(m))^\times \to \mathbb{C}^\times$. ⌟

Prop. (17.3.3.2) [Kronecker Characters]. For $a \in \mathbb{Z}^\times$, denote $\chi_a \in \mathrm{Diri}(4a)$ the character $\chi_a(m) = \left(\frac{a}{m}\right)$. Notice $\chi_a \neq \mathbf{1}$ if $a \neq 1$. ⌟

Proof: □

Def. (17.3.3.3) [Gauss Sums]. For $\chi \in \mathrm{Diri}(N)$, the **Gauss sum** of χ is defined to be

$$\tau(\chi) = \sum_{n \in \mathbb{Z}/(N)} \chi(n) e^{2\pi \mathrm{i}\, n/N}.$$

⌟

Prop. (17.3.3.4). $\tau(\overline{\chi}) = \chi(-1)\overline{\tau(\chi)}$. ⌟

Prop. (17.3.3.5). $\sum_{n \in \mathbb{Z}/(N)} \chi(n) e^{2\pi \mathrm{i}\, nm/N} = \overline{\chi(m)}\tau(\chi)$(17.3.3.3). ⌟

Proof: If $(m, N) = 1$, then this follows from

$$\tau(\chi) = \sum_{n (\mathrm{mod}\ N)} \chi(mn) e^{2\pi \mathrm{i}\, mn/N} = \chi(m) \sum_{n (\mathrm{mod}\ N)} \chi(n) e^{2\pi \mathrm{i}\, mn/N}.$$

If $(m,N)\neq 1$, then we need to show the LHS is 0. Let $m=dM,N=dN_1$. Because χ is primitive character mod N, there is some $c\equiv 1 \mod N_1$ that $\chi(c)\neq 1$, otherwise χ is defined mod N_1. Notice

$$\sum_{n(\text{mod } N)}\chi(n)e^{2\pi\,\mathrm{i}\,nm/N}=\sum_{r(\text{mod } N_1)}\{\sum_{n(\text{mod } N),n\equiv r(\text{mod } N_1)}\chi(n)\}e^{2\pi\,\mathrm{i}\,rM/N_1}$$

But $r\mapsto cr$ is a permutation of $\{n(\text{mod } N),n\equiv r(\text{mod } N_1)\}$, thus

$$\sum_{n(\text{mod } N),n\equiv r \mod N_1}\chi(n)=\sum_{n \mod N,n\equiv r \mod N_1}\chi(cn)=\chi(c)\sum_{n(\text{mod } N),n\equiv r \mod N_1}\chi(n)$$

which means this sum vanishes. □

Prop. (17.3.3.6). $|\tau(\chi)|^2=N$. ⌟

Proof: For any m,

$$|\sum_{n \mod N}\chi(n)e^{2\pi inm/N}|^2=\sum_{(n_1n_2,N)=1}\chi(n_1)\overline{\chi(n_2)}e^{2\pi i(n_1-n_2)m/N},$$

summing over $m\in(\mathbb{Z}/(N))^*$,

$$\varphi(N)|\tau(\chi)|^2=\sum_{m \mod N}\sum_{(n_1n_2,N)=1}\chi(n_1)\overline{\chi(n_2)}e^{2\pi\,\mathrm{i}(n_1-n_2)m/N}=\sum_{n_1\equiv n_2 \mod N,(n_1n_2,N)=1}N=\varphi(N)N$$

□

Cor. (17.3.3.7). From this and(17.3.3.5) and also(17.3.3.4), we get that

$$\chi(n)=\frac{\chi(1)\tau(\chi)}{N}\sum_{m(\text{mod } N)}\overline{\chi(m)}e^{2\pi imn/N}.$$

⌟

Cor. (17.3.3.8). If χ is real(i.e. $\chi^2=1$), by(17.3.3.4), $\tau(\chi)^2=\chi(-1)N$. ⌟

Cor. (17.3.3.9). For $p\geq 3\in\mathbf{P}$,

$$\tau(\left(\frac{-}{p}\right))^2=\left(\frac{-1}{p}\right)p.$$

More precisely,

$$\tau(\left(\frac{-}{p}\right))^2=\varepsilon_p\sqrt{p},\quad \varepsilon_p=\begin{cases}1 & p\equiv 1(\text{mod } 4)\\ -1 & p\equiv 3(\text{mod } 4)\end{cases}.$$

⌟

Proof: **?** □

Prop. (17.3.3.10) [Finite Fourier Transform]. Let ψ be a non-trivial character on a finite field $\mathbb{F}_q$, then let $g_\psi=\sum_{x\in\mathbb{F}_q}\psi(x^2)$, then

- $|g_\psi|^2=q^{1/2}$.
- $g_\psi(a)=(\frac{a}{\mathbb{F}_q})g_\psi(1)$.

⌟

Proof: Use Fourier transform on $\mathbb{F}_q$**?**. □

4 Kloosterman Sums

References are [K-W01].

Def. (17.3.4.1) [Generalized Kloosterman Sums]. Let $p \in \mathbf{P}, q \in p^{\mathbb{Z}_+}, m \in \mathbb{Z}_+$, and $\psi \in \chi(\mathbb{F}_q)$, then the generalized **Kloosterman sum** is defined to be

$$\mathrm{Kloos}_m(q,\psi,a) = \sum_{x_1,\ldots,x_m\in\mathbb{F}_q^\times, x_1\ldots x_m=a} \psi(x_1+\ldots+x_m) \in \mathbb{C}.$$

And $\mathrm{Kloos}_2(q,\psi,a)$ is denoted by $\mathrm{Kloos}(q,\psi,a)$. ⌟

Thm. (17.3.4.2) [Weil/Deligne]. $|\mathrm{Kloos}_m(q,\psi,a)| \le \min(mq^{\frac{m-1}{2}}, q^{m/2})$. ⌟

Proof: Let $X_0 = \mathrm{Spec}\,\mathbb{F}_q[X_1,\ldots,X_m]/(X_1\ldots X_m = a)$ and $h : X \to \mathbb{A}^1_{\mathbb{F}_q} : (x_1,\ldots,x_m) \mapsto x_1+\ldots+x_m$. Let $\mathcal{L}(\psi^{-1})$ be the Artin-Schreier sheaf on $\mathbb{A}^1_{\mathbb{F}_q}$(8.4.7.30), then by(8.4.7.32), for any $x \in X(\mathbb{F}_q)$, the Frobenius action $F^*_{x_0}$ at x_0 on $h^*(\mathcal{L}(\psi^{-1}))$ is multiplication by $\psi(h(x))$.

Then it follows from(17.2.2.5) that

$$\mathrm{Kloos}_m(q,\psi,a) = \mathrm{tr}(F^*_X) = \mathrm{tr}(F^*_X|[\mathrm{R}\Gamma(X, h^*\mathcal{L}(\psi^{-1}))]).$$

Thus, to show that $|\mathrm{Kloos}_m(q,\psi,a)| \le mq^{\frac{m-1}{2}}$, it suffices to show the following:

- $$\dim H^k_{\text{ét},c}(X_{\overline{\mathbb{F}_q}}, h^*(\mathcal{L}(\psi^{-1}))) = m\delta_{k,m-1}.$$
- $H^{m-1}_{\text{ét},c}(X_{\overline{\mathbb{F}_q}}, h^*(\mathcal{L}(\psi^{-1})))$ is pure of weight $m-1$.

For this, Cf.[Deligne, Applications de la formule des traces aux sommes trigonometriques, in SGA4.5]Thm7.4.?

For the second inequality, Cf.[K-W01]P227.? □

Def. (17.3.4.3) [Kloosterman Sums]. For $m \in \mathbb{Z}_+$ and $u, v \in \mathbb{Z}$, a classical **Kloosterman sum** is defined to be the summation

$$\mathrm{Kloos}(u,v,\mod m) = \sum_{r\in(\mathbb{Z}/m)^*} e^{2\pi\mathrm{i}\,\frac{ur+v[r^{-1}]}{m}} \in \mathbb{C}.$$

⌟

Prop. (17.3.4.4) [Properties of Kloosterman Sums].

- $\mathrm{Kloos}(u,v,\mod m) = \mathrm{Kloos}(v,u,\mod m)$.
- $\mathrm{Kloos}(ac,b,\mod m) = \mathrm{Kloos}(a,bc,\mod m)$ if $(c,m)=1$.
- If $m_1,m_2 \in \mathbb{Z}_+, (m_1,m_2) = 1$, and choose $n_1,n_2 \in \mathbb{Z}$ s.t. $n_1m_1 \equiv 1 \mod m_2$ and $n_2m_2 \equiv 1 (\mod m_1)$, then

$$\mathrm{Kloos}(a,b,\mod m_1m_2) = \mathrm{Kloos}(n_2a,n_2b,\mod m_1)\,\mathrm{Kloos}(n_1a,n_1b,\mod m_2).$$

- If $p \in \mathbf{P}$ and $p|m$, then
$$\mathrm{Kloos}(pa,pb,pm) = p\,\mathrm{Kloos}(a,b,m).$$

⌟

Lemma (17.3.4.5). If $p \in \mathbf{P}, m, n, u, v \in \mathbb{Z}_+$ s.t. $m/2 \le n < m$, and $\gcd(u, v, p) = 1$, then

$$|\operatorname{Kloos}(u, v, \mod p^m)| \le Cp^n,$$

where $C = \begin{cases} 4 & , p = 2 \ \& \ m - n \ge 3 \\ 2 & , \text{otherwise} \end{cases}$. ⌟

Proof: In this case, for $s \in \mathbb{Z} \setminus (p)$ and $t \in \mathbb{Z}$, it is easy to verify that

$$[s + p^n t]^{-1} \equiv [s^{-1}] - p^n [s^{-1}]^2 t (\mod p^m).$$

So

$$\begin{aligned} \operatorname{Kloos}(u, v, \mod p^m) &= \sum_{s \in (\mathbb{Z}/p^n)^*} e^{2\pi \mathrm{i} \frac{us + v[s^{-1}]}{p^m}} \sum_{t=1}^{p^{m-n}} e^{2\pi \mathrm{i} \frac{(u - v[s^{-1}]^2)t}{p^{m-n}}} \\ &\le p^{m-n} \#\{s \in (\mathbb{Z}/p^n)^* | us^2 \equiv v (\mod p^{m-n})\} \\ &= p^m \#\{s \in (\mathbb{Z}/p^{m-n})^* | us^2 \equiv v (\mod p^{m-n})\} \\ &\le Cp^n \end{aligned}$$

where $C = \begin{cases} 4 & , p = 2 \ \& \ m - n \ge 3 \\ 2 & , \text{otherwise} \end{cases}$. □

Thm. (17.3.4.6) [Weil-Estermann]. The Kloosterman sum(17.3.4.3) satisfies

$$|\operatorname{Kloos}(u, v, \mod m)| \le \tau\Big(\frac{m}{(u, v, m)}\Big) \sqrt{\gcd(u, v, m) m}.$$

⌟

Proof: As the assertion is multiplicative in m, by(17.3.4.4), it suffices to show for $m = p^k$, where $p \in \mathbf{P}, k \in \mathbb{Z}_+$. If $\gcd(a, b, p^k) = p^k$, then the assertion is trivial. And if $\gcd(a, b, p^k) < p^k$, then it follows from(17.3.4.4) that we can reduce to the case $\gcd(a, b, p^k) = 1$.

If $p = 2$ and $k = 1$, the assertion is trivial, and if $p = 2$ and $k \ge 2$, then the assertion follows from the lemma(17.3.4.5).

If $p \ge 3$, and $2|k$, then the assertion follows from(17.3.4.5).

So suppose $p \ge 3$ and $2 \nmid k$. If $k = 1$ and $p \nmid uv$, this is just theorem of Weil(17.3.4.2). And if $k = 1$ and $p|uv$, this is also trivial, because $\operatorname{Kloos}(u, v, \mod p) \in \{0, 1\}$.

So suppose $m > 1$ and denote $n = \frac{k-1}{2}$. In this case, for $s \in \mathbb{Z} \setminus (p)$ and $t \in \mathbb{Z}$, it can be verified that

$$[(s + p^n t)^{-1}] \equiv [s^{-1}] - p^n [s^{-1}]^2 t + p^{2n} [s^{-1}]^3 t^2 (\mod p^k).$$

So

$$\operatorname{Kloos}(u, v, \mod p^k) = \sum_{s \in (\mathbb{Z}/p^n)^*} e^{2\pi \mathrm{i} \frac{us + v[s^{-1}]}{p^k}} \Big(\sum_{t \in (\mathbb{Z}/p^{n+1})^*} e^{2\pi \mathrm{i} [\frac{(u - v[s^{-1}]^2)t}{p^{n+1}} + \frac{v[s^{-1}]^3 t^2}{p}]} \Big).$$

It follows from(17.3.2.3) that

$$\sum_{t \in (\mathbb{Z}/p^{n+1})^*} e^{2\pi \mathrm{i} [\frac{(u - v[s^{-1}]^2)t}{p^{n+1}} + \frac{v[s^{-1}]^3 t^2}{p}]} = \begin{cases} p^{n + \frac{1}{2}} & , us^2 \equiv v (\mod p^n), p \nmid v \\ 0 & , us^2 \not\equiv v (\mod p^n) \end{cases}.$$

So

$$\operatorname{Kloos}(u, v, \mod p^k) = p^{n + \frac{1}{2}} \#\{s \in (\mathbb{Z}/p^n)^* | us^2 \equiv v (\mod p^n)\} \le 2p^{n + \frac{1}{2}} = 2p^{\frac{m}{2}}.$$

□

5 Irrational Trigonometric Sums

Conj. (17.3.5.1). Given $k \in \mathbb{Z}_+$, then for any $N \in \mathbb{Z}_+$,

$$\sum_{n=1}^{N} e^{2\pi \mathrm{i}\sqrt{2}n^k} = \widetilde{O}(N^{1/2}).$$

⌟

Proof: □

Def. (17.3.5.2). For $\alpha \in \mathbb{R}$ and $D, N \in \mathbb{Z}_+$, define

$$R_{D,N}(\alpha) = \sum_{d\in\mathbb{Z}_+, d\leq D} \min(N, ||d\alpha||^{-1}).$$

Then this $R_{D,N}$ satisfies:

- $D \leq R_{D,N}(\alpha) \leq DN$.
- If α is (C,μ)-Diophantine, then $R_{D,N}(\alpha) \leq C^{-1}DN^{\mu-2}\log N$.
- $R_{D,N}(\sqrt{2}) \sim D\log N$.

⌟

Proof: □

Thm. (17.3.5.3)[Weyl]. Let $P(X) = \alpha X^k + \sum_{j=1}^{k-1}\alpha_j X^k \in \mathbb{R}[X]$, $N, N_1, N_2 \in \mathbb{Z}_+$, $N_1 < N_2 \leq N_1 + N$, then for each $\delta \in \mathbb{R}_+$, there exists $C(\delta) \in \mathbb{R}_+$ s.t.

$$\Big|\sum_{n=N_1}^{N_2} e^{2\pi \mathrm{i} P(n)}\Big|^{2^{k-1}} \leq C(\delta)N^\delta N^{2^{k-1}-k} R_{k!N^{k-1},N}(\alpha)(17.3.5.2).$$

In particular, if α is μ-Diophantine, then by(17.3.5.2), for each $\delta \in \mathbb{R}_+$, there exists $C'(\delta) \in \mathbb{R}_+$ s.t.

$$\Big|\sum_{n=N_1}^{N_2} e^{2\pi \mathrm{i} P(n)}\Big|^{2^{k-1}} \leq C'(\delta)N^{\delta+\mu-2} N^{2^{k-1}-1}.$$

⌟

Proof: Cf.[Larry Guth]P19. □

Thm. (17.3.5.4) [Vinogradov]. Let $P(X) = \sum_{j=1}^{k}\alpha_j X^k \in \mathbb{R}[X]$, then there exists $C_k \in \mathbb{R}_+$ s.t. for $N \in \mathbb{Z}_+$,

$$|\sum_{n=1}^{N} e^{2\pi \mathrm{i} P(n)}| \leq C_k N^{1-\frac{1}{10k^2\log k}},$$

unless there exists $\frac{a}{q} \in \mathbb{Q}$ s.t. $1 \leq q \leq N$ and

$$|\alpha_k - \frac{a}{q}| \leq \frac{1}{N^{k-1}}.$$

⌟

Proof: Cf.[Larry Guth]P44.?

For $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{R}/\mathbb{Z})^k$, denote

$$W_{k,N}(\alpha) = \sum_{n=1}^{N} e^{2\pi \mathrm{i}\, P_\alpha(n)}, \quad P_\alpha(X) = \alpha_k X^k + \ldots + \alpha_1 X.$$

For $l \in \mathbb{Z}_+$, define the linear operator

$$T_l : (\mathbb{R}/\mathbb{Z})^k \to (\mathbb{R}/\mathbb{Z})^k : P_\alpha(X + l) - P_\alpha(X) = P_{T_l(\alpha)}(X).$$

Notice that for any $s \in \mathbb{Z}_+$,

$$\int_{(\mathbb{R}/\mathbb{Z})^k} |W_{k,N}(\beta)|^{2s} \mathrm{d}\beta = J_{s,k}(N) \overset{\triangle}{=} \#\{(a_1, \ldots, a_s, b_1, \ldots, b_s) \in [N]_+^{2s} | \sum_i a_i^j = \sum_i b_i^j, \forall j \in [1, k]\}.$$

Lemma (17.3.5.5) [W-BDG]. For $s, k, N \in \mathbb{Z}_+$ and $\varepsilon \in \mathbb{R}_+$, there exists $C(k, \varepsilon) \in \mathbb{R}_+$ s.t.

$$J_{k,N}(N) \le C(k, \varepsilon) N^\varepsilon (N^s + N^{2s - \binom{k+1}{2}}).$$

┘

Proof: □

Lemma (17.3.5.6) [Vinogradov]. For $s, k, N \in \mathbb{Z}_+$, there exists $C(k) \in \mathbb{R}_+$ s.t.

$$J_{k,N}(N) \le C(k) N^{2s - \binom{k+1}{2}} + k^{2 - \frac{s}{k^2 \log k}}.$$

┘

Proof: □

Denote

$$\varphi_{s,k} : \mathbb{R}^s \to \mathbb{R}^k : (a_1, \ldots, a_n) \mapsto (\sum_i a_i, \sum_i a_i^2, \ldots, \sum_i a_i^k),$$

Then we have:

Lemma (17.3.5.7). For $\gamma \in \mathbb{R}_+$, a sequence $(a_1, \ldots, a_n) \in \mathbb{R}$ is said to be in WS_γ if $|a_i - a_j| > \gamma$ for any $i \neq j$. Then there exists $C(k, \gamma) \in \mathbb{R}_+$ s.t. for any rectangular R with lengths greater than $1/N$, we have:

$$\#\Big\{(a_1, \ldots, a_k) \in (\frac{\mathbb{Z}}{N})^k \cap [0, 1]^k \cap WS_\gamma | \varphi_{s,k}(\underline{a}) \in R\Big\} \le C(k, \gamma) N^k \operatorname{Vol}(R).$$

┘

Proof: Cf.[Larry Guth]P49.? □

□

17.4 p-adic Modular Forms

Main references are [p-adic Modular Forms]

17.5 Formal and Rigid Geometry

Main references are [Bos15] and [BGR84], but there are other approaches, such as given by Berkovich, or given by Huber, and used in Scholze's work, which is most natural because it behaves well w.r.t. the formal model.

1 Affinoid K-Spaces

Def. (17.5.1.1) [Affinoid K-Space]. an affinoid algebra A can be viewed as the function ring on the space $\operatorname{Sp} A$ of maximal ideals of A with the usual Zariski topology called the **affinoid K-space associated to A**. A morphism of affinoid algebras induce a map on their $\operatorname{Sp} A$. This is because residue fields of maximal ideals are finite over K. So we *define* the category of affinoid K-spaces as the opposite category of affinoid K-algebras. ⌟

Cor. (17.5.1.2). The category of affinoid spaces admits fiber products, because of(11.2.4.30). ⌟

Prop. (17.5.1.3). By the properties of a Jacobson space(4.12.3.24)(4.12.3.21), the affinoid K-space has good properties w.r.t. closed, open hence irreducible compared to $\operatorname{Spec} A$ in Zariski topology. In particular, it is a Noetherian space. ⌟

Def. (17.5.1.4) [Canonical Topology]. The affinoid K-space has another topology, called the **canonical topology**, generated by $X(f,\varepsilon) = \{x | f(x) \leq \varepsilon\}$ as a subbasis. And this topology is in fact generated by $X(f) = X(f,1)$ as a subbasis. ⌟

Proof: For the last assertion, notice $f(x)$ assume value in $|\overline{K}|$, which is dense in $\mathbb{R}_+$, so we can assume $\varepsilon \in |\overline{K}|$(by approximation from below), hence $\varepsilon^n = |c|$, where $c \in K$, so $X(f,\varepsilon) = X(f^n, c) = X(c^{-1}f^n)$. □

Prop. (17.5.1.5). $\{x | f(x) = \varepsilon\}$ is open in $\operatorname{Sp} A$. ⌟

Proof: We let $f(x) = \varepsilon$ and $k = A/\mathfrak{m}_x$, let the minipoly of f in $A/\mathfrak{m}_x$ be P of degree n, and let $g = P(f)$, then $g(x) = 0$, and if $|g(y)| < \varepsilon^n$, then $|f(y)| = \varepsilon$, otherwise $|f(y) - \alpha_i| \geq |\alpha_i| = \varepsilon$ for every root α_i of P, hence $|P(f(y))| \geq \varepsilon^n$, contradiction. □

Cor. (17.5.1.6). By the proof, we have, $X(f_1, \ldots, f_r)$, $f_i \in \mathfrak{m}_x$ forms a basis of x in $\operatorname{Sp} A$.(Replace every $X(f_i)$ by $\{y || f_i(y)| = \varepsilon\}$, then by some $X(g_i)$ for $g_i \in \mathfrak{m}_x$. ⌟

Def. (17.5.1.7) [Affinoid Subdomain]. For an affinoid K-space X, a subset U is called a **affinoid subdomain** of X if there is an closest affinoid space map $X' \to X$ with image in U, i.e. any other these maps factor through it. The definition is weird but the situation is clarified by the following proposition. ⌟

Prop. (17.5.1.8). For an affinoid subdomain $i : X' \to X$,

- i is injective and $\operatorname{Im} i = U$.
- i^* induce an isomorphism $A/\mathfrak{m}_{i(x)}^k \cong A'/\mathfrak{m}_x^k$.
- $\mathfrak{m}_x = \mathfrak{m}_{i(x)} A'$.

⌟

Proof: Consider a point $y \in U$, there is a commutative diagram $\begin{array}{ccc} A & \xrightarrow{i^*} & A' \\ \downarrow & \swarrow_{\alpha} & \downarrow \\ A/\mathfrak{m}_y^n & \xrightarrow{\sigma} & A'/\mathfrak{m}_y^n A' \end{array}$. Then there is a map $\alpha : A' \to A/\mathfrak{m}_y^n$ that makes the upper diagram commutative by universal property of subdomain, and the lower triangle is commutative by universal properties again. Then we see σ is surjective and notice the kernel of the projection is $\mathfrak{m}_y A'$ is in the kernel of α, thus σ is injective.

Now the case $n = 1$ shows $\mathfrak{m}_y A'$ is maximal, hence i is surjective and the inverse image is just one point. □

Prop. (17.5.1.9) [Special Subdomains]. There are three special affinoid subdomain of X: **Weierstrass domain** $X(f_1, \ldots, f_r)$, **Laurent domain** $X(f_1, \ldots, f_r, g_1^{-1}, \ldots, g_s^{-1})$, **rational domain** $X(\frac{f_1}{f_0}, \ldots, \frac{f_r}{f_0}) = \{x \mid |f_i(x)| \leq |f_0(x)|\}$ for $(f_0, \ldots, f_r) = (1)$. They are all open by(17.5.1.5). ⌟

Proof: The Weierstrass domain corresponds to $A \to A\langle X_1, \ldots, X_r\rangle/(X_i - f_i)$.

The Laurent domain corresponds to $A \to A\langle X_1, \ldots, X_{r+s}\rangle/(X_i - f_i, 1 - X_{r+j} g_j)$.

The rational domain corresponds to $A \to A\langle X_1, \ldots, X_r\rangle/(f_i - f_0 X_i)$.

They are affinoid subdomains is in fact, easily checked. □

Lemma (17.5.1.10). Weierstrass domain are Laurent, and Laurent domain are rational, this is because intersection of rational domains are rational.

Any rational domain is a Weierstrass domain of a Laurent domain. ⌟

Proof: Notice a Laurent subdomain is a finite intersections of $X(\frac{f}{1})$ and $X(\frac{1}{g})$, so it is rational.

For a rational domain U, f_0 is a unit in $\mathcal{O}(U)$, hence its inverse has a bounded value, then $|cf_0| > 1$ for some $c \in K^*$. Hence U is Weirerstrass in $X((cf_0)^{-1})$. □

Cor. (17.5.1.11) [Pullback & Composition of Affinoid Subdomain]. The pullback(hence intersections) of affinoid subdomains is affinoid subdomain and it is just the set-theoretic inverse image, and specialness are preserved.

The affinoid subdomain of an affinoid subdomain is affinoid subdomain, and Weierstrassness and rationalness are preserved(while Laurentness not). ⌟

Proof: Pullback: fiber product exist in the category of affinoid K-spaces, then the universal property is checked. The set-theoretic property follows from(17.5.1.8).

Speciality: Clear.

Transitivity: Clear by universal property.

For the speciality, if $V = X(f_i)$, $U = V(g_j)$ is Weierstrass, then because by(11.2.4.26) A is dense in $A\langle f_i\rangle$, we can replace g_j by elements from A, by adding elements of small sup-norm, because valuation is non-Archimedean. Then $U = X(f_i, g_j)$. For the rational subdomain $V = X(\frac{f_1}{f_0}, \ldots, \frac{f_r}{f_0})$, use(17.5.1.10), it suffices to prove for $U = V(g)$ or $U = V(g^{-1})$. For this, notice the image of $A[f_0^{-1}]$ is dense in $A\langle \frac{f_1}{f_0}, \ldots, \frac{f_r}{f_0}\rangle$, by(11.2.4.26), so as before, we change g that it $g_0 f_0^n g \in A$ for some n. Now

$$V(g) = V \cap \{x \in X \mid |g_0(x)| \leq |f_0^n(x)|\}, \quad V(g^{-1}) = V \cap \{x \in X \mid |g_0(x)| \geq |f_0^n(x)|\}.$$

But now f_0^n is a unit in $A\langle \frac{f_1}{f_0}, \ldots, \frac{f_r}{f_0}\rangle$, so $|f(x)|_{\sup} \geq |c|$ for some $c \in K^*$, so

$$V(g) = V \cap X(\frac{g_0}{f_0^n}, \frac{c}{f_0^n}), \quad V(g^{-1}) = V \cap X(\frac{f_0^n}{g_0}, \frac{c}{g_0}).$$

is rational in X. □

Cor. (17.5.1.12). For a special subdomain U of X, the canonical topology induces the canonical topology of U, by the transitivity property of affinoid subdomains and(17.5.1.10). In fact, by(17.5.1.14), any affinoid subdomain is open and the topology coincides. ⌟

Prop. (17.5.1.13). Let $\varphi : Y = \mathrm{Sp}\, B \to X = \mathrm{Sp}\, A$ be a morphism, if x is a point of X that $A/\mathfrak{m}_x \to B/\mathfrak{m}_x B$ is a surjection, then there is an affinoid nbhd U of x that φ restricts to a closed immersion on $\varphi^{-1}(U)$. If $A/\mathfrak{m}_x^n \cong B/\mathfrak{m}^n$ for all n, then there is an affinoid nbhd U of x that φ restricts to an isomorphism $\varphi^{-1}(U) \cong U$. ⌟

Proof: Cf.[Rigid and Formal Geometry P57]. □

Cor. (17.5.1.14). Every affinoid subdomain of X is open and has the restriction topology of X(canonical topology), because it satisfies the second condition of(17.5.1.13), by(17.5.1.8). ⌟

Lemma (17.5.1.15). If $f \subset A\langle X_1, \ldots, X_n\rangle$ is X_n-distinguished of order $\leq s$ for each element of $\mathrm{Sp}\, A$, then the set of elements that f is X_n-distinguished of exact order s is a rational subdomain of A. ⌟

Proof: Let $f = \sum f_v X_n^v$, let the constant coefficient of f_v be a_v, then the set is in fact $U = \{x \in \mathrm{Sp}\, A | |a_v(x)| \leq |a_s(x)|\}$. This is because, if f is distinguished of order s_x at x, then $a_{s_x} \neq 0$ because f_{s_x} is a unit, and $|a_v|_x \leq |f_v| \leq |f_{s_x}| = |a_{s_x}|_x$ for $v \leq s_x$ and strict inequality holds for $v > s_x$. In particular, $a_0, \ldots, a_s$ cannot have a common zero, so it is truly a rational subdomain. □

Prop. (17.5.1.16). If $f \subset A\langle X_1, \ldots, X_n\rangle$ is X_n-distinguished of order s for each element of $\mathrm{Sp}\, A$, then the map
$$A\langle X_1, \ldots, X_{n-1}\rangle \to A\langle X_1, \ldots, X_n\rangle/(f)$$
is finite. ⌟

Proof: Cf.[Rigid And Formal Geometry P79]. □

Presheaf of Affinoid Functions

Def. (17.5.1.17). The **weak Grothendieck category**(affine topology) on an affinoid space X has coverings defined by the finite cover by affinoid subdomains, called **affinoid covering**.

The **strong Grothendieck category**(fpqc topology) on an affinoid space X is defined by: objects are unions of affinoid subdomains $U = \cup U_i$ that for any morphism from an affinoid space $\varphi : Z \to U \subset X$, the pullback covering $\cup \varphi^{-1}(U_i)$ has a finite subcover by affinoid subdomains. A covering is defined by the same finiteness property.

The strong Grothendieck topology satisfies completeness conditions G_0, G_1, G_2 defined in(6.1.1.10), as easily verified.

The weak Grothendieck topology is a temporary notion, it will be obsolete after Tate's acyclicity theorem is proved. Admissible opens and admissible covers are notions w.r.t. the strong Grothendieck topology. ⌟

Proof: The weak Grothendieck category is a Grothendieck category by(17.5.1.11). The strong Grothendieck category is a Grothendieck category because: the finiteness condition lifts along base change, and also for base change, because we can first choose a finite subcover, then choose a finite subcover of the base change covering of that finite covering. □

Def. (17.5.1.18). For n functions $f_1, \ldots, f_n$ without common zeros, the rational subdomains $U_i = X(\frac{f_1}{f_i}, \ldots, \frac{f_n}{f_i})$ is an affinoid covering, called the **rational covering**. For n functions $f_1, \ldots, f_n$, there is a **Laurent covering** $X(\prod f_i^{\varepsilon_i}), \varepsilon_i = \pm 1$. ⌟

Prop. (17.5.1.19). Morphisms of affinoid spaces are continuous in weak Grothendieck topology by(17.5.1.11). It is also continuous in the strong Grothendieck topology, as one can check the finiteness conditions. ⌟

Prop. (17.5.1.20). Let X be an affinoid K-space, for any $f \in \mathcal{O}_X(X)$, consider the following sets:

$$U_1 = \{x||f(x)| < 1\}, \quad U_2 = \{x||f(x)| > 1\}, \quad U_3 = \{x||f(x)| > 0\}.$$

Then any finite union of sets of the form is admissible, and any finite cover by finite union of sets of the form is an admissible covering. ⌟

Proof: We first show that U_1 is admissible open, the others are similar. Let ε_n be an ascending sequence of elements in $\sqrt{|K^*|}$ converging to 1, then $U_1 = \cup_n X(\varepsilon_n^{-1} f)$ is a union of open subsets because $\varepsilon_n \in \sqrt{|K^*|}$. Now for any affinoid space Z mapping into U_1, $|\varphi^*(f)(z)|_{\sup} < 1$ for all $z \in Z$, thus by maximal principle(11.2.4.21), $|f|_{\sup} < 1$, thus the cover $U_1 = \cup_n X(\varepsilon_n^{-1} f)$ can be refined by a finite cover, thus it is admissible open.

For the admissibility of covering, the proof is similar, but use the following lemma(17.5.1.21). □

Lemma (17.5.1.21). For any affinoid K-algebra A, if f_i, g_j, h_k are system of functions on A that: for every $x \in A$, either $|f_i(x)| < 1, |g_j > 1$ or $h_k(x) > 0$, then we can replace $>, <$ by $\geq, \leq$ and elements in $\sqrt{|K^*|}$ that the same condition is true. ⌟

Proof: Cf.[Rigid and Formal Geometry P97]. □

Cor. (17.5.1.22). The strong Grothendieck category is finer than the Zariski category, because any standard affine open set is of the form U_3 and also Zariski covering is open covering because $\mathrm{Sp}(A)$ is Noetherian(11.2.4.16). ⌟

Def. (17.5.1.23) [Presheaf of Affinoid Functions]. There is a **presheaf of affinoid functions** defined on the weak Grothendieck topology because of the universal property of the affinoid subdomains.

Then the stalk $\mathcal{O}_{X,x}$ are local ring with maximal ideal $\mathfrak{m}_x\mathcal{O}_{X,x}$. Hense let $X = \mathrm{Sp}\, A$, the stalk map factor thorough $A \to A_{\mathfrak{m}_x} \hookrightarrow \mathcal{O}_{x,X}$, and

$$A/\mathfrak{m}_x^n \cong A_{\mathfrak{m}_x}/\mathfrak{m}_x^n A_{\mathfrak{m}_x} \cong \mathcal{O}_{X,x}/\mathfrak{m}_x^n\mathcal{O}_{X,x}$$

so it induces isomorphisms between their $\mathfrak{m}_x$-adic completions. ⌟

Proof: By(17.5.1.8), there is an isomorphism $K' = \mathcal{O}_X(X)/\mathfrak{m}_x \cong \mathcal{O}_X(U)/\mathfrak{m}_x\mathcal{O}(U)$. Take the converse and pass to direct colimit(it is exact), $\mathcal{O}_{X,x}/\mathfrak{m}_x O_{X,x} \cong K'$. This map will be regarded as evaluation at x. The kernel $\mathfrak{m}_x\mathcal{O}_{X,x}$ is a maximal ideal. There are no other maximal ideals in $\mathcal{O}_{X,x}$ because if f in not in the kernel, then $f(x) \neq 0$, and multiply by an element in K^*, it can be made $|f(x)| \geq 1$, and then $U(f^{-1})$ is an affinoid subdomain containing x that f is invertible in it.

For the second assertion, for an affinoid subdomain $\mathrm{Sp}\, A'$, there are maps

$$A/\mathfrak{m}^n \to A'/\mathfrak{m}^n \to \mathcal{O}_{X,x}/\mathfrak{m}^n\mathcal{O}_{X,x}.$$

We first show these are isomorphisms: the first map is an isomorphism by(17.5.1.8), then take direct colimit, the composition map is also isomorphism.

$A/\mathfrak{m}_x^n \cong A_{\mathfrak{m}_x}/\mathfrak{m}_x^n A_{\mathfrak{m}_x}$ is classical.

$A_{\mathfrak{m}_x} \hookrightarrow \mathcal{O}_{x,X}$ is injective because by Krull's intersection theorem(5.2.2.15), $A_{\mathfrak{m}_x} \hookrightarrow \mathcal{O}_{x,X} \to \widehat{\mathcal{O}_{X,x}} \cong \widehat{A_{\mathfrak{m}}}$ is injective. □

Cor. (17.5.1.24). $f \in A = \mathcal{O}_X(X)$ vanish iff it vanish at every stalk, this is because $A \to \prod_{\mathfrak{m}} A_{\mathfrak{m}} \to \prod \mathcal{O}_{X,x}$ is injective. ⌟

Cor. (17.5.1.25). Giving a covering of affinoid subdomain of an affinoid space $X_i \to X$, then $\mathcal{O}_X(X) \to \prod \mathcal{O}_{X_i}(X_i)$ is an injection. (This is because the kernel vanishes at each stalk.) ⌟

Cor. (17.5.1.26). For a subdomain of an affinoid space X, the corresponding ring map is flat. ⌟

Proof: Cf.[Formal and Rigid Geometry P68]. □

Prop. (17.5.1.27). The stalk $\mathcal{O}_{X,x}$ is Noetherian, in particular it is $\mathfrak{m}$-adically separated by Krull's intersection theorem(5.2.2.15). ⌟

Proof: First it is $\mathfrak{m}$-adically separated, because by(17.5.1.23), for a $f \in \cap \mathfrak{m}^n \mathcal{O}_{X,x}$, we can choose an affinoid subdomain $\operatorname{Sp} A$ that $f \in A$(17.5.1.8), then $f \in \mathfrak{m}^n A$, so by Krull's intersection theorem(5.2.2.15), we have $f = 0$ in $A_{\mathfrak{m}}$.

In the same way, any f.g. ideal $\mathfrak{a}$ of $\mathcal{O}_{X,x}$ is $\mathfrak{m}$-adically closed, this is because it is generated by an ideal in the affinoid algebra of a nbhd, and then $\mathcal{O}_{x,X}/\mathfrak{a}$ is separated as the stalk of an affinoid algebra $A'/\mathfrak{a}'$.

Now pass a chain of f.g. ideals to their completion, then that chain is stationary because $\widehat{\mathcal{O}}_{X,x} = \widehat{A}_{\mathfrak{m}_x}$ is Noetherian(5.1.1.43). And now this chain is also stationary because ideals are closed in $\mathfrak{m}$-adic topology. □

Locally Closed Immersions

Def. (17.5.1.28) [Immersions]. A morphism of affinoid spaces is called a **closed immersion** iff the corresponding ring map is surjective. It is called a **locally closed immsetion** iff it is injective and the stalk map are all surjective. It is called an **open immersion** iff it is injective and the corresponding stalk maps are isomorphism. All these notions are stable under compositions.

An affinoid subdomain is an open immersion by(17.5.1.8)(17.5.1.23) and(17.5.1.27). ⌟

Lemma (17.5.1.29). Base change by affinoid subdomain of closed/locally closed/open immersions are of the same type. ⌟

Proof: This is obvious for locally close and open, because affinoid subdomains are open(17.5.1.14), for the closed immersion, use(11.2.4.32). □

Prop. (17.5.1.30). A closed immersion of affinoid spaces is equivalent to a locally closed immersion that the corresponding ring map is finite. ⌟

Proof: Cf.[Rigid and Formal Geometry P70]. A closed immersion $X' \to X$ is a locally closed immersion because the canonical topology of $\operatorname{Sp} A$ restricts to the canonical topology on $\operatorname{Sp} A/\mathfrak{a}$(17.5.1.4), then use(11.2.4.32), and the fact direct limit is exact. □

Prop. (17.5.1.31)[Clopen Immersion]. The image of an open and closed immersion is Zariski closed and open. In particular, it is a Weierstrass subdomain. ⌟

Proof: Cf.[Rigid and Formal Geometry P71]. □

Def. (17.5.1.32). A **Runge immersion** is a closed immersion followed by an open immersion of Weierstrass subdomain. Runge immersion is table under base change of affinoid subdomains by(17.5.1.29) ⌟

Prop. (17.5.1.33) [Equivalent Definition of Runge Immersions]. For a morphism $\sigma : A \to A'$, $\mathrm{Sp}\, A' \to \mathrm{Sp}\, A$ is a Runge immersion iff $\sigma(A)$ is dense in A' iff $\sigma(A)$ contains a set of affinoid generator of A' over A. ⌟

Proof: For a Runge immersion, $\sigma(A)$ is dense in A', because this is true for Weierstrass subdomain and closed immersion.

If $\sigma(A)$ is dense in A', then by(11.2.4.28), we can modify a set of affinoid generators by a set of affinoid generators in $\sigma(A)$.

If h_i is a set of affinoid generators in $\sigma(A)$, then $A \to A\langle h_i\rangle \to A'$ is a Runge immersion. □

Cor. (17.5.1.34). Runge immersion is stable under composition. ⌟

Prop. (17.5.1.35). An open and Runge immersion is an immersion of Weierstrass subdomain. ⌟

Proof: By localizing on this Weierstrass subdomain, and notice Weierstrass subdomain is stable under composition(17.5.1.11), we reduce to clopen immersion case, and result follows by(17.5.1.31). □

Lemma (17.5.1.36) [Extension of Runge Immersion]. For a morphism of affinoid spaces $X' \to X = \mathrm{Sp}\, A$, if $f_1, \ldots, f_n, g$ generate A, for $\varepsilon \in \sqrt{\{|K^*|\}}$, denote $X_\varepsilon = \{x||f_i(x)| \leq \varepsilon|g|\}$, this is a rational subdomain. The inverse image of X_ε is X'_ε, then if $X'_{\varepsilon_0} \to X_{\varepsilon_0}$ is a Runge immersion for some ε_0, then there is a $\varepsilon > \varepsilon_0$ that $X'_\varepsilon \to X_\varepsilon$ is also a Runge immersion. ⌟

Proof: Cf.[Rigid and Formal Geometry P73]. □

Prop. (17.5.1.37) [Gerritzen-Grauert]. For a locally closed immersion $\varphi : X' \to X$, there is a finite cover of X of rational subdomains X_i that $\varphi^{-1}(X_i) \to X_i$ are Runge immersions. ⌟

Proof: Cf.[Formal and Rigid Geometry P79]. □

Cor. (17.5.1.38) [Gerritzen-Grauert]. Any affinoid subdomain is equivalent to a finite union of rational subdomains. ⌟

Proof: An affinoid subdomain is an open immersion by(17.5.1.28), so $\varphi^{-1}(X_i) \to X_i$ is open and Runge, so it is Weierstrass by(17.5.1.35). In particular, $X \cap X_i$ is rational in X by transitivity, thus the result. □

Tate's Acyclicity

Lemma (17.5.1.39) [Reduction of Weak Grothendieck Topology].

- Every affinoid covering has a refinement of rational covering.
- For every rational covering, there is a Laurent covering $\{V_i\}$ that restriction on each V_i is rational covering generated by units.
- Every rational covering generated by units has a refinement of Laurent covering.

⌟

Proof: 1: By(17.5.1.38), we can assume the covering consists of rational subdomains $U_i = X(\frac{f_{i1},\ldots,f_{ii_k}}{f_{i0}})$, then consider the elements $f_{v_1\ldots v_n} = \prod_{i=1}^n f_{iv_i}$, where at least some $v_i = 0$. Denote the set of these elements by I.

Firstly, these elements has no common zero on X, thus generating a rational covering of X: for any $x\in U_i$, f_{i0} doesn't vanish at x, thus the product $\prod_{j\neq i} f_{jv_j}$ vanishes for all choices of v_j, but this is impossible because for each j, $(\{f_{ik}\}_k)=(1)$.

Secondly, this is a refinement of U_i: We show $X_{f_{v_1\ldots v_n}}\subset U_k$ where $v_k=0$. For this, consider $x\in X_{f_{v_1\ldots v_n}}$, then $x\in U_j$ for some j. If $j=k$, we are done, otherwise,

$$|f_{v_1\ldots\mu_k\ldots v_n}(x)|\leq |f_{v_1\ldots 0\ldots\mu_k\ldots v_n}(x)|\leq |f_{v_1\ldots v_n}(x)|.$$

Where the last inequality is because $(v_1,\ldots,0,\ldots,\mu_k,\ldots,v_n)$ has a 0, thus $f_{v_1\ldots 0\ldots\mu_k\ldots v_n}\in I$.

2: For a rational covering, f_i is invertible in the ring of $U=X(\frac{f_0}{f_i},\ldots,\frac{f_n}{f_i})$, thus it has a inverse that attains maximum value on U(11.2.4.21). Hence there is a $c\in K^*$ that $|c|^{-1}<\inf(\max\{|f_i(x)|\})$.

I claim the Laurent covering w.r.t. the elements $cf_0,\ldots,cf_n$ satisfies the requirement. Because for example, on $V=X((cf_0)\cdots(cf_s)(cf_{s+1})^{-1}\cdots(cf_n)^{-1})$, $|f_i(x)|<|f_j(x)|$ for $i\leq s<j$, so the covering restricted to V is just the rational covering generated by $f_{s+1},\ldots,f_n$, and they are all invertible in $\mathcal{O}(V)$.

3: In fact the Laurent covering generated by the element $f_if_j^{-1}$ for $i<j$ is a refinement of the rational covering generated by $f_1,\ldots,f_n$, because in any one of this Laurent subdomains V, for any two i,j, either $|f_i(x)|<|f_j(x)|$ or $|f_j(x)|<|f_i(x)|$ for all $x\in V$, so there is a maximal one f_s, then $V\subset X(\frac{f_0}{f_s},\ldots,\frac{f_n}{f_s})$. □

Prop. (17.5.1.40) [Tate's Acyclicity Theorem]. The presheaf of affinoid functions on an affinoid space $X=\operatorname{Sp}A$ is a sheaf w.r.t the weak Grothendieck category. In fact, for any A-module M, the presheaf $\widetilde{M}=M\otimes_A\mathcal{O}_X$ is a sheaf w.r.t. the weak Grothendieck topology, called the **quasi-coherent** sheaf on X.

Moreover, for any finite cover of affinoid subdomains, the Čech cohomology group $\check{H}^q(\operatorname{Sp}A,\widetilde{M})$ vanish for $q\neq 0$. ⌟

Proof: It suffices to prove the last assertion. First reduce to the case of Laurent covering by(17.5.1.39) and(6.3.2.10)(6.3.2.11). Noticing the base change invariance of the specialities of affinoid subdomains(17.5.1.11). Even more, by(6.3.2.12) and an induction process, it suffices to prove for the simple Laurent covering $X(f),X(f^{-1})$.

It suffices to prove for the sheaf of affinoid functions $\mathcal{O}_X$, because for any Qco sheaf $\widetilde{M}$, choose a free resolution of M, then use dimension shifting, notice the covering is finite(the flatness of the algebra map(17.5.1.26) is used to deduce the long exact sequence).

For the sheaf $\mathcal{O}_X$, the main tool is the following commutative diagram:

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & (X-f)A\langle X\rangle\times(1-fY)A\langle Y\rangle & \xrightarrow{\delta''} & (X-f)A\langle X,X^{-1}\rangle & \longrightarrow & 0\\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A & \xrightarrow{\varepsilon'} & A\langle X\rangle\times A\langle Y\rangle & \xrightarrow{\delta'} & A\langle X,X^{-1}\rangle & \longrightarrow & 0\\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A & \xrightarrow{\varepsilon} & A\langle f\rangle\times A\langle f^{-1}\rangle & \xrightarrow{\delta} & A\langle f,f^{-1}\rangle & \longrightarrow & 0
\end{array}$$

where δ' is given by $(h_1(X),h_2(Y))\mapsto h_1(X)-h_2(X^{-1})$, and δ'' is induced by δ'. The columns are all exact, and the first row and the second row are exact. ε is injective by(17.5.1.25). Then the last row is also exact, by spectral sequence. □

Prop. (17.5.1.41) [Strong/Weak Topos The same]. If X is an affinoid K-space, the category of sheaves w.r.t the strong Grothendieck topology is equivalent to the category of sheaves w.r.t. the weak Grothendieck topology by pushforward and pullback of sheaves by(6.1.2.25) because the strong and weak Grothendieck category satisfies the conditions.

In particular, this applies to the case $\mathcal{O}_X$ by(17.5.1.40), the resulting sheaf is called the **sheaf of rigid analytic functions** on X, also denoted by $\mathcal{O}_X$. ⌟

2 Rigid Analytic Spaces

Def. (17.5.2.1). A **G-ringed K-space** is a pair $(X, \mathcal{O}_X)$ where X is a G-topological space and $\mathcal{O}_X$ is a sheaf of K-algebras. It is called **local G-ringed K-space** if the stalks are all local rings. Their morphisms are defined routinely. ⌟

Prop. (17.5.2.2) [Morphisms Between Affinoid Spaces]. An affinoid K-space with the sheaf of analytic functions $(X, \mathcal{O}_X)$(17.5.1.41) is an example of local G-ringed K-space(17.5.1.23).

A continuous homomorphism of rings induces a local G-ringed morphism. And all morphisms come from these.

Moreover, an affinoid K-space is a complete G-ringed K-space(i.e. rigid)(6.1.1.10). ⌟

Proof: It is a G-space by(17.5.1.40)(17.5.1.41), morphisms by(17.5.1.19), notice the $\mathfrak{m}_x$ generate the maximal ideal of $\mathcal{O}_{X,x}$(17.5.1.23), so the morphism is local.

To show all morphisms are like these, we need to show a morphism $\sigma : A \to B$ gives at most one $\operatorname{Sp} B \to \operatorname{Sp} A$: the morphism is local, so it maps $\mathfrak{m}_{\varphi(x)}$ to $\mathfrak{m}_x$, and from the commutative diagram

$$\begin{array}{ccc} A/\mathfrak{m}_{\varphi(x)} & \longrightarrow & B/\mathfrak{m}_x \\ \downarrow\cong & & \downarrow\cong \\ \mathcal{O}_{\varphi(x),\operatorname{Sp} A}/\mathfrak{m}_{\varphi(x)}\mathcal{O}_{\varphi(x),\operatorname{Sp} A} & \longrightarrow & \mathcal{O}_{x,\operatorname{Sp} B}/\mathfrak{m}_x\mathcal{O}_{x,\operatorname{Sp} B} \end{array}$$

(17.5.1.23) shows $\mathfrak{m}_{\varphi(x)}$ is mapped into $\mathfrak{m}_x$, so $\mathfrak{m}_{\varphi(x)} = (\sigma^*)^{-1}\mathfrak{m}_x$, which shows φ is unique set-theoretically, and on the level of structure sheaf, the uniqueness of $\mathcal{O}_{\operatorname{Sp} A}(V) \to \mathcal{O}_{\operatorname{Sp} B}(\varphi^{-1}(V))$ is unique by the definition of affinoid subdomain(17.5.1.7). □

Def. (17.5.2.3) [Rigid Spaces]. The category of **rigid (analytic) space** is a full subcategory of local G-ringed K-spaces that it is complete G_0, G_1, G_2, and it has an admissible covering $\{X_i \to X\}$ that $(X_i, \mathcal{O}_X|_{X_i})$ are affinoid K-spaces.

It follows easily that an admissible open subset of a rigid space is again rigid. ⌟

Prop. (17.5.2.4) [Glueing Rigid Spaces]. Glueing rigid analytic spaces is legitimate, so does glueing morphisms on the source. ⌟

Proof: First glue the set, then use(6.1.1.12) to glue G-topology, finally the glue of structure sheaf is similar to(6.1.5.3). □

Cor. (17.5.2.5) [Spectrum Adjointness]. If X is rigid and Y is affinoid, then $\operatorname{Hom}(X, Y) \cong \operatorname{Hom}(\mathcal{O}_Y(Y), \mathcal{O}_X(X))$. This follows from(17.5.2.2) and glue(17.5.2.4). ⌟

Prop. (17.5.2.6) [Fiber Products]. Fiber products exist in the category of rigid analytic space. This is fiber product of affinoid spaces are affinoid so we can glue them by universal property, the same as(6.2.7.15). ⌟

Prop. (17.5.2.7). An affinoid space is connected in the weak Grothendieck topology iff it is connected in the strong Grothendieck topology iff it is connected in the Zariski topology. ⌟

Proof: Firstly the weak and strong are equal because any strong covering of X has a refinement of weak covering, and a weak covering is a strong covering. So it suffices to prove the equivalence of the last two.

One direction is trivial, for the other direction, use Tate's acyclicity, if $X_1, X_2 \to \mathrm{Sp}\, A$, $X_1 \cap X_2 = 0$, then $A = \mathcal{O}_X(X_1) \times \mathcal{O}_X(X_2)$, so $\mathrm{Spec}\, A$ is not connected, neither do $\mathrm{Sp}\, A$. □

Prop. (17.5.2.8). We can define the connected components of X as the equivalence classes of elements that can be reached using connected admissible open subsets of X. Then the connected components are admissible and forms an admissible cover of X. ⌟

Proof: Notice that there exists a finite covering consisting of connected Zariski subsets, by(17.5.2.7) and the fact $\mathrm{Sp}\, A$ has f.m. connected components because $\mathrm{Spec}\, A$ does as A is Noetherian(11.2.4.12) and(17.5.1.3).

Thus we are done, because by(17.5.1.22), a Zariski covering is admissible, and clearly the connected components of X are just this Zariski covering. □

Rigid GAGA

Lemma (17.5.2.9). Let Z be an affine scheme algebraic over K, and Y a rigid K-space, then the set of morphisms of local G-ringed spaces $(Y, \mathcal{O}_Y) \to (Z, \mathcal{O}_Z)$ corresponds to K-algebra morphisms from $\mathcal{O}_Z(Z)$ to $\mathcal{O}_Y(Y)$. ⌟

Proof: Cf.[Formal and Rigid Geometry P111]. □

Def. (17.5.2.10)[Rigid Analytification]. There is a partial functor X^{rig} from the category of schemes X locally algebraic over a valued field K to the category of rigid K-spaces that are right adjoint to the forgetful functor from the category of rigid K-spaces to local ringed K-space, called the **GAGA functor**.

The existence of this functor is proven in(17.5.2.14). ⌟

Def. (17.5.2.11)[Analytification of Affine Schemes]. Let $T_n(r)$ be the elements $\sum a_v \zeta^v$ in T_n that $\lim a_v r^{|v|} = 0$. Then choose a $c \in K$, $|c| > 1$, define $T_n^{(i)} = T_n(|c|^i)$. Then $T_n^{(i)} = K\langle c^{-i}X_1, \ldots, c^{-i}X_n\rangle$, so clearly $\mathrm{Sp}(T_n^{(i)})$ is an affinoid subdomain of $\mathrm{Sp}(T_n^{(i+1)})$ by(17.5.1.9). Thus there is a chain of inclusions of affinoid subdomains:

$$B^n = \mathrm{Sp}(T_n^{(0)}) \hookrightarrow \mathrm{Sp}(T_n^{(1)}) \hookrightarrow \mathrm{Sp}(T_n^{(2)}) \hookrightarrow \ldots$$

Then we can use(17.5.2.4) to glue them together as $\mathbb{A}_K^{n,rig}$. ⌟

Prop. (17.5.2.12). The maximal spectrum $\mathrm{Max}(K[X_i]) = \cup_n \mathrm{Spa}(T_n^{(i)})$ as sets. ⌟

Proof: It suffices to show the following two.

- For any maximal ideal $\mathfrak{m} \subset T_n$, $\mathfrak{m}' = \mathfrak{m} \cap K[X_i]$ is maximal.
- For any maximal ideal $\mathfrak{m}' \subset K[X_i]$, there is some N that $\mathfrak{m}' T_n^{(i)}$ is maximal in $T_n^{(i)}$ for all $i > N$.

For 1: Consider the $K \subset K[X_i]/\mathfrak{m}' \subset T_n/\mathfrak{m}$, $T_n/\mathfrak{m}$ is a finite extension of K by(11.2.4.10), then so does $K[X_i]/\mathfrak{m}'$, by(5.2.1.3). To prove $\mathfrak{m}' = \mathfrak{m} \cap K[X_i]$, consider the following diagram:

$$\begin{array}{ccc} K[X_i]/\mathfrak{m}' & \longrightarrow & T_n/\mathfrak{m}'T_n \\ \| & & \downarrow \\ K[X_i]/\mathfrak{m}' & \longrightarrow & T_n/\mathfrak{m} \end{array}$$

As $K[X_i]/\mathfrak{m}'$ is finite over K, it is complete, but $K[X_i]$ is dense in T_n, thus the horizontal maps are surjective. But then the lower horizontal is isomorphism, then the upper horizontal is also isomorphism, and then the vertical map is isomorphism, thus we are done.

For 2, $K[X_i]/\mathfrak{m}'$ is a finite extension of K, thus has a unique valuation, let N be large that $|\overline{X}_i| \leq |c|^N$, then for $i > N$, the quotient map factors uniquely as $K[X_i] \to T_n^{(i)} \to K/\mathfrak{m}'$. Then the kernel $\mathfrak{m}$ of $T_n^{(i)}$ is a maximal ideal(same reason as before) that satisfies $\mathfrak{m} \cap K[X_i] = \mathfrak{m}'$. Then we finish by item1. □

Cor. (17.5.2.13) [Analytification for Affine Schemes]. Similarly, for an affine scheme $Z = \operatorname{Spec} K[X_i]/\mathfrak{a}$ of f.t over K, we construct its analytification Z^{rig} as the glue of the inclusions:

$$\operatorname{Sp}(T_n^{(0)}/\mathfrak{a}) \hookrightarrow \operatorname{Sp}(T_n^{(1)}/\mathfrak{a}) \hookrightarrow \dots$$

Then Z^{rig} is the analytification of $K[X_i]/\mathfrak{a}$.

And we see from the proof of(17.5.2.12) the maximal spectrum $\operatorname{Max}(K[X_i]/\mathfrak{a}) = \cup_n \operatorname{Spa}(T_n^{(i)}/\mathfrak{a})$ as sets. ⌟

Proof: The canonical map $K[X_i]/\mathfrak{a} \to T_n^{(i)}/\mathfrak{a}$ glue together to be a morphism $\mathcal{O}_Z(Z) \to O_{Z^{rig}}(Z^{rig})$, which by(17.5.2.9) corresponds to a map $Z^{rig} \to Z$ of local ringed spaces.

Now any other morphism $Y \to Z$ from a rigid K-space Y to Z, choose an affinoid K-space covering Y_i of Y, then the map $Y_i \to Z$ corresponds by(17.5.2.9) to a morphism $\sigma : K[X_i]/\mathfrak{a} \to \mathcal{O}_{Y_i}(Y_i)$, thus if we choose i large enough that $|\sigma(X_i)| \leq |c|^i$, then σ can be extended uniquely to

$$K[X_i]/\mathfrak{a} \to T_n^{(i)}/\mathfrak{a} \xrightarrow{\sigma} \mathcal{O}_{Y_i}(Y_i),$$

By the universality of affinoid subdomains. This σ corresponds to a morphism $Y_i \to \operatorname{Sp}(T_n^{(i)}) \to Z^{rig}$, and these clearly glue together to give a morphism $Y \to Z^{rig}$, thus proving the universal property. □

Prop. (17.5.2.14) [General Analytification]. For any locally algebra scheme X over K, choose an affine covering Z_i, consider the analytification of Z_i by(17.5.2.13), then $Z_i \cap Z_j$ obviously has the inverse image as the rigid analytification by universal property, thus unique, so the analytifications of Z_i can be glued to an analytification of X.

Moreover, the underlying set of X^{rig} is identified with the closed pts of the scheme X, because this is the case of Z_i(17.5.2.11). ⌟

Prop. (17.5.2.15). Rigid analytification preserves fiber products. ⌟

Proof: This follows from the construction of fibered product of schemes(6.2.7.15), so we only need to prove the affine case. For this, Cf.[U. Köpf, Über eigentliche Familien algebraischer Varietäten über affinoiden Räumen. Schriftenr, Satz 1.8]. □

Prop. (17.5.2.16) [Stalks]. For a point $z \in Z^{rig}$, the completion of $\mathcal{O}_{Z^{rig},z}$ and $\mathcal{O}_{Z,z}$ are the same. ⌟

Proof: Cf.[U. Köpf, Über eigentliche Familien algebraischer Varietäten über affinoiden Räumen. Schriftenr, Satz 2.1]. □

3 Coherent Sheaves on Rigid Spaces

Prop. (17.5.3.1). For an affinoid K-space X, there is a Qco module construction $M \to M \otimes_A \mathcal{O}_X$ as in(17.5.1.40) in the weak Grothendieck topology, and it extends uniquely to a sheaf w.r.t. the strong Grothendieck topology by(17.5.1.41), also denoted by $M \otimes_A \mathcal{O}_X$. This is a faithfully exact, fully faithful functor between Abelian categories from $\mathcal{A}b$ to $\mathcal{O}_X$-modules, and it preserves tensor product and direct sums. ⌟

Proof: Because $\Gamma(X, M \otimes_A \mathcal{O}_X) = M$ and obviously fully faithful, this map is fully faithful, and it is exact because the restriction map of an affinoid subdomain is flat(17.5.1.26), and shifification is exact. □

Def. (17.5.3.2)[Coherent Sheaves]. For an $\mathcal{O}_X$-module $\mathcal{F}$ on a rigid space X, **finite type, of finite presentation, coherence** are defined w.r.t the strong topology as X is a ringed site. All these notions are stable under passing to an admissible open subspaces. ⌟

Proof: For the passing of coherence to admissible open subspaces, use the fact that restriction maps are flat(17.5.1.26). □

Cor. (17.5.3.3). Notice $\mathcal{O}_X^n = A^n \otimes_A \mathcal{O}_X$, by(17.5.3.1) and the fact A is Noetherian, passing to a refinement covering, $\mathcal{F}$ is coherent iff there is an admissible affinoid covering $\mathfrak{U} : X_i \to X$ that $F|_{X_i}$ is associated to a finite $\mathcal{O}_{X_i}$-module. In this case, $\mathcal{F}$ is said to be **$\mathfrak{U}$-coherent**. Thus the coherent sheaves form a weak Serre subcategory of $\mathcal{O}_X$-modules.

In particular, $\mathcal{O}_X$ is coherent. ⌟

Prop. (17.5.3.4). If $\mathcal{F}, \mathcal{G}$ are all $\mathfrak{U}$-coherent modules, then:

- $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ and $\mathcal{F} \oplus \mathcal{G}$ are $\mathfrak{U}$-coherent,
- if $\mathcal{F} \to \mathcal{G}$ is a $\mathcal{O}_X$-module morphism, then the kernel and image are all $\mathfrak{U}$-coherent.
- If $\mathcal{I}$ is a $\mathfrak{U}$-coherent sheaf of ideal of $\mathcal{O}_X$, then $\mathcal{I}\mathcal{F}$ is $\mathfrak{U}$-coherent.

⌟

Proof: The first and the second are consequences of(17.5.3.1), noticing A_i is Noetherian. The third is an image of $\mathcal{I} \otimes_{\mathcal{O}_X} \mathcal{F}$. □

Lemma (17.5.3.5). If $\mathcal{F}$ is $\mathfrak{U}$ coherent for a simple Laurent covering $\mathfrak{U}$, then $H^1(\mathfrak{U}, \mathcal{F}) = 0$. ⌟

Proof: The goal is to show any element in $\mathcal{F}(U_1 \cap U_2)$ can be represented by $u_1 + u_2$, where $u_i \in \mathcal{F}(U_i)$. Let $U_1 = \operatorname{Sp} A\langle f\rangle, U_2 = \operatorname{Sp} A\langle f^{-1}\rangle, U_1 \cap U_2 = \operatorname{Sp} A\langle f, f^{-1}\rangle$. Now $A\langle f\rangle = A\langle X\rangle/(X - f), A\langle f^{-1}\rangle = A\langle Y\rangle/(Yf - 1), A\langle f, f^{-1}\rangle = A\langle X, Y\rangle/(X - f, Yf - 1)$, and we endow them with the residue norm.

Now we want to give norms to $M_1 = \mathcal{F}(U_1), M_2 = \mathcal{F}(U_2), M_{12} = \mathcal{F}(U_1 \cap U_2)$. M_i are finite $\mathcal{O}_X(U_i)$-modules, so there are elements $v_i, w_j, i \leq m, j \leq n$ that generate M_1, M_2 respectively. So there are attached morphisms

$$(A\langle f\rangle)^m \to M_1, \quad (A\langle f^{-1}\rangle)^n \to M_2, \quad (A\langle f, f^{-1}\rangle)^m \to M_{12}$$

And endow them with the residue norm, which is complete..

Notice that to prove the assertion, it suffice to show for each $\varepsilon > 0$, there is an α that for each $u \in_{12}$, there are u_1 and u_2 in M_i respectively that $|u_i| < \alpha|u|$ and $|u - u_1 - u_2| < \varepsilon|u|$, because then we can use iteration and completeness to get the result.

Giving $\beta > 1$, any $g \in A\langle f, f^{-1}\rangle$ can be lifted to an element $\sum c_{ij}X^iY^j$ that $|c_{ij}| \leq \beta|g|$. Then by regrouping terms that $i \geq j$ or $i < j$, there are two element $g^+ \in A\langle f\rangle$ and $g^- \in A\langle f^{-1}\rangle$ that $g^+ + g^-$ restricts to g on $U_1 \cap U_2$, and $|g^+|, |g^-| \leq \beta|g|$.

Now that $\mathcal{F}$ is coherent, so v_i and w_j both generate M_{12} separately. Then there are equations $v_i = \sum c_{ij}w_j$ and $w_i = \sum d_{ij}v_j$, where $c_{ij}, d_{ij} \in A\langle f, f^{-1}\rangle$. The image of $A\langle f\rangle$ is dense in $A\langle f, f^{-1}\rangle$(11.2.4.26), so there are elements $c'_{ij} \in A\langle f^{-1}\rangle$ s.t. $\max_{ijl} |c_{ij} - c'_{ij}||d_{jl}| < \beta^{-2}\varepsilon$.

Now I claim the above approximation process is true for $\alpha = \beta^2 \max(|c'_{ij}| + 1)$. For this, notice for any $u = \sum a_i v_i$ with $a_i \in A\langle f, f^{-1}\rangle$, which we may assume $|a_i| \leq \beta|u|$ by the definition of the norm on M_{12}, then $a_i = a_i^+ + a_i^-$, that $|a_i^*| \leq \beta|a_i|$. Consider the following element

$$u^+ = \sum a_i^+ v_i \in M_1, \quad u^- = \sum a_i^- \sum c'_{ij}w_j \in M_2$$

Then it is easily verified that $|u^*| < \alpha|u|$, and

$$u - u^- - u^+ = \sum\sum a_i^-(c_{ij} - c'_{ij})w_j = \sum\sum\sum a_i^-(c_{ij} - c'_{ij})d_{jl}v_l.$$

which has norm smaller than $\max |a_i^-(c_{ij} - c'_{ij})d_{jl}| \leq \beta^2|u| \cdot \beta^{-2}\varepsilon = \varepsilon|u|$, finishing the proof. □

Prop. (17.5.3.6)[Kiehl]. An $\mathcal{O}_X$-module $\mathcal{F}$ on an affinoid K-space $\operatorname{Sp} A$ is coherent iff it is associated to a finite A-module. ⌟

Proof: The converse is obvious, for the other direction, by(17.5.1.39), it suffices to prove for $\mathfrak{U}$ a Laurent covering, and further, it suffices to prove for the simplest Laurent covering $X(f), X(f^{-1}) \to X$ because: $U(f,g) \cup U(f,g^{-1}) \cup U(f^{-1},g) \cup U(f^{-1},g^{-1}) = (U(f,g) \cup U(f,g^{-1})) \cup (U(f^{-1},g) \cup U(f^{-1},g^{-1}))$.

Thus the above lemma shows that $H^1(\mathfrak{U}, \mathcal{F}) = 0$. Now I prove that for any finite affinoid covering $\mathfrak{U} = \cup \operatorname{Sp} A_i$, if $H^1(\mathfrak{U}, \mathcal{F}) = 0$ for any coherent sheaf $\mathcal{F}$, then any $\mathfrak{U}$-coherent sheaf $\mathcal{F}$ is associated to a finite A-module, this will finish the proof.

Consider any maximal ideal $\mathfrak{m}_x$ of A, $\mathfrak{m}_x \otimes_A \mathcal{O}_X$ is a coherent sheaf as $\mathfrak{m}_x$ is finite because A is Noetherian, so there is a short exact sequence

$$0 \to \mathfrak{m}_x\mathcal{F} \to \mathcal{F} \to \mathcal{F}/\mathfrak{m}_x\mathcal{F} \to 0$$

of $\mathfrak{U}$-coherent sheaves, because $A/\mathfrak{m}_x$ is a field, thus flat.

Now for any affinoid space U' in U_i for some i, the section of this exact sequence is exact, because the ring morphism associated to an affinoid subdomain is flat(17.5.1.26). In particular, this can be applied to any intersections of U_i, in particular the Čech complex of these sheaves. Then the long exact sequence and the fact $H^1(\mathfrak{U}, \mathfrak{m}_x\mathcal{F}) = 0$ shows

$$0 \to \mathfrak{m}_x\mathcal{F}(X) \to \mathcal{F}(X) \to \mathcal{F}/\mathfrak{m}_x\mathcal{F}(X) \to 0$$

Next we want to show $\mathcal{F}/\mathfrak{m}_x\mathcal{F}(X) \to \mathcal{F}/\mathfrak{m}_x\mathcal{F}(U_i)$ is isomorphism for any $x \in U_i$. To prove this, first for any affinoid subspace $U' = \operatorname{Sp} B$ contained in some U_j, let $U' \cap U_i = \operatorname{Sp} B_i$, $\mathcal{F}|_{U'} = M' \otimes_A \mathcal{O}_{U'}$, we show $\mathcal{F}/\mathfrak{m}_x\mathcal{F}(U') \cong \mathcal{F}/\mathfrak{m}_x\mathcal{F}(U' \cap U_i)$, this is equivalent to

$$M'/\mathfrak{m}_x M' \to M'/\mathfrak{m}_x M' \otimes_B B_i = M'/\mathfrak{m}_x M' \otimes_{B/\mathfrak{m}_x B} B_j/\mathfrak{m}_x B_j$$

is an isomorphism. But $B/\mathfrak{m}_x B \cong B_j/\mathfrak{m}_x B_j$: This is true when $x \in U'$ by(17.5.1.8), and they are both trivial ring if $x \notin U'$. Then look at the morphism of Čech complex induced by $\mathcal{F}/\mathfrak{m}_x\mathcal{F} \to$

$\mathcal{F}/\mathfrak{m}_x\mathcal{F}|_{U_i}$, then it is an isomorphism, by what we just proved, so its H^0 is also isomorphism, which is $\mathcal{F}/\mathfrak{m}_x\mathcal{F}(X) \cong \mathcal{F}/\mathfrak{m}_x\mathcal{F}(U_i)$.

Finally, by the commutative diagram $\begin{array}{ccc} \mathcal{F}(X) & \longrightarrow & \mathcal{F}/\mathfrak{m}_x\mathcal{F}(X) \\ \downarrow & & \downarrow \\ \mathcal{F}(U_i) & \longrightarrow & \mathcal{F}/\mathfrak{m}_x\mathcal{F}(U_i) \end{array}$, the right vertical arrow is isomorphism, so if denote $\mathcal{F}(U_i)$ by M_i, then $\mathcal{F}(X)$ generate $M_i/\mathfrak{m}_x M_i$ for every x, then consider $L = M_i/\mathcal{F}(X)$, then $\mathfrak{m}_x L = L$ for every x, then by Nakayama, for each maximal ideal $\mathfrak{m}$, there is a $m \in \mathfrak{m}$ that $(1+m)L = 0$, so $Ann(L) = (1)$, so $L = 0$, i.e. $\mathcal{F}(X)$ generate M_i for each i.

Now choose f_i in $\mathcal{F}(X)$ that generate M_i simultaneously, then the map $\mathcal{O}_X^n \to \mathcal{F}$ is a surjection of $\mathfrak{U}$-coherent sheaves, its kernel $\mathcal{G}$ is also coherent by(17.5.3.4), now all the above argument works for $\mathcal{G}$, so there is a surjection $\mathcal{O}_X^m \to \mathcal{G}$, so $\mathcal{O}_X^m \to \mathcal{O}_X^n \to \mathcal{F} \to 0$, so $\mathcal{F}$ is associated to the cokernel of the map $A^m \to A^n$. □

Cor. (17.5.3.7). Coherence for a $\mathcal{O}_X$-module on a rigid K-space is affinoid local on the target. ⌟

Cohomology on Rigid Analytic Spaces

Lemma (17.5.3.8). The category of $\mathcal{O}_X$-modules on a rigid K-space is a Grothendieck category by(4.8.3.29). ⌟

Def. (17.5.3.9) [Derived Cohomologies]. Consider the right derived functor for Γ and more general f_*, these are left exact by(6.1.2.9). Then $R^p f_*\mathcal{F} = (f_*\mathcal{H}^p(\mathcal{F}))^\sharp$ by Grothendieck spectral sequence.

The Cech-to-Derived spectral sequence(6.3.2.13) is applied: $H^p(\{U_i \to U\}, \mathcal{H}^q(F)) \Rightarrow H^{p+q}(U, F)$, $\check{H}^p(U, \mathcal{H}^q(F)) \Rightarrow H^{p+q}(U, F)$ and $\check{H}^1(U, F) \cong H^1(U, F)$.

In particular, if $H^q(U_{i_0 i_1 \ldots i_r}, \mathcal{F}) = 0, q > 0$, then $H^p(\{U_i \to U\}, \mathcal{F}) = H^p(U, \mathcal{F})$(6.3.2.15). And it is enough to have $\check{H}^q(U_{i_0 i_1 \ldots i_r}, \mathcal{F}) = 0, q > 0$ by(6.3.2.16). ⌟

Cor. (17.5.3.10). A Qco sheaf on an affinoid space has vanishing higher sheaf cohomology by Tate's acyclicity(17.5.1.40) and(6.3.2.16). ⌟

Properties of Rigid K-Spaces

This subsubsection is strongly suggested to read after reading the parallel part of schemes.

Def. (17.5.3.11). A morphism is called a **closed immersion** if there is an admissible affinoid covering that it restricts to a closed immersion of affinoid spaces(It is compatible with definition(17.5.1.28) before by(17.5.3.15)). It is called an **open immersion** iff it is injective and the corresponding stalk maps are isomorphisms. The **(quasi-)separatedness, quasi-compactness, finiteness** are defined similarly as for schemes. ⌟

Lemma (17.5.3.12) [Nike's Trick]. In a rigid analytic K-space X and $\operatorname{Sp} A$, $\operatorname{Sp} B$ be affinoid subspaces, then there is an admissible affinoid covering of $\operatorname{Sp} A \cap \operatorname{Sp} B$. ⌟

Proof: This is analogous to the scheme case(6.4.1.1), but the proof is different: X has an admissible covering, this restricts to an admissible covering of $\operatorname{Sp} A \cap \operatorname{Sp} B$, and any admissible covering can be refined by an affinoid admissible covering. □

Prop. (17.5.3.13) [Affinoid Communication Theorem]. A property P of affinoid open subsets of X is called **affiniod local** if: $\operatorname{Sp} A$ has $P \Rightarrow$ all affinoid subdomains of $\operatorname{Sp} A$ has P, and any admissible affinoid cover of $\operatorname{Sp} A$ has $P \Rightarrow \operatorname{Sp} A$ has P. Notice a stalk-wise property is obviously affine-local.

Now if we call X has $\widetilde{P}$ if there is an admissible affinoid covering $A_i \to X$ that A_i has P. Then the following are equivalent:

- all open affinoid subsets of X has P.
- all open subspace of X has $\widetilde{P}$.
- X has a cover of open subspaces that has $\widetilde{P}$.
- X has $\widetilde{P}$.

⌟

Proof: The proof is the same as the scheme case(6.4.1.2). □

Prop. (17.5.3.14). Separated morphism is quasi-separated because closed immersion is affinoid hence quasi-compact(17.5.1.3). ⌟

Prop. (17.5.3.15) [Finite Morphism]. For a morphism $\varphi : X \to Y$ of rigid K-spaces

- It is finite iff the inverse image of any affinoid space is affinoid, and $\varphi_*\mathcal{O}_Y$ is a coherent $\mathcal{O}_X$-module. In particular, finiteness is local on the target because coherence do.
- It is closed immersion iff it is finite and $\mathcal{O}_Y \to \varphi_*\mathcal{O}_X$ is surjective, this shows the definition of closed immersion is compatible with before.

⌟

Proof: Coherence is affinoid local on the target by Kiehl's theorem, so it suffices to prove the inverse image of any affinoid space is affinoid for a finite morphism: Consider any affinoid subdomain $U \subset X$ with inverse image $\varphi^{-1}(U)$, by Kiehl's theorem, $B = \mathcal{O}_X(f^{-1}(U))$ is finite over $A = \mathcal{O}_Y(U)$, thus can be given an affinoid K-algebra structure(11.2.4.33). Now

$$\varphi^{-1}(U) \xrightarrow{\chi} \operatorname{Sp} B \xrightarrow{\rho'} \operatorname{Sp} A$$

χ is locally an isomorphism, as ρ is finite, so χ is an isomorphism.

The second assertion is because locally $\mathcal{O}_Y, \varphi_*\mathcal{O}_X$ are both Qco so surjectivity is equivalent to the global section is surjective(17.5.3.1). □

Prop. (17.5.3.16). Closed/Open immersion, quasi-compactness, (quasi-)separatedness are all local on the target, and stable under base change. ⌟

Proof: Closed immersion is local on the target because finiteness do and surjectiveness of $\mathcal{O}_Y \to \varphi_*\mathcal{O}_X$ is checked locally. Open immersion is local on the target because stalk and injectivity are all checked locally.

Then Closed/Open immersion are stable under base change because the affinoid case is true(17.5.1.29).

Quasi-compact is easily seen local on the target and stable under base change.

(Quasi-)Separateness is local on the target because closed immersion and quasi-compact do.

(Quasi-)Separateness is stable under base change because closed immersion and quasi-compact do, because diagonal commutes with base change(4.1.1.48). □

Prop. (17.5.3.17). Morphisms between affinoid K-spaces are separated. Moreover, because of localness, any finite morphism is separated. ⌟

Proof: The diagonal is $\operatorname{Sp} A \to \operatorname{Sp} A\widehat{\otimes}_B A$, whose ring map is surjective. □

Prop. (17.5.3.18). By(4.1.1.50), for $X \to S$ and $Y \to S$, the map $X = X \times_Y Y \to X \times_S Y$ is an immersion. It is closed immersion if $Y \to S$ is separated, and it is qc if $Y \to S$ is quasi-separated. ⌟

Cor. (17.5.3.19). If $s : S \to X$ is a section of $f : X \to S$, the above proposition applies to this case, because $S = S \times_X X \to S \times_S X = X$. ⌟

Prop. (17.5.3.20). A morphism is quasi-separated iff there is an admissible affinoid covering W_i that, for any two affinoid open U, V that are mapped to an affinoid open, their intersection is quasi-compact. This is because quasi-compact is local on the target.

A morphism is separated iff there is an admissible affinoid covering W_i that, for any two affinoid open U, V that are mapped to an affinoid open, their intersection is affinoid open and $\mathcal{O}(U)\widehat{\otimes}_{\mathcal{O}(W_i)}\mathcal{O}(V) \to \mathcal{O}(U \cap V)$ is surjective. This is because closed immersion is local on the target(17.5.3.16). ⌟

Cor. (17.5.3.21). If $g \circ f$ is (quasi-)separated, then so is f. ⌟

Cor. (17.5.3.22). If X is (quasi-)separated, then $X \to Y$ is (quasi-)separated. ⌟

4 Proper Mapping Theorem

Def. (17.5.4.1). For a rigid space X over affinoid space Y, if $U \subset U' \subset X$ be affinoid subspaces, U is called **relatively compact** in U' iff there is a set of affinoid generators f_i of $\mathcal{O}_X(U')$ over $\mathcal{O}_Y(Y)$ that $|f_i(x)| < 1$ on U. This is denoted by $U \Subset_Y U'$. ⌟

Prop. (17.5.4.2). If X_1, X_2 are affinoid spaces over an affinoid space Y, and U_i are affinoid space of X_i, then

- if $U_1 \Subset_Y X_1$, then $U_1 \times_Y X_2 \Subset_{X_2} X_1 \times_Y X_2$.
- if $U_i \Subset_Y X_i$, then $U_1 \times_Y U_2 \Subset_Y X_1 \times_Y X_2$.
- If $U_i \Subset_Y X_i$, and X_i are affinoid subspaces of a rigid space separable over Y, then $U_1 \cap U_2 \Subset_Y X_1 \cap X_2$.
- If $U_1 \Subset_Y X_1$, and $i : T \to X_1$ is a closed immersion, then $i^{-1}(U_1) \Subset_Y i^{-1}(X_1)$.

The proof is easy. For the last one, should notice $|f(x)| = |f(i(x))|$, because it is closed immersion, so the residue field is the same. ⌟

Def. (17.5.4.3)[Proper Morphism]. A **proper** morphism $\varphi : X \to Y$ of rigid K-spaces is a separated morphism that there is an admissible affinoid covering Y_i of Y that there are two admissible affinoid coverings X_{ij}, X'_{ij} of $\varphi^{-1}(Y_i)$ that $X_{ij} \Subset_{Y_i} X'_{ij}$ for any i, j. ⌟

Prop. (17.5.4.4). Properness is stable under base change and composition ⌟

Proof: The base change follows directly from(17.5.4.2).

For the composition, Cf.[Formal and Rigid Geometry P131](difficult). □

Prop. (17.5.4.5). Properness is local on the target. ⌟

Proof: This is because separatedness is local on the target(17.5.3.16) and the second condition of properness is itself local. □

Prop. (17.5.4.6). If $g \circ f : X \to Y \to Z$ is proper and g is separated, then f is proper. ⌟

Proof: By(17.5.3.18), $\tau : X \to X \times_Z Y$ is closed immersion, and f is separated by(17.5.3.21). Now proper is local, so we may assume Z is affinoid, so there are two admissible covering X_i, X_i' of X that $X_i \Subset_Z X_i'$, and choose an admissible affinoid covering $Y_i \to Y$, then $X_j \times_Z Y_i, X_j' \times_Z Y_i$ are admissible coverings of Y_i that is $X_j \times_Z Y_i \Subset_{Y_i} X_j' \times_Z Y_i$. And it can be pulled back to an affinoid admissible coverings of $f^{-1}(Y_i)$ that $\tau^{-1}(X_j \times_Z Y_i) \Subset_{Y_i} \tau^{-1}(X_j' \times_Z Y_i)$, because τ is closed immersion. So $X \to Y$ is proper. □

Prop. (17.5.4.7). Finite morphism is proper, in particular, closed immersion is proper. ⌟

Proof: Finite morphism is separated by(17.5.3.17), and locally, assume both space are affinoid, $X = \mathrm{Sp}\, B \to \mathrm{Sp}\, A = Y$, then B is a finite A-module, in priori a f,g, A-algebra, so there is a set of generators f_i of B over A that (by multiplying a constant in K^*) $|f_i|_{sup} < 1$(11.2.4.21), so $X \Subset_Y X$, hence it is proper. □

Prop. (17.5.4.8) [Proper and Analytification]. For a morphism between schemes locally of f.t. over K, it is proper iff its rigid analytification is proper. ⌟

Proof: Cf.[U. Köpf, Über eigentliche Familien algebraischer Varietäten über affinoiden Räumen. Schriftenr. Math. Inst. Univ. Münster, 2. Serie, Heft 7 (1974) Satz 2.16]. □

For the following: Cf.[Formal and Rigid Geometry P132].

Prop. (17.5.4.9) [Proper Mapping theorem, Kiehl]. The higher direct images of a proper map of rigid analytic spaces takes coherent sheaves to coherent sheaves. ⌟

Proof: □

Prop. (17.5.4.10). For a scheme X locally of f.t. over K, an $\mathcal{O}_X$-module $\mathcal{F}$ on X gives rise to an $\mathcal{O}_{X^{rig}}$-module on X^{rig}, and it is coherent iff $\mathcal{F}$ is coherent. ⌟

Proof: □

Prop. (17.5.4.11). For a proper scheme over K, $H^q(X, \mathcal{F}) \cong H^q(X^{rig}, \mathcal{F}^{rig})$ for $\mathcal{F}$ coherent. ⌟

Proof: □

Prop. (17.5.4.12). When X is proper, coherent sheaves on X^{rig} corresponds to coherent sheaves on X. This gives an analog of Chow's theorem when applied to $X = \mathbb{P}^n_K$ and $\mathcal{F}'$ is a sheaf of ideals in $\mathcal{O}_{X^{rig}}$. ⌟

Proof: □

5 Formal Geometry

Main references for this subsection is [Bos15], [Hartshorne] and [Topics in Algebraic Geometry, Illusie].

Def. (17.5.5.1) [Formal Spectrum Spf A]. Let A be a complete adic ring(11.2.1.8) with an ideal of definition $\mathfrak{a}$ that the A is $\mathfrak{a}$-adically complete and separated. Then we let $\mathrm{Spf}\, A$ be the ringed space with underlying topological space $\mathrm{Spec}(A/\mathfrak{a})$(open primes of A), and the structure sheaf $\mathcal{O}$ that $\mathcal{O}(D(f)) = A\langle f^{-1}\rangle$(11.2.1.10). ⌟

Proof: To construct this sheaf, we first check that $\mathcal{O}(D(f)) = A\langle f^{-1}\rangle = \varprojlim_n (A/\mathfrak{a}^n[f^{-1}])$ defines a sheaf on the site of subspaces of Spf A of the form $D(f)$: For any open covering $\{D(f_i)\}$ of $D(f)$, there are exact sequences:

$$0 \to (A/\mathfrak{a}^n)_f \to \prod_i (A/\mathfrak{a}^n)_{f_i} \to \prod_{i,j} (A/\mathfrak{a}^n)_{f_i f_j}$$

by(5.4.2.3). Then we take inverse limit, which is exact by Mittag-Leffler(5.9.3.2), to get an exact sequence, which is just the sheaf condition of $\mathcal{O}$. Then, we can use(6.1.2.25) to extend this sheaf to a sheaf on Spf A. □

Prop. (17.5.5.2) [Stalks of Spf A**].** Let $x \in$ Spf A correspond to a prime $\mathfrak{p}_x$ in A. Then the stalk of Spf A at x is just $\mathcal{O}_x = \varinjlim_{x\in D(f)} A\langle f^{-1}\rangle$, which is a local ring with maximal ideal $\mathfrak{m}_x$ containing $\mathfrak{p}_x\mathcal{O}_x$. Moreover, $\mathfrak{m}_x = \mathfrak{p}_x\mathcal{O}_x$ iff $\mathfrak{a}$ is f.g.. So Spf A is a local ringed space, called the **affine formal scheme** of A. ⌟

Proof: Cf.[Bos15]P159.**?** □

Remark (17.5.5.3). In many case, for example in Scholze's treatment of the p-adic geometry, the ideal of definition $\mathfrak{a}$ is assumed to be f.g., because we need this to show that the $\mathfrak{a}$-adic completion of $A[f^{-1}]$ is $(\mathfrak{a})$-adically complete(5.2.3.6), so that we can interpret $D(f) \subset$ Spf A as an affine formal scheme Spf$(A\langle f^{-1}\rangle)$(11.2.1.11).

Another way to get around this finiteness condition is to consider formal spectrum for a larger class of rings, called the **admissible rings**, which is a complete and separated topological ring with a basis consisting of open ideals, and with an ideal of definition $\mathfrak{a}$ that $\mathfrak{a}^n \to 0$ for $n \to 0$. ⌟

Prop. (17.5.5.4) [Affine Formal Adjointness]. Morphisms between local topologically ringed spaces Spf $B \to$ Spf A corresponds to continuous homomorphisms $A \to B$. ⌟

Def. (17.5.5.5) [Formal Schemes]. The category of **formal schemes** is the full subcategory of the category of local topologically ringed topological spaces $(X, \mathcal{O}_X)$ consisting of objects that is locally isomorphic to an affine formal scheme Spf A.

The category of formal schemes contains the category of schemes, by mapping Spec A to Spf A, where A is endowed with the discrete topology. ⌟

Prop. (17.5.5.6) [Glueing and Fiber Products]. Formal Schemes can easily be glued, and also spectrum adjointness holds as in(17.5.2.5). Finally there are fibered products, constructed as in(6.2.7.15), where the affine case corresponds to completed tensor product(11.2.1.12). ⌟

Def. (17.5.5.7)[Formal Completion of Schemes Along a Closed Subscheme]. Let X be a scheme and Y a closed subscheme of X defined by a Qco ideal $\mathcal{I} \subset \mathcal{O}_X$, then consider the sheaf $\mathcal{O}_Y$ defined by restricting the projective limit $\varprojlim_n \mathcal{O}_X/\mathcal{I}^n$ to Y, then $(Y, \mathcal{O}_Y)$ is a locally topologically ringed space, called the **formal completion** of X along Y. ⌟

Noetherian Adic Formal Schemes

Cf.[Hartshorne Chap2.9] and [Sta]30.23. and Illusie.

Def. (17.5.5.8) [Noetherian Formal Adic Schemes]. ⌟

Def. (17.5.5.9) [Coherent Sheaves on Noetherian Formal Adic Schemes]. ⌟

Prop. (17.5.5.10). Let A be a Noetherian ring and I an ideal, let X be a proper scheme over A and $\mathcal{F}$ a coherent sheaf on X, then for any $p \geq 0$, the inverse systems $(H^p(X, I^n\mathcal{F}))$ and $(I^n H^p(X, \mathcal{F}))$ are isomorphic pro-A-modules. ⌟

Proof: Cf.[Sta]02OA. □

Thm. (17.5.5.11) [Theorem of Formal Functions]. Let A be a Noetherian ring with an ideal I, X be a proper scheme over A and $\mathcal{F}$ a coherent scheme on X. Then for any $p \geq 0$, the system of maps

$$H^p(X, \mathcal{F})/I^n H^p(X, \mathcal{F}) \to H^p(X, \mathcal{F}/I^n\mathcal{F})$$

induce an isomorphism of limits

$$H^p(X, \mathcal{F})^\wedge \cong \varprojlim_n H^p(X, \mathcal{F}/I^n\mathcal{F}).$$

⌟

Proof: Cf.[Sta]02OC. □

Prop. (17.5.5.12) [Grothendieck's Existence Theorem]. Cf.[Sta]0883. ⌟

Prop. (17.5.5.13) [Grothendieck's Algebrization Theorem]. Cf.[Sta]089A. ⌟

6 Admissible Formal Schemes

Remark (17.5.6.1) [Setup]. For a good theory of Admissible formal schemes, let the base ring R be an adic ring with an ideal of definition I that satisfies either one of the following situation:

- R is an adic valuation ring with a principal ideal of definition.
- R is Noetherian and has no I-torsion.

⌟

Def. (17.5.6.2) [Admissible Formal Schemes]. Let R be an adic ring, then a formal R-scheme X is called **locally of topologically finite type/finite presentation/admissible** if there is an open affine covering $\operatorname{Spf} A_i$ of X that A_i satisfies those properties(11.2.1.13).

X is called **topologically of finite type** if it is locally of topologically finite type and quasi-compact. It is called **topologically of finite presentation** if it is locally of topologically finite presentation, quasi-compact and quasi-separated. ⌟

Prop. (17.5.6.3) [Induced Admissible Formal Subscheme]. Let X be a formal R-scheme that is locally of topologically finite type, and let $\mathcal{O}_X$ be its structure sheaf. Then we can look at the ideal sheaf $\mathcal{I} \subset \mathcal{O}_X$ consisting of all elements locally killed by a power of I^n. This is a qco sheaf, as $\mathcal{I}(U) = \{f \in \mathcal{O}(U) | I^n f = 0 \text{ for some } n\}$, because the quotient by the RHS is locally topologically of finite type and has no I-torsion, thus admissible, by(11.2.1.15), and admissibility is local(11.2.1.16).

In particular we can take the closed subscheme $X_{adm} \subset X$ corresponding to $\mathcal{I}$, then it is an admissible formal scheme, called the **induced admissible formal subscheme** of X. ⌟

7 Formal Models

Prop. (17.5.7.1)[Generic Fiber Functor]. Let R be a complete valuation ring of height 1 with field of fraction 1 with field of fraction K, then the functor $A \mapsto A \otimes_R K$ from the category of R-algebras topologically of finite type to the category of affinoid K-algebras ⌟

Proof: Cf.[Bos15]P174. □

Def. (17.5.7.2)[Formal Models]. In view of(17.5.7.1), one would like to describe all formal R-schemes that the generic fiber X_{rig} is isomorphic to a given rigid K-space X_K. But first notice $A \mapsto A \otimes_R K$ kills all R-torsion, in particular the generic fiber functor only depends on the induced admissible formal scheme X_{adm}(17.5.6.3). So given any rigid K-space X_K, any admissible formal R-scheme X satisfying $X_{rig} \cong X_K$ is called a **formal R-model** of X_K. ⌟

Def. (17.5.7.3)[Admissible Formal Blowing-up]. ⌟

17.6 p-adic Uniformizations

1 Mumford Curves

References are [Schottky Groups and Mumford Curves, 1980], [Mihran Papikian, Non-archimedean uniformization and monodromy pairing].

Def. (17.6.1.1) [p-adic Schottky Groups]. For $p \in \mathbf{P}$, a **p-adic Schottky group** is a discrete, f.g. free subgroup $\Gamma \subset PGL_2(\mathbb{Q}_p)$. ⌟

Prop. (17.6.1.2). A subgroup $\Gamma \subset PGL(2, \mathbb{Q}_p)$ is a p-adic Schottky group if it is discrete, f.g. and torsion-free. ⌟

Proof: Γ acts on the Bruhat-Tits building Δ of $PGL(2, \mathbb{Q}_p)$, and the stabilizer is $\Gamma \cap PGL(2, \mathbb{Z}_p)$, which is a finite group as Γ is discrete and $PGL(2, \mathbb{Z}_p)$ is compact. Thus it is trivial as Γ is torsion-free. Thus Γ acts freely on Δ, so Γ must be a free group.? □

Def. (17.6.1.3). A p-adic Schottky group Γ acts on $\mathbb{P}^1(\mathbb{C}_p)$. Denote $\mathcal{L}_\Gamma$ is the set of limit points of this action, $\Omega_\Gamma = \mathbb{P}^1(\mathbb{C}_p) - \mathcal{L}_\Gamma$. ⌟

Thm. (17.6.1.4) [Mumford]. Let Γ is a p-adic Schottky group of rank g, then there is a smooth complete curve $X_\Gamma/\mathbb{Q}_p$ of genus g with an analytic isomorphism $\Omega_\Gamma/\Gamma \cong X_\Gamma(\mathbb{C}_p)$. Such a curve X_Γ is called a p-adic **Mumford curve**. ⌟

Proof:

□

Thm. (17.6.1.5) [Mumford]. Let Γ is a p-adic Schottky group of rank $g \geq 2$, then the corresponding Mumford curve X_Γ has split degenerate stable reduction. Conversely, and smooth complete curve over $\mathbb{Q}_p$ with split degenerate stable reduction is a Mumford curve.

Where split degenerate reduction means that the normalization of all components of $\widetilde{X}$ are $\mathbb{F}_p$-rational, and all nodes are $\mathbb{F}_p$-rational with two $\mathbb{F}_p$-rational branches. ⌟

Proof:

□

Prop. (17.6.1.6) [Herrlich]. Suppose $p \in \mathbf{P}$ and $X/\mathbb{Q}_p$ is a Mumford curve with genus $g \geq 2$, then

$$\#\operatorname{Aut}(X) \leq \begin{cases} 84(g-1) & ,p=2 \\ 24(g-1) & ,p=3 \\ 30(g-1) & ,p=5 \\ 12(g-1) & ,p=3 \end{cases}$$

⌟

Proof: □

17.7 Rapoport-Zink Spaces

Main references are [Period Spaces for p-Divisible Groups, Rapoport-Zink], [Kot85], [On the Classification and Specialization of F-Isocrystals with Additional Structure, Rapoport-Richartz, 1996] and [Rap95].

Notation (17.7.0.1).

- Use notations from18.4.

⌟

1 $B(G)$ and Isocrystals with Structures

Notation (17.7.1.1).

- Let $L = K_0E$ where $E \in p-\texttt{LField}$. Thus $e(L) = e(E)$.
- Let $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/\mathbb{Q}_p$ be a linear algebraic group.

⌟

Remark (17.7.1.2). The σ-conjugacy classes of $GL(n; K_0)$ are in bijection with the isomorphism classes of n-dimensional isocrystals, so the Dieudonné-Manin classification of isocrystals can be translated to a classification of σ-conjugacy classes of $GL(n; K_0)$. And this generalizes to other connected reductive group G/K as well, and the description of the set of σ-conjugacy classes $B(G)$ are useful in studying the points mod p of Shimura varieties. ⌟

Def. (17.7.1.3)[$B(G)$]. Denote $B(G) = H^1(\langle\sigma\rangle, G(K_0))$, which is equal to the set of φ-conjugate classes of $G(K_0)$, i.e. $x \sim y \in G(K)$ iff $x = gx\sigma(g)^{-1}$ for some $g \in G(K)$. ⌟

The Newton Map

Def. (17.7.1.4) [Equivalent Pairs]. Two pairs $(\mu, b), (\mu', b')$ as in(17.7.1.24) are called **equivalent** if there exists $g \in G(K_0)$ s.t. $b' = gb\sigma(g)^{-1}$, and the cocharacters $\mu', g\mu g^{-1}$ define the same filtration on $\mathrm{Rep}_{\mathbb{Q}_p}(G)$. Equivalent, $\mathcal{I}_{b,\mu} = \mathcal{I}_{b',\mu'}$. ⌟

Def. (17.7.1.5) [Slope Morphisms]. Let $\mathbb{D} = \mathrm{Spec}\,\mathbb{Q}_p[\{T^{1/k}\}_{k\in\mathbb{Z}}] = \mathbb{D}(\mathbb{Q})_{\mathbb{Q}_p}$ be the pro-algebraic torus over $\mathbb{Q}_p$ with character group $\mathbb{Q}$, and $b \in G(K_0)$, then there is a morphism $\nu_b : \mathbb{D}_{K_0} \to G_{K_0}$, called the **slope morphism** associated to b, which is defined as follows:

For any $(\rho, V) \in \mathrm{Rep}_{\mathbb{Q}_p}(G)$, there is an associated isocrystal defined in(17.7.1.20), then there is a morphism $\nu_\rho \in \mathrm{Hom}_{K_0}(\mathbb{D}, \mathrm{GL}(V))$ that $\mathbb{D}$ acts on the isotypical component V_λ of V by the character $\lambda \in \mathbb{Q} = X^*(\mathbb{D})$. Then for any $x \in \mathbb{D}(R)$, the mapping $\rho \to \nu_\rho(x)$ gives an automorphism of the standard fiber functor on $\mathrm{Rep}_{\mathbb{Q}_p}(G)$, so by Tannakian duality corresponds to a unique element $y \in G(R)$ that $\rho(y) = \nu_\rho(x)$ for any ρ. The homomorphism $x \mapsto y$ is functorial in R and thus defines an element $\nu \in \mathrm{Hom}_L(\mathbb{D}, G)$. ⌟

Remark (17.7.1.6). Notice the group $\mathbb{Q}^*$ acts on $\mathbb{D}$, and for $s \in \mathbb{Q}^*$ and $v \in \mathrm{Hom}_{K_0}(\mathbb{D}, G)$, denote by v^s the composite $\mathbb{D}_{K_0} \xrightarrow{s} \mathbb{D}_{K_0} \xrightarrow{v} G_{K_0}$, and $\mathbb{D} \to \mathbb{G}_m$ the natural morphism, then for any v, there is a suitable s that sv factors through a morphism also denoted by $\nu^s : \mathbb{G}_{m,K_0} \to G_{K_0}$, as G is algebraic. ⌟

Prop. (17.7.1.7) [Characterizing the Slope Morphism]. The slope morphism associated to $b \in G(K_0)$ can be characterized intrinsically to be the unique morphism $\nu \in \mathrm{Hom}_L(\mathbb{D}, G)$ s.t.: There exists some $s \in \mathbb{Z}_+, c \in G(L)$ that

- $s\nu \in \mathrm{Hom}_L(\mathbb{G}_m, G)$,
- $c\nu^s c^{-1}$ is defined over $\mathbb{Q}_{p^s}$.
- $c(b\sigma)^s c^{-1} = c\nu^s(p)c^{-1}\sigma^s$.

⌟

Proof: Cf.[Kottwitz, P13]. □

Cor. (17.7.1.8). σ acts on $\nu_b \in \mathrm{Hom}_{K_0}(\mathbb{D}, G)$, and it satisfies the following properties:

- $\nu_{\sigma(b)} = \sigma(\nu_b)$.
- $\nu_{gb\sigma(g)^{-1}} = g\nu_b g^{-1}$.
- $b\nu^\sigma b^{-1} = \nu$.

⌟

Proof: 1 follows from the fact $(V \otimes_{\mathbb{Q}_p} K_0, b\sigma) \xrightarrow{\sigma,\cong} (V \otimes_{\mathbb{Q}_p} K_0, \sigma(b)\sigma)$.

2 follows from the fact $(V \otimes_{\mathbb{Q}_p} K_0, b\sigma) \xrightarrow{\rho(g),\cong} (V \otimes_{\mathbb{Q}_p} K_0, gb\sigma(g)^{-1}\sigma)$by(17.7.1.20).

3 follows from 2 as $b = b\sigma(b)\sigma(b)^{-1}$. □

Cor. (17.7.1.9) [Newton Map]. If G/F is a connected reductive group with a maximal torus T and Weyl group W_T, we get a map of sets

$$\nu : B(G) \to \mathcal{N}(G) = (\mathrm{int}(G(K_0))\backslash \mathrm{Hom}_{K_0}(\mathbb{D}, G)^{\langle\sigma\rangle}) = (X_*(T)_{\mathbb{Q}}/W_T)^{\mathrm{Gal}_{\mathbb{Q}}}$$

called the **Newton map**, and it is functorial in G. It follows from the Dieudonné-Manin classification(8.8.4.13) that when $k = \overline{k}$ and $G = \mathrm{GL}(n)$, this Newton map is injective. ⌟

Def. (17.7.1.10) [Kottwitz-Decent Elements]. $[b] \in B(G)$(17.7.1.3) is called **Kottwitz-decent** if there is some $s \in \mathbb{Z}_+$ and some $b \in [b]$ that $\nu_b^s : \mathbb{D} \to G$ factors through $\mathbb{D} \to \mathbb{G}_m$ and

$$(b\sigma)^s = \nu_b^s(p)\sigma^s \in G(K_0) \rtimes \langle\sigma\rangle.$$

it can be verified that this doesn't depends on the choice of b. ⌟

Prop. (17.7.1.11). If G is connected, then any $[b] \in B(G)$ is Kottwitz decent(17.7.1.10). ⌟

Proof: Cf.[Kottwitz]. □

Prop. (17.7.1.12). If $b \in G(K_0)$ satisfies the descent condition for s in(17.7.1.10), then $b \in G(\mathbb{Q}_{p^s})$ and ν is defined over $\mathbb{Q}_{p^s}$. ⌟

Proof: Set $b_s = b\sigma(b)\ldots\sigma^{s-1}(b)$, then iterating(17.7.1.8), $b_s\nu^{\sigma^s}b_s^{-1} = \nu$. And we have $b_s = \nu^s(p)$, so $\nu^{\sigma^s} = \nu$, so ν is defined over $\mathbb{Q}_{p^s}$.

To show the first assertion, notice $(b\sigma)(b\sigma)^s = (b\sigma)^s(b\sigma)$ shows

$$\nu^s(p)\sigma^s b\sigma = b\sigma\nu^s(p)\sigma^s = \nu^s(p)b\sigma^{s+1}(17.7.1.8).$$

and then $b\sigma^s = \sigma^s b$. □

Cor. (17.7.1.13). If $b_1, b_2 \in [b]$ are Kottwitz-decent w.r.t the same $s \in \mathbb{Z}_+$, then they are conjugate w.r.t. $G(K_0 \cap \mathbb{Q}_{p^s})$.

In particular, for any descent $b \in G(\mathbb{Q}_{p^s})$ and any $V \in \mathrm{Rep}_{\mathbb{Q}_p}(G)$, the induced isocrystal(17.7.1.20) is defined over the field $\mathbb{Q}_{p^s}$, and it only depends on $[b] \in B(G)$. ⌟

Proof: Suppose $b_2 = gb_1\sigma(g)^{-1}$, then $\nu_2 = g\nu_1 g^{-1}$, and the descent equations are

$$(b_1\sigma)^2 = s\nu_1(p)\sigma^s, \quad g(b_1\sigma)^s g^{-1} = gs\nu_1(p)g^{-1}\sigma^s.$$

Comparing these two, g commutes with σ^s, so $g \in G(K_0 \cap \mathbb{Q}_{p^s})$. □

Prop. (17.7.1.14) [Scheme J and Conjugacy Classes]. For $b_1, b_2 \in G(K_0)$, then the functor

$$J(R) = \{g \in G(R \otimes_{\mathbb{Q}_p} K_0) | g(b_1\sigma) = (b_2\sigma)g\}$$

is representable by a smooth affine scheme over $\mathbb{Q}_p$. When $b_1 = b_2 = b$, denote the scheme by J_b.

Assume $b_1, b_2 \in G(W(k')[\frac{1}{p}])$ where $k' = \overline{k'} \subset k$, and J' the corresponding smooth affine scheme, then $J' \to J$ is an isomorphism. In particular, $B(G) \to B'(G)$ is injective, and it is surjective if G is connected and $k = \overline{k}$. ⌟

Proof: Choose an embedding $G \subset \mathrm{GL}(n)_{\mathbb{Q}_p}$ and let G be defined by functions $f_1, \ldots, f_k$, consider the functor:

$$F(R) = \{g \in \mathrm{Mat}(n; R \otimes_{\mathbb{Q}_p} K_0) | g = b\sigma(g)b^{-1}\},$$

then it is representable by an affine space by(17.7.1.15) applied to the σ-linear map $g \mapsto b\sigma(g)b^{-1}$.

So there is a f.d. $\mathbb{Q}_p$-vector space $W \subset \mathrm{Mat}(n; K_0)$ that $F(R) = W \otimes_{\mathbb{Q}_p} R$. Choose a basis (A_i) of W, then $J(R)$ is just the subfunctor of $r_i \in R$ that

$$f_k(\sum r_i A_i) = 0, \quad \det(\sum r_i A_i) \neq 0.$$

Taking a basis of K_0 over $\mathbb{Q}_p$, then these are polynomials with coefficients in $\mathbb{Q}_p$. It is automatically smooth by Cartier's theorem(9.1.4.2).

The assertion about base change follows from(17.7.1.15).

The surjectivity follows from(17.7.1.11) and(17.7.1.12). □

Lemma (17.7.1.15). Let N be a f.d. isocrystal over K_0 w.r.t. σ^s for some $s \neq 0$, then the following functor

$$F : \mathcal{CR}\mathrm{ing}_{\mathbb{Q}_p} \to \mathcal{A}\mathrm{b} : R \mapsto (V \otimes_{\mathbb{Q}_p} R)^{\varphi = \mathrm{id}}$$

is representable by a vector space over $\mathbb{Q}_p$. ⌟

Proof: $F(R) = V^{\varphi=\mathrm{id}} \otimes_{\mathbb{Q}_p} R$, so it suffices to show $\dim_{\mathbb{Q}_p} V^{\varphi=\mathrm{id}} < \infty$. Firstly assume that L is alg.closed, then this is a consequence of Dieudonné-Manin classification(8.8.4.13). This functor F doesn't depend on k as long as $k = \overline{k}$: if k'/k is a field extension and $k' = \overline{k'}$, then the corresponding functor F' defined by $N \otimes_{W(k)[\frac{1}{p}]} W(k)[\frac{1}{p}]$ coincide with F.(This is also by Dieudonné-Manin classification.) □

Cor. (17.7.1.16). Assume $[b] \in B(G)$ is Kottwitz-decent for $s \in \mathbb{Z}_+$(17.7.1.10), then J_b is a $\mathbb{Q}_{p^s}/\mathbb{Q}_p$-inner form of the centralizer $G_{\nu^s(p)}$(17.7.1.12). ⌟

Proof: The descent equation shows $b_s = s\nu(p)$, so the adjoint $b_{ad} : g \mapsto (b\sigma)g(b\sigma)^{-1} = b\sigma(g)b^{-1}$ defines an element in $H^1(G(\mathbb{Q}_{p^s}/\mathbb{Q}_p), \mathrm{Aut}(G_{s\nu(p)}(\mathbb{Q}_{p^s})))$, because

$$\sigma^k b_{ad} : g \mapsto ((\sigma(b\sigma^{-1}(g))b^{-1})) = \sigma^k(b)\sigma(g)\sigma^k(b)^{-1}.$$

so

$$b_{ad} \circ \sigma(b_{ad}) \circ \ldots \circ \sigma^{s-1}(b_{ad}) : g \mapsto b_s g b_s^{-1} = s\nu(p)g(s\nu(p))^{-1} = g.$$

So it defines an inner form, which is just

$$J'(R) = G_{s\nu(p)}(\mathbb{Q}_{p^s})^{b_{ad}\sigma} = \{g \in G_{s\nu(p)}(R \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^s}) | g(b\sigma) = (b\sigma)g\}$$

Now it suffices to show $J'(R)$ is just $J(R)$ defined in(17.7.1.14). For this, notice any $g \in J(R)$ commutes with $b\sigma$ thus commutes with $s\nu(p)$ by(17.7.1.8), and the descent condition $(b\sigma)^n = s\nu(p)\sigma^n$ shows it commutes with σ^n, so $g \in J'(R)$. □

Prop. (17.7.1.17) [Basic Elements]. Let G be a connected reductive group and $k = \overline{k}$, then the following are equivalent for $b \in G(K_0)$:

- The slope morphism ν factors through the center $Z(G)$ of G.
- b is σ-conjugate to an element in $T(K_0)$ where T is an elliptic maximal torus of G.
- J_b in(17.7.1.14) is an inner form on G.

In this case, b and its conjugacy class $\overline{b}$ are called **Kottwitz-basic**. The set of Kottwitz-basic classes in $B(G)$ is denoted by $B(G)_b$. ⌟

Proof: Cf.[Kottwitz]. □

Prop. (17.7.1.18). Situation as in(17.7.1.17), if $[G, G]$ is simply-connected, then $G \to G_{\mathrm{ab}}$ induces a bijection $B(G)_b \cong B(G_{\mathrm{ab}})$. In particular, $B(G)_b$ is trivial if G is semisimple and simply-connected. ⌟

Proof: Cf.[Kottwitz, P17]. □

F-Isocrystals with G-Structures

Def. (17.7.1.19) [Isocrystals with G-structures]. Given $S \in \mathcal{S}\mathrm{ch}^p$, an **Isocrystal with G-structures** over S is an exact faithful tensor functor(4.2.1.2)

$$M : \mathrm{Rep}_{\mathbb{Q}_p}(G) \to \text{F-Isoc}(S)(8.8.4.2).$$

The category of isocrystals with G-structures over S is denoted by $\text{F-Isoc}_G(S)$. ⌟

Prop. (17.7.1.20) [Associated Isocrystals with G-Structure]. For $b \in G(K_0)$, there is a functor

$$\mathcal{I}_b : \mathrm{Rep}_{\mathbb{Q}_p}(G) \to \text{F-Isoc}(k) : V \mapsto (V \otimes_{\mathbb{Q}_p} K_0, \rho(b) \circ (\mathrm{id} \otimes \sigma)).$$

this is an isocrystal with G-structures over K_0 associated to b.

If $g \in G(K_0)$ and $b' = gb\sigma(g)^{-1}$, then multiplying by g implies a natural isomorphism between $\mathcal{I}_b$ and $\mathcal{I}_{b'}$. ⌟

Cor. (17.7.1.21) [Isocrystals and $B(G)$]. From any isocrystal with G-structures on S, we get a function

$$S \to B(G) : s \mapsto [b]_s.$$

And if $k = \overline{k}$ and $S = \operatorname{Spec} k$, then the isomorphism classes of isocrystals with G-structure over S are in bijection with $B(G)$. ⌟

Proof: ? Cf.[RR96, P171]. □

Prop. (17.7.1.22) [Newton Map Constency]. If S is connected locally Noetherian, and $M \in \text{F-Isoc}_G(S)$ s.t. $\nu \circ b_M$ is constant, then b_M is constant. ⌟

Proof: Cf.[RR96, P173].? □

Cor. (17.7.1.23). If S is locally Noetherian, then $M \in \text{F-Isoc}_G(S)$, and $[b_0] \in B(G)_b$, then

$$\{s \in S | [b_M(s)] = [b_0]\} \subset S$$

is closed. ⌟

Proof: □

Weakly-Admissible Pairs

Prop. (17.7.1.24) [Associated Filtered Isocrystals]. Let K be a field extension of K_0, and $\mu : \mathbb{G}_{m,K} \to G_K$ be a cocharacter over K, then the associated isocrystal over K_0 prolongs to a filtered isocrystal over K(18.4.8.22),

$$\mathcal{I}_{b,\mu} : \mathrm{Rep}_{\mathbb{Q}_p}(G) \to \varphi\text{-}\mathcal{M}\mathrm{od}\,\mathrm{Fil}_K : V \mapsto (V \otimes_{\mathbb{Q}_p} K_0, \rho(b) \circ (\mathrm{id} \otimes \sigma), \mathrm{Fil}^\bullet_\mu),$$

where the filtration comes from μ by weight-filtrations(because $\mathbb{G}_m$ is diagonalizable(9.2.3.1)). ⌟

Def. (17.7.1.25) [Weakly-Admissible Pairs]. Let G be a reductive group, then a pair (μ, b) as in(17.7.1.24) is called a **(weakly)admissible pair** if for any $V \in \mathrm{Rep}_{\mathbb{Q}_p}(G)$, the filtered isocrystal $\mathcal{I}_b(V)$ is weakly admissible**??**(18.4.4.10).

It suffices to check this condition for one faithful representation V. ⌟

Proof: This is because for a faithful representation V, any $\mathbb{Q}_p$-representation appears as a direct summand of $V^{\otimes n} \otimes \widehat{V}^{\otimes m}$(18.5.1.16). Then the assertion follows from the fact direct summands and tensor products of weakly admissible filtered isocrystals are weakly admissible(18.4.8.26). □

2 Period Domain

Def. (17.7.2.1) [Associated Partial Flag Variety]. Let $[\mu] : \mathbb{G}_m \to G$ be a conjugacy class of cocharacters defined over a finite extension field $E/\mathbb{Q}_p$(18.5.2.5), then there is associated a faithful tensor functor

$$\mathrm{Rep}_{\mathbb{Q}_p} \to \mathrm{gr}^{\mathbb{Z}}_E \to \mathrm{Fil}_E$$

Now call two cocharacters equivalent if their associated functor are isomorphic. Consider the functor

$$\mathcal{CR}\mathrm{ing}_E \to \mathcal{S}\mathrm{et} : R \mapsto \{\text{the equivalence classes in the } G(R)\text{-conjugacy class of } \mu_R\}$$

and also consider the closed algebraic subgroup $P(\mu) \subset G$ over E:

$$P(\mu)(R) = \{g \in G(R) | g\mu_R g^{-1} \text{ is equivalent to } \mu_R\}$$

then the functor above is representable by the G_E-homogenous variety $\mathcal{F} = G_E/P(\mu) \in \mathcal{S}\mathrm{ch}\,/E$. ⌟

Prop. (17.7.2.2). $\mathcal{F}$ is a projective variety, or equivalently, $P(\mu)$ is a parobolic subgroup. ⌟

Proof: If V is a faithful representation in $\mathrm{Rep}_{\mathbb{Q}_p}(G)$, we denote $\mathrm{Flag}(V)$ the partial flag variety over $\mathbb{Q}_p$ which associates to any $\mathbb{Q}_p$-algebra R the filtration $\mathrm{Fil}^\bullet$ of $V \otimes_{\mathbb{Q}_p} R$ s.t. $\mathrm{gr}^i(R)$ are direct summands and $\mathrm{rank}\,\mathrm{Fil}^i = \dim_E \mathrm{Fil}^i_\mu(V_E)$. Then $\mathrm{Flag}(V)$ is a projective variety, by classical results, and there is a closed immersion

$$\mathcal{F} \hookrightarrow \mathrm{Flag}(V)_E$$

because the isocrystal on other representations are determined by this faithful representation. □

Def. (17.7.2.3)[p-adic Period Space]. Let $\breve{E}=E(\mathbb{Q}_p^{\mathrm{ur}})^\wedge$ be the completion of the maximal unramified extension of E, then there is a rigid-analytic structure on $\breve{\mathcal{F}}=\mathcal{F}_{\breve{E}}$. define the **$p$-adic period space** $(\breve{\mathcal{F}}_b^{\mathrm{weak.\,adm}})^{\mathrm{rig}}\subset\breve{\mathcal{F}}^{\mathrm{rig}}$ associated to $(G,b,[\mu])$ the set of points ξ conjugate to μ that (ξ,b) is weakly admissible.

Let J_b be the algebraic group associated to b as in(17.7.1.14), then $J_b(\mathbb{Q}_p)\subset G(K_0)$ acts on $\breve{\mathcal{F}}^{\mathrm{rig}}$, and it preserves the set $(\breve{\mathcal{F}}_b^{\mathrm{weak.\,adm}})^{\mathrm{rig}}$.

$(\breve{\mathcal{F}}_b^{\mathrm{weak.\,adm}})^{\mathrm{rig}}$ has a natural structure of an admissible open subset of $\breve{\mathcal{F}}^{\mathrm{rig}}$. if $b'=gb\sigma(g)^{-1}$, then $\mu\mapsto g^{-1}\mu g$ induces an isomorphism from $(\breve{\mathcal{F}}_b^{\mathrm{weak.\,adm}})^{\mathrm{rig}}$ to $(\breve{\mathcal{F}}_{b'}^{\mathrm{weak.\,adm}})^{\mathrm{rig}}$. Moreover, if b is Kottwitz-decent w.r.t. $s\in\mathbb{Z}_+$, then this admissible open subset is defined over $E\mathbb{Q}_{p^s}$. ⌟

Proof: Cf.[Rapoport Zink, P26]. □

3 Groups of EL/PEL Types

Def. (17.7.3.1) [Algebraic Groups of EL/PEL Types]. Let F be a finite étale algebra over $\mathbb{Q}_p$, B a finite central algebra over F, and $V\in\mathcal{M}\mathrm{od}_B^{\mathrm{fg}}$.

An **algebraic group of EL type** over $\mathbb{Q}_p$ is an algebraic group of the form $GL_B(V)$. They are related to the classification of p-divisible groups with an endomorphism and level structures.

Let $(-,-)$ be a non-degenerate alternating $\mathbb{Q}_p$-bilinear form on V together with a formal involution $*$ on B that

$$(bv,w)=(v,b^*w).$$

Let F_0 be the field of elements of F fixed by $*$.

An **algebraic group of PEL type** over $\mathbb{Q}_p$ is an algebraic group over $\mathbb{Q}_p$ given by

$$G(R)=\{g\in GL_B(V\otimes_{\mathbb{Q}_p}R)|\exists c\in X(G),\quad (gv,gw)=c(g)(v,w),\quad \forall v,w\}$$

⌟

Prop. (17.7.3.2) [Setups]. If G is an algebraic group of EL/PEL type, $K_0=W(\overline{\mathbb{F}_p})[\frac{1}{p}]$, $b\in G(K_0)$, then we associate to b and the natural representation of G on V the isocrystal

$$(N(V),\Phi)=(V\otimes_{\mathbb{Q}_p}K_0,b(1\otimes\sigma)).$$

This isocrystal is equipped with an action of B, and in the PEL case an alternating bilinear form

$$\psi:N(V)\otimes N(V)\to 1(n).$$

where $n=v_p(c(b))$. In fact, we can find some unit u that $c(b)=p^n u\sigma(u)^{-1}$, then the pairing is defined as

$$\psi(v,v')=u^{-1}(v,v'),$$

any other choices of u multiplies ψ by an element in $\mathbb{Z}_p^*$.

We will fix in addition a conjugacy class of cocharacters $\mu:\mathbb{G}_m\to G$ defined over a field E, and the associated homogenous algebraic variety $\mathcal{F}$ defined over E of filtrations(17.7.2.1). $\mathcal{F}$ is equipped with a B-action, as $G\in GL_B(V)$.

Notice in the PEL case, these filtrations satisfy $\mathcal{F}^i=(\mathcal{F}^{m-i+1})^\perp$, where $m=c\circ\mu\in\mathrm{Hom}(\mathbb{G}_m,\mathbb{G}_m)\cong\mathbb{Z}$. This is due to the fact $(kv,kw)=k^m(v,w)$ and the fact the pairing is non-degenerate. ⌟

Prop. (17.7.3.3) [Shimura Field]. Fix a conjugacy class of cocharacters $\{\mu\}$ defined over E and $\mu_0 \in \{\mu\}$, its corresponding filtration $\mathcal{F}_0^\bullet$, The field E in(17.7.3.2) can be described as the field of definition of the isomorphism class of $\mathcal{F}_0^\bullet$ as a B-invariant filtration, or equivalently as the finite extension of $\mathbb{Q}_P$ generated by the traces

$$\mathrm{tr}(d; \mathrm{gr}^i_{\mathbb{F}_0}(V \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p})), d \in B, i \in \mathbb{Z}.$$

And the filtration $\mathcal{F}$ is described as the functor that for any E-algebra R, $\mathcal{F}(R)$ is the set of filtrations $\mathcal{F}^\bullet$ of $V \otimes_{\mathbb{Q}_p} R$ by R-modules that are direct summands that

$$\mathrm{tr}(d; \mathrm{gr}^i_{\mathcal{F}}(V \otimes_{\mathbb{Q}_p} R)) = \mathrm{tr}(d; \mathrm{gr}^i_{\mathbb{F}_0}(V \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p})).$$

and moreover in the PEL case satisfies $\mathcal{F}^i = (\mathcal{F}^{m-i+1})^\perp$. ⌟

Proof: 1: The field of definition E of the conjugacy class $\{\mu\}$ is determined by Tannakian duality, so it suffices to check over which field these two filtrations are isomorphic as G-filtrations, but G is just the group fixing the B-module structure, so it suffices to show they are equivalent as B-modules, which is then determined by the traces, by(3.6.1.27).

2: It suffices to show $\mathcal{F}$ is a homogenous space under G. We restrict to the PEL case, the EL case is simpler. After base change from $\mathbb{Q}_p$ to $\overline{\mathbb{Q}_p}$, the data decomposes to the following types:

- (A) : $B = \mathrm{End}(W) \times \mathrm{End}(W^\vee)$ where W is a f.d. $\overline{\mathbb{Q}_p}$-vector space and $(u, v)^* = (v^t, u^t)$. And $V = W \otimes V' \bigoplus W^\vee \otimes V'^\vee$ where the pairing is natural and makes the sum orthogonal.

$$G = \{(1 \otimes g, c \cdot (1 \otimes g^{-t})| g \in GL(V'), c \in X(G)\}$$

- (C) : $B = \mathrm{End}(W)$ where W is a f.d. $\overline{\mathbb{Q}_p}$-vector space equipped with a symmetric bilinear form $(-,-)_W$ and $*$ is the transposition w.r.t it.
  And $V = W \otimes V'$ where V' is equipped with an alternating form $(-,-)_{V'}$ that $(-,-)_V = (-,-)_W \otimes (-,-)_{V'}$.

$$G = \{cg | g \in \mathrm{Sp}(V'), c \in X(G)\}$$

- (BD): As in (C), except that $(-,-)_W$ is skew-symmetric and $(-,-)_{V'}$ is symmetric.

$$G = \{cg | g \in SO(V'), c \in C(G)\}$$

Under this decomposition, the functor $\mathcal{F}$ in the proposition is represented by products of partial flags of V:

- (A) : $\mathcal{F}^i = W \otimes (\mathcal{F}')^i \bigoplus W^\vee \otimes ((\mathcal{F}')^{m+1-i})^\perp$ and the correspondence $\mathcal{F}^\bullet \mapsto (\mathcal{F}')\bullet$ identifies $\mathcal{F}$ with the partial flag variety of V' with fixed dimensions $\dim((\mathcal{F}')^i)$.
- (B, CD) : $\mathcal{F}^\bullet = W \otimes (\mathcal{F}')^\bullet$ and $\mathcal{F}$ is identified with the partial flag variety of V' of fixed dimensions $\dim((\mathcal{F}')^i)$ and $(\mathcal{F}')^i = ((\mathcal{F}')^{m+1-i})^\perp$.
  The (A) case G clearly acts transitively on $\mathcal{F}$, and the (B, CD) case $(\mathcal{F}')^i$ is isotropic for $i \geq (m+1)/2$, and it determines all other components, so G acts transitively, by Witt's theorem(14.5.2.3).

The reason is(3.6.3.27) and the fact representations of B is semisimple, then contemplating on the pairing condition. □

Prop. (17.7.3.4) [Examples of PEL Type]. Let $B = D$ be the quaternion algebra over $\mathbb{Q}_p$ and $*$ be the involution, i.e.

$$D = \mathbb{Q}_{p^2}[\Pi], \quad \Pi^2 = p, \quad \Pi a = \sigma(a)\Pi$$

and

$$a^* = \sigma(a), a \in \mathbb{Q}_{p^2}, \quad , \Pi^* = \Pi.$$

Let (V, ι) be a free D-module of rank n with a non-degenerate bilinear form satisfying the conditions in(17.7.3.1). Then G is a non-trivial inner form of the group GSp_{2n} of symmetric similitudes:

Firstly $\mathbb{Q}_{p^2} \otimes K_0 \cong K_0 \oplus K_0$, then $\mathbb{Q}_{p^s}$ acts on $K_0 \oplus K_0$ by $a(x, y) = ax, \sigma(a)y)$. As V is a $\mathbb{Q}_{p^2}$-vector space, there is a decomposition

$$V = V_0 \oplus V_1$$

where $\mathbb{Q}_{p^2}$ acts on V_i by $a(v) = v.\sigma^i(a)$, then G_{K_0} is just GSp_{2n,K_0}, and $G \neq GSp_{2n}$ as the Galois action σ on $\mathbb{Q}_{p^2} \otimes K_0$ and $K_0 \cong K_0 \oplus K_0$ are different.

Take $b \in G(K_0)$ the element with $c(b) = p$ and the corresponding isocrystal (N, Φ) is isotypical of slope $1/2$. N decomposes as $N_0 \oplus N_1$. Notice now Π and $\Phi = b\sigma$ interchanges N_i, and $\Pi\Phi = \Phi\Pi$. Also N_i is isotropic: For $v, w \in N_i, a \in \mathbb{Q}_{p^2}$,

$$a(v, w) = (av, w) = (\iota(\sigma^i(a))v, w) = (v, \iota(\sigma^{i+1}(a))w) = (v, \sigma(a)w) = \sigma(a)(v, w)$$

so $(v, w) = 0$.

We can define a new non-degenerate alternating form

$$\langle -, - \rangle : N_0 \times N_0 \to K_0 : \langle v, v' \rangle = (v, \Pi v')$$

and also a σ-linear endomorphism of N_0: $\Phi_0 = \Pi^{-1} \circ \Phi|_{N_0}$. From the condition, $v_p(\det \Phi_0) = 0$, and Φ has all the slopes 0. Also $\langle \Phi_0 v, \Phi_0 w \rangle = \sigma(\langle v, w \rangle)$, as

$$\langle \Phi_0 v, \Phi_0 w \rangle = (\Pi^{-1}\Phi v, \Phi w) = (\Pi^{-1} b\sigma v, b\sigma w) = \sigma(v, \Pi w) = \sigma(\langle v, w \rangle).$$

so this alternating form is defined over $\mathbb{Q}_p$, denoted by $(V_0, \langle -, - \rangle)$, and Φ_0 corresponds to σ. Then $J_b = GSp(V_0, \langle -, - \rangle)$.

Next we consider

$$(0) = \mathcal{F}_0^2 \subset \mathcal{F}_0^1 \subset \mathcal{F}_0^0 = V \otimes \overline{\mathbb{Q}_p}$$

be a filtration where $\mathcal{F}_0^1$ be a D-invariant Lagrangian subspace. This corresponds to a cocharacter $\mu \to G$, and $\mathcal{F}$ is just the $\mathbb{Q}_{p^2}$ variety of D-invariant Lagrangian subspaces of $V_{\mathbb{Q}_{p^2}}$. By(17.7.3.3), the Shimura field is $\mathbb{Q}_p$.

Let $\mathcal{F} \subset \mathcal{F}(K)$ where K/K_0 is a field extension, then

$$\mathcal{F} = \mathcal{F}_0 \oplus \mathcal{F}_1$$

where $\mathcal{F}_i \in N_0 \otimes_{K_0} K$, as $\mathcal{F}$ is Π-invariant. Now $\mathcal{F}_0$ is also a Lagrangian subspace of $(V_0, \langle -, - \rangle)$. $\mathcal{F}(K)$ identifies the K-points of the Grassmannian of Lagrangian subspaces of $(V_0, \langle -, - \rangle)$. ⌟

Cor. (17.7.3.5). Under the above identification, the subset $\mathcal{F}^{wa}(K)$ of the Grassmannian of Lagrangian spaces $\mathcal{F}$ of $(V_0 \otimes K, \langle -, - \rangle)$ is characterized by $\mathcal{F}$ satisfying the the following conditions:

For all totally isotropic subspaces $W_0 \subset V_0$, we have $\dim_K \mathcal{F} \cap (W_0 \otimes K) \leq 1/2 \dim W_0$. ⌟

Proof: It's clear $\mu(N,\Phi,\mathcal{F})=0$, so weakly-admissibility is equivalent to semi-stability. The uniqueness of the HN-filtration of $\mathcal{F}$ implies its D-invariance, thus semi-stability is equivalent to the fact that for any subspace $P\subset N$ stable under Φ and D-action, we have

$$\dim_K(\mathcal{F}\cap(P\otimes_{K_0}K))\leq v_p(\det(\Phi;P)).$$

Now Φ is isotypical with slope $1/2$, $v_p(\det(\Phi;P))=\frac{1}{2}\dim P$, and the D-invariance of P is equivalent to $P=P_0\oplus P_1$ and the Φ-invariance of P is equivalent to the Φ_0-invariance of P_0, i.e. P_0 is a $\mathbb{Q}_p$-rational subspace $W_0\subset V_0$.

Finally we show it suffices to check for totally isotropic subspaces: Let W_0' be the radical of W_0, then there is a non-singular alternating form on W_0/W_0', then the image of $\mathcal{F}_0'\cap(P\otimes_{K_0}K)$ in this quotient is a totally isotropic space, thus has dimension$\leq\frac{1}{2}\dim(W_0/W_0')$. then it suffices to check the condition for W_0'. □

17.8 Adic Spaces and Perfectoid Spaces(Scholze)

References are [Hub93], [Hub96], [Mor19], [Bha17], [Wed14], [S-W20], [Sch12].

Notation (17.8.0.1).
- Use notations as in Topological Commutative Algebra.

⌟

1 (Continuous)Valuation Spectrums

Main references are [Mor19]. Notice this should be prior to the definition of adic spaces.

Def. (17.8.1.1) [Riemann-Zariski Space]. Let $K \in \mathtt{Field}$ and $A \subset K \in \mathcal{CR}\mathrm{ing}$, the Riemann-Zariski space $RZ(K,A)$ is defined to be the space of all valuation subrings of K containing A with the topology generated by

$$U(x_1,\ldots,x_n) = \{P \in RZ(K,A) | x_1,\ldots,x_n \in P\}.$$

$RZ(K,0)$ is also denoted by $RZ(K)$. $RZ(K,A)$ is just isomorphic to $\mathrm{Spa}(K,A^{itc})$, so it is spectral by(17.8.2.23). ⌟

Cor. (17.8.1.2). Clearly the specialization relations of $RZ(K,A)$ is identical to inclusion relations. ⌟

Def. (17.8.1.3) [Valuation Spectrum]. For $A \in \mathcal{CR}\mathrm{ing}$, the **valuation spectrum** $\mathrm{Spv}(A) \in \mathcal{T}\mathrm{op}$ is the set of equivalent classes of valuations on A, topologized by the open subsets

$$\mathrm{Spv}(A)(\frac{f}{g}) = \{x \in \mathrm{Spa}(A) | |f(x)| \le |g(x)| \ne 0\}.$$

$\mathrm{Spv}(A)$ is spectral, with sub-basis generated by $\mathrm{Spv}(\frac{f}{g})$

There is a kernel map $\ker : \mathrm{Spv}(A) \to \mathrm{Spec}\, A$ sending a valuation to its kernel(support). Then this map is continuous, and the fiber of this map over $\mathfrak{p}$ is just isomorphic to the Riemann-Zariski space $RZ(k(\mathfrak{p}))$.

Moreover, the map $\ker : \mathrm{Spv}(A) \to \mathrm{Spec}\, A$ is spectral, as the kernel of $D(f)$ is $U(\frac{f}{f})$. ⌟

Specialization Relations in $\mathrm{Spv}(A)$

Def. (17.8.1.4) [Vertical Specializations]. Let $x, y \in \mathrm{Spv}(A)$. We say that x is a vertical specialization of y if x is a specialization of y and $\mathfrak{p}_x = \mathfrak{p}_y$. ⌟

Valuations with Support Conditions

Def. (17.8.1.5) [$\mathrm{Spv}(A,J)$]. We define a space $\mathrm{Spv}(A,J) \subset \mathrm{Spv}(A)$ by

$$\mathrm{Spv}(A,J) = \{x \in \mathrm{Spv}(A) | r(x) = x\} = \{x \in \mathrm{Spv}(A) | c\Gamma_x(J) = \Gamma\}.$$

with the subset topology from $\mathrm{Spv}(A)$. ⌟

Prop. (17.8.1.6).
- $\mathrm{Spv}(A,J)$ is a spectral space.

- A basis of quasi-compact open subsets for the topology is given by the sets $U(\frac{f_1,\ldots,f_n}{g})$ where $J \subset \sqrt{(f_1,\ldots,f_n)}$.
- The retraction $r : \mathrm{Spv}(A) \to \mathrm{Spv}(A, J)$ is a spectral map.

⌟

Proof: Cf.[Mor19]P52. □

Continuous Valuation Spectrum

Def. (17.8.1.7) [Continuous Valuations]. For $A \in \mathcal{H}ub\,\mathcal{R}ing$, define $\mathrm{Cont}(A) \in \mathcal{T}op$ as the subspace of $\mathrm{Spv}(A)$(17.8.1.3) consisting of continuous valuations on A. Then

$$\mathrm{Cont}(A) = \{x \in \mathrm{Spv}(A, A^{00}A) | x(A^{00}) < 1\}$$

⌟

Proof: Cf.[Mor19]P64. □

Cor. (17.8.1.8) [Cont(A) is Spectral]. For any Huber ring A, $\mathrm{Cont}(A)$ is a spectral space, with a basis of quasi-compact open subsets given by $U(\frac{f_1,\ldots,f_n}{g})$, where $A^{00} \subset \sqrt{(f_1,\ldots,f_n)}$, or equivalently $(f_1,\ldots,f_n)$ is open**??**. ⌟

Proof: This is because

$$\mathrm{Cont}(A) = \mathrm{Spv}(A, A^{00}A) - \bigcup_{g\in A^{00}} U(\frac{1}{g}),$$

which is an open subset of $\mathrm{Spv}(A, A^{00}A)$, thus the assertion follows from(17.8.1.6) and(4.12.4.7). □

2 Adic Spectra

Def. (17.8.2.1)[Adic Spectra]. For any $(A, A^+) \in \mathcal{H}ub\mathrm{Pair}$(11.2.5.13), the **adic spectrum** of (A, A^+) is defined to be

$$\mathrm{Spa}(A, A^+) = \{x \in \mathrm{Cont}(A) | x(A^+) \le 1\}.$$

And for $A \in \mathcal{H}ub\,\mathcal{R}ing$, denote $\mathrm{Spa}\,A = \mathrm{Spa}(A, A^0)$, where A^0 is the ring of power-bounded elements(11.2.5.8).

The shape of these open sets is dictated by the desired properties that both $\{x|f(x) \ne 0\}$ and $\{x|f(x) \le 1\}$ be open. These desiderata combine features of classical algebraic geometry and rigid geometry, respectively.

This adic spectrum construction(17.8.2.1) defines a functor

$$\mathrm{Spa} : \mathcal{H}ub\mathrm{Pair}^{\mathrm{op}} \to \mathcal{T}op\,.$$

And for any ring of integers A^+ of A, $\mathrm{Spa}\,A = \mathrm{Spa}(A, A^0) \hookrightarrow \mathrm{Spa}(A, A^+)$ is an immersion of spaces, by(11.2.5.13). ⌟

Def. (17.8.2.2) [Kernel map]. Taking kernels of valuations gives a map $\ker : \mathrm{Spa}(A, A^+) \to \mathrm{Spec}\,A$. This map is continuous, as the inverse image of $D(f)$ is $\mathrm{Spa}(A, A^+)(\frac{f}{f})$. We call a subset a **Zariski open subset** of $\mathrm{Spa}(A, A^+)$ iff it is open in the initial topology along ker. ⌟

Def. (17.8.2.3) [Rational Subsets]. A **rational subset** of $\mathrm{Spa}(A, A^+)$ is defined to be

$$\mathrm{Spa}(A, A^+)(\frac{f_1, \ldots, f_n}{g}) = \{x \in \mathrm{Spa}(A, A^+) | x(f_i) \le x(g)\},$$

where (f_i) is an open ideal. ⌟

Prop. (17.8.2.4) [Adic Spectrums are Spectral]. The adic spectrum $\mathrm{Spa}(A, A^+)$ is spectral, and a basis of quasi-compact open subsets are given by rational subsets. And the Spa functor is naturally a functor from the category of Huber rings to the category of spectral spaces. ⌟

Proof: Firstly $\mathrm{Spa}(A, A^+)$ is closed in the constructible topology of $\mathrm{Cont}(A)$: for any $a \in A$,

$$\{x \in \mathrm{Cont}(A) | |a|_x \le 1\} = U(\frac{1, a}{1})$$

is a quasi-compact open subset of $\mathrm{Cont}(A)$, so constructible, thus $\mathrm{Spa}(A, A^+) = \cap_{a \in A^+}\{x \in \mathrm{Cont}(A) | |a|_x \le 1\}$ is closed in the constructible topology.

So the assertions follow from(4.12.4.7) and(17.8.1.8). □

Remark (17.8.2.5). In spite of the proposition that adic spaces are spectral, it is very different from classical algebraic geometry. For example, the generalizations of a point y is totally ordered(localization of the valuation ring), but this nearly never happen for an affine variety. ⌟

Remark (17.8.2.6). The rational subsets forms a basis for the topology of $\mathrm{Spa}(A, A^+)$. But in general $\mathrm{Spa}(\frac{f}{g})$ is not quasi-compact, in particular, $\ker : \mathrm{Spa}(A, A^+) \to \mathrm{Spec}\, A$ is not quasi-compact. ⌟

Def. (17.8.2.7) [Specialization Map]. The **specialization map**

$$\mathrm{Sp} : \mathrm{Spa}(A, A^+) \to \mathrm{Spec}(A^+/A^{00})$$

that maps a point x to the inverse image of the maximal ideal of R_x along the valuation map $A^+ \to R_x$ it corresponds. It clearly lies in $\mathrm{Spec}(A^+/A^{00})$ as any pseudo-uniformizer is mapped to a pseudo-uniformizer in R_x thus in the maximal ideal.

This map is continuous and spectral, unlike that the kernel map(17.8.2.22): the inverse image of a $D(f)$ for $f \in A^+$ is the set of points $x \in \mathrm{Spa}(A, A^+)$ that $x(f)$ is a unit, i.e. $|x(f)| = 1$. As $|x(f)| \le 1$ for all $f \in A^+$, this set is just $\mathrm{Spa}(A, A^+)(\frac{1}{f})$, so specialization map sp is both continuous and spectral. ⌟

Completed Residue Fields

Def. (17.8.2.8) [Completed Residue Fields]. Let $x \in \mathrm{Spa}(A, A^+)$, then we denote by $k(x)$ the fraction field of $A/\mathfrak{p}_x$, with a valuation ring $k^+(x)$. If x is not analytic, we set $\kappa(x) = k(x), \kappa^+(x) = k^+(x)$. If x is analytic, we set $\kappa(x) = k(x)^\wedge, \kappa^+(x) = k^+(x)^\wedge$. $(\kappa(x), \kappa(x)^+)$ is called the **completed residue field** of x. ⌟

Prop. (17.8.2.9) [Vertical Generalizations]. The morphism

$$\mathrm{Spa}(\kappa(x), \kappa(x)^+) \to \mathrm{Spa}(A, A^+)$$

induces a homeomorphism onto the set of vertical generalizations of x.

x is analytic iff $\kappa(x)$ is microbial. ⌟

Proof: For the first assertion, if x is not analytic, then $\mathrm{Spa}(k(x), k(x)^+) \cong RZ(k(x), k(x)^+)$ is homeomorphic to the vertical generalizations of x.

If x is analytic, then by(17.8.2.16), $\mathrm{Spa}(\kappa(x), \kappa(x)^+) \to \mathrm{Spa}(k(x), k(x)^+)$ is a homeomorphism. And now we need to check more that if $R \in RZ(k(x), k(x)^+)$ corresponds to a vertical generalization y, then $|\cdot|_R$ is continuous iff $|\cdot|_y$ is continuous. For this, see[Mor19]107.

The second assertion follows from(11.2.6.7). □

Prop. (17.8.2.10) [Residue of Rational Subsets]. Let $f : (A, A^+) \to (A\langle \frac{T}{s} \rangle, A\langle \frac{T}{s} \rangle^+)$ be a rational subset, and $y \in \mathrm{Spa}(A\langle \frac{T}{s} \rangle, A\langle \frac{T}{s} \rangle^+)$ with $x = \mathrm{Spa}(f)(y)$, then the canonical map $(k(x), k(x)^+) \to (k(y), k(y)^+)$ induces an isomorphism of Huber pairs $(\kappa(x), \kappa(x)^+) \cong (\kappa(y), \kappa(y)^+)$ after completion. ⌟

Proof: Cf.Morel P108.**?** □

Def. (17.8.2.11) [Adic Points]. An **adic point** is $\mathrm{Spa}(K, K^+)$ where
- $(K, K^+) \in \mathcal{H}\mathrm{ubPair}$,
- $K \in \texttt{Field}$, and K is either complete non-Archimedean or discrete,
- K^+ is an open and bounded valuation subring(hence integrally closed).

An **analytic adic point** is an adic point s.t. K is complete non-Archimedean. ⌟

Remark (17.8.2.12). The adic point is not a point in general. In fact, if K is non-Archimedean, $\mathrm{Spa}(K, K^+)$ is totally ordered by inclusion**?**, with a unique closed point corresponding to K^+ and a unique generic point corresponding to $\mathcal{O}_K$. ⌟

Prop. (17.8.2.13) [Valuation Ring Characterization of Spa]. For a Huber pair (A, A^+), there is a natural bijection between $\mathrm{Spa}(A, A^+)$ and the set of maps $\varphi : (A, A^+) \to (K, K^+)$ that $\mathrm{Spa}(K, K^+)$ is an adic point where $K_x = \kappa(x)$ and x corresponds to the image of the closed point of $\mathrm{Spa}(K, K^+)$ under the map $\mathrm{Spa}(\varphi)$. And x is analytic iff the corresponding adic point $\mathrm{Spa}(K, K^+)$ is analytic. ⌟

Proof: Let $\varphi : (A, A^+) \to (K, K^+)$ be a map of Huber pairs, then correspond the maps gives a continuous valuation on A which is in $\mathrm{Spa}(A, A^+)$ and $\mathfrak{p}_x = \ker(\varphi)$. Notice x is the image of the closed point of $\mathrm{Spa}(K, K^+)$. And we get a map $k(x) \to K$ such that $k(x)^+ = k(x) \cap K^+$, and that has dense image by assumption, so after completion(when non-Archimedean) induces an isomorphism $(\kappa(x), \kappa(x)^+) \cong (K, K^+)$. Thus this is a bijection of sets. □

Prop. (17.8.2.14) [Uniformity]. If A is uniform, then the map

$$A \to \prod_{x \in \mathrm{Spa}(A, A^+)} \kappa(x)$$

is a homeomorphism of A onto its image, where $\kappa(x)$ is the completed residue field(17.8.2.8). ⌟

Proof: Berkovich, Étale cohomology for non-Archimedean analytic spaces.**?** □

Cor. (17.8.2.15). Let $\widetilde{\mathcal{O}}_X$ be the sheafification of $\mathcal{O}_X$, then if A is uniform, $A \to H^0(X, \widetilde{\mathcal{O}}_X)$ is injective. ⌟

Proof: In fact, $A \to H^0(X, \widetilde{\mathcal{O}}_X) \to \prod_x \kappa(x)$ is injective. □

Properties of Adic Spectrums

Prop. (17.8.2.16) [Properties of Adic Spectrums].

- The completion map $(A, A^+) \to (\widehat{A}, \widehat{A}^+)$ induces an homeomorphism on the adic spectrums that preserves rational subsets.
- $\mathrm{Spa}(A, A^+)$ vanishes iff its completion $\widehat{A}$ vanishes.
- (Adic Nullstellensatz)$A^+ = \{f \in A | x(f) \leq 1, \forall x \in \mathrm{Spa}(A, A^+)\}$.
- If A is complete, then $f \in A$ is a unit iff $|f|_x \neq 0$ for all $x \in \mathrm{Spa}(A, A^+)$.
- If A is Tate, then f is topologically nilpotent iff $|f|_x^n \to 0$ for any $x \in \mathrm{Spa}(A, A^+)$.

⌟

Proof: 1: Use the valuation ring characterization(17.8.2.13), a point of x determined a continuous map $(A, A^+) \to (K, K^+)$. Now this extends to a map under completion, thus determines a point of $\mathrm{Spa}(\widehat{A}, \widehat{A}^+)$, so the Spa map is surjective. And injectivity follows from the fact A is dense in $\widehat{A}$.

For the homeomorphism, just notice that if $f_i - f_i', g - g' \in t^{N+1}\widehat{A}$, then

$$\mathrm{Spa}(\frac{f_1, \ldots, f_n}{g}) = \mathrm{Spa}(\frac{f_1', \ldots, f_n'}{g'}).$$

where $f_n = t^N$. So now A is dense in $\widehat{A}$, if we choose $f_i, g \in A$, then this rational subset is clearly induced from A.

2: Cf.[Mor19]P104.

3: Cf.[Mor19]P91.

4: Cf.[Mor19]P106.

5: Cf.[Mor19]P106. □

Cor. (17.8.2.17) [Generalizations in Adic Spectrum]. The above proposition shows that the generalization relations of Spa are easily determined, for an element y, all generalizations of y are in bijection with $\mathrm{Spec}(R_y/(t))$ as a poset, thus totally ordered, and each y has a unique generic point as generalization, because it is microbial.

Moreover, $\mathrm{Spa}(A, A^0)$ is closed under generalization in $\mathrm{Spa}(A, A^+)$, and they have the same set of generic points. ⌟

Proof: The last assertion is because the generalizations of a point y is just valuation rings containing R_y, and R_y contains $A^0/\mathfrak{p}_y$, so does its generalizations. And for any generic point $x \in \mathrm{Spa}(A, A^+)$, A^0 is mapped to the valuation ring R_x, because it is a rank 1 valuation, so if $t^k f^{\mathbb{N}} \subset R_x$, then $f \in R_x$ because otherwise we have $|t| < |f^{-n}|$ for n large. □

Def. (17.8.2.18) [Specialization Map]. The **specialization map**

$$\mathrm{Sp} : \mathrm{Spa}(A, A^+) \to \mathrm{Spec}(A^+/A^{00})$$

that maps a point x to the inverse image of the maximal ideal of R_x along the valuation map $A^+ \to R_x$ it corresponds. It clearly lies in $\mathrm{Spec}(A^+/A^{00})$ as any pseudo-uniformizer is mapped to a pseudo-uniformizer in R_x thus in the maximal ideal.

This map is continuous and spectral, unlike that the kernel map(17.8.2.22): the inverse image of a $D(f)$ for $f \in A^+$ is the set of points $x \in \mathrm{Spa}(A, A^+)$ that $x(f)$ is a unit, i.e. $|x(f)| = 1$. As $|x(f)| \leq 1$ for all $f \in A^+$, this set is just $\mathrm{Spa}(A, A^+)(\frac{1}{f})$, so specialization map sp is both continuous and spectral. ⌟

Prop. (17.8.2.19) [Maximal Hausdorff Quoteint]. Let $X = \mathrm{Spa}(A, A^+)$ be an affinoid Tate space, the if $\overline{X}$ is the quotient of X by the equivalence relation generated by specialization, then $\overline{X}$ is the Hausdorffization of X, i.e. $\overline{X}$ is Hausdorff. ⌟

Proof: To show $\overline{X}$ is Hausdorff, if $x, y \in X$ is not mapped to the same point in $\overline{X}$, then by(17.8.2.17), we may assume x, y is generic in X, and $\overline{\{x\}} \cap \overline{\{y\}} = \varnothing$. Now we must find two disjoint open subsets of x, y that is stable under specialization. Cf.[Bhatt Perfectoid Spaces P75]. □

Spectrality of Adic Spectrums

Def. (17.8.2.20) [Rational Subsets]. A **rational subset** of $\mathrm{Spa}(A, A^+)$ is defined to be

$$\mathrm{Spa}(A, A^+)(\frac{f_1, \ldots, f_n}{g}) = \{x \in \mathrm{Spa}(A, A^+) | x(f_i) \leq x(g)\},$$

where $(f_i) = (1)$. ⌟

Prop. (17.8.2.21). Rational subsets are stable under intersection(Easy). ⌟

Prop. (17.8.2.22). The rational subsets forms a subbasis for the topology of $\mathrm{Spa}(A, A^+)$.**?** But in generally $\mathrm{Spa}(\frac{f}{g})$ is not quasi-compact, in particular, $\mathrm{Spv}(A) \to \mathrm{Spa}(A, A^+)$ is not quasi-compact(proper). ⌟

Prop. (17.8.2.23) [Adic Spectrums are Spectral]. The adic spectrum $\mathrm{Spa}(A, A^+)$ is spectral, and a basis of quasi-compact open subsets are given by rational subsets. And the Spa functor is naturally a functor from the category of Huber rings to the category of spectral spaces. ⌟

Proof: Firstly $\mathrm{Spa}(A, A^+)$ is closed in the constructible topology of $\mathrm{Cont}(A)$: for any $a \in A$,

$$\{x \in \mathrm{Cont}(A) || a|_x \leq 1\} = U(\frac{1, a}{1})$$

is a quasi-compact open subset of $\mathrm{Cont}(A)$, so constructible, thus

$$\mathrm{Spa}(A, A^+) = \cap_{a \in A^+} \{x \in \mathrm{Cont}(A) || a|_x \leq 1\}$$

is closed in the constructible topology.

So the assertions follow from(4.12.4.7) and(17.8.1.8). □

Remark (17.8.2.24). In spite of the proposition that adic spaces are spectral, it is very different from classical algebraic geometry. For example, the generalizations of a point y is totally ordered(localization of the valuation ring), but this nearly never happen for an affine variety. ⌟

Cor. (17.8.2.25) [Detecting Nilpotence Locally]. If (A, A^+) is an affinoid Tate ring and $f \in A$, then $f \in A^{00}$ iff $|f(x)|^n \to 0$ for all x. ⌟

Proof: If f is topological nilpotent, then $f^N \in tA^+$ for some n, so $|f(x)|^{nN} \leq |t(x)|^n \to 0$ because x is continuous. Conversely, if $|f(x)|^n \to 0$ for all x, then $X = \cup_n X(\frac{f^n}{t})$. But X is quasi-compact, so $|f(x)|^n \leq |t(x)|$ for all x, for some n. So by(17.8.2.16) $f^n \in tA^+$. Now A^+ is a filtered colimits of rings of definitions(11.2.5.14), so $f^n \in tA_0$ for some tA_0, which shows that $f \in A^{00}$. □

Constructions of Adic Spectrums

Prop. (17.8.2.26) [Direct Limits of Uniform Affinoids]. The direct limits exists in the category of uniform affinoid Tate rings. and $A^+ = \operatorname{colim} A_i^+$.

Moreover,

$$|\operatorname{Spa}(A, A^+)| \cong \varprojlim_i |\operatorname{Spa}(A_i, A_i^+)|$$

as a homeomorphism of spectral spaces, and each rational subset of $\operatorname{Spa}(A, A^+)$ is pulled back from some rational subset of $\operatorname{Spa}(A_i, A_i^+)$.

The same conclusion also hold in the category of complete uniform affinoid Tate rings(For the homeomorphism, (17.8.2.16) is used). ⌟

Proof: Suppose the colimit index has a minimal element i_0, let t be a pseudo-uniformizer, then each A_i^+ is a ring of definition with pseudo-uniformizer t. Now we set $A = \operatorname{colim} A_i$ with ring of definitions $A^+ = \operatorname{colim} A_i^+$, then A^+ is integrally closed in A, thus (A, A^+) is truly a uniform affinoid Tate ring. Now we check it is the colimit: For any compatible map $(A_i, A_i^+) \to (B, B^+)$, there is a map $f : (A, A^+) \to (B, B^+)$ as abstract rings. We check it is continuous: we may assume B^+ is the ring of definition, then $t^n A^+ \subset f^{-1}(t^n B^+)$, thus it is continuous.

For the adic spectrum, now a point $x \in \operatorname{Spa}(A, A^+)$ is determined by the map of uniform affinoid Tate rings $(A, A^+) \to (k(\mathfrak{p}), R_x)$, and by the universal property, it is defined by a compatible set of maps $(A_i, A_i^+) \to (k(\mathfrak{p}), R_x)$. Now it is easy to see the desired bijection of topological spaces, as the elements defining rational subsets are pullbacks from some A_i. □

Prop. (17.8.2.27) [Perfection of Adic Spectrum]. Let (A, A^+) be an affinoid Tate ring of char$p$, then

- The Frobenius map induces a homeomorphism on the adic spectrum of (A, A^+).
- If (A, A^+) is uniform, then there is a perfection functor, which is left adjoint to the forgetful functor from the category of perfect uniform affinoid Tate rings to the category of affinoid Tate rings. And it is just $(A_{\text{perf}}, A_{\text{perf}}^+)$.
- The natural map $(A, A^+) \to (A_{\text{perf}}, A_{\text{perf}}^+)$ induces a homeomorphism on the adic spectrum.

⌟

Proof: 1: The Frobenius pulls a valuation a multiple of itself, thus equals itself.

2: Clearly A_{perf}^+ is integrally closed in A^+ and is in A_{perf}^0. It suffices to show $(A_{\text{perf}}, A_{\text{perf}}^+)$ is uniform, but this is because $A_{\text{perf}}^0 = (A_{\text{perf}})^0 \subset (t^{-n} A_0)_{\text{perf}} = t^{-n} (A_0)_{\text{perf}}$.

3: The Spa map is checked to be continuous and injective, for the converse, using the microbial valuation ring characterization, a point x of $\operatorname{Spa}(A, A^+)$ corresponds to a map A^+ to a complete field $k^+(x)$, thus a map $A_{\text{perf}}^+ \to k^+(x)_{\text{perf}}$, now $k^+(x) \to k^+(x)_{\text{perf}}$ is faithfully flat that preserves pseudo-uniformizers, thus it is a point y that maps to y. □

3 Structure Presheaf and Adic Spaces

Lemma (17.8.3.1) [Functions on Rational Subsets]. If $X = \operatorname{Spa}(A, A^+)$ is an affinoid adic space, and U is a rational subset, then there is a unique complete affinoid Tate ring $(\mathcal{O}_X(U), \mathcal{O}_X^+(U))$ over (A, A^+) s.t. the the map of spectra

$$\operatorname{Spa}(\mathcal{O}_X(U), \mathcal{O}_X^+(U)) \to \operatorname{Spa}(A, A^+)$$

is universal w.r.t. all the complete affinoid Tate space with a map to X that has image in U.

And in this case, this Spa map is a homeomorphism identifying the rational subsets contained in U to rational subsets of $\mathrm{Spa}(\mathcal{O}_X(U),\mathcal{O}_X^+(U))$. In particular, U is quasi-compact. ⌟

Proof: **?** See Hub94 P1.3 for the proof in the Huber ring case.

Choose a ring of definition (A_0,t), and $U=\mathrm{Spa}(A,A^+)(\frac{f_1,\ldots,f_n}{g})$ for $f_i,g\in A_0$, and $f_n=t$**??**, and let $B=A[g^{-1}]$ and $B_0=A_0[\frac{f_i}{g}]$. Then $B=B_0[t^{-1}]$(notice that $A_0[t^{-1}]=A$). So B is a Tate A-algebra with ring of definition (B_0,t). Now if B^+ is the integral closure of the subring of B generated by $A^+[\frac{f_i}{g}]$, then (B,B^+) is an affinoid Tate ring. Set $(\mathcal{O}_X(U),\mathcal{O}_X^+(U))$ to be its completion.

By construction $\mathrm{Spa}(\mathcal{O}_X(U),\mathcal{O}_X^+(U))$ maps into U, because $x(g)\neq 0$ because g is a unit, and $|x(f_i)|\leq |x(g)|$ as $f_i/g\in B^+$.

Now check universal property: if $\mathrm{Spa}(C,C^+)$ maps into U, then g is a unit in C by(17.8.2.16), and then $f_i/g\in C^+$ by(17.8.2.16) again. Now C^0 is the filtered colimit of all rings of definition, so there is a ring of definition C_0 that contains A_0 and all f_i/g((11.2.5.17) is used). Then this gives a map of affinoid Tate rings that maps B_0 into C_0, and when passed to completion, induces a map $\mathcal{O}_X(U)\to C$ of Tate algebras. Now also B^+ is mapped into C^+ because C^+ is integrally closed, so we are done.

For the last assertion, by(17.8.2.16), we only have to prove $\mathrm{Spa}(B,B^+)\to U$ is a homeomorphism preserving rational subsets, for this, the injectivity is clear as B is a localization of A. And the surjectivity follows immediately from the valuation ring characterization and universal property. Continuity is also clear.

For the openness, for any rational subset $X(\frac{f_1,\ldots,f}{g})$ of $X=\mathrm{Spa}(B,B^+)$, because $B=A[g^{-1}]$, g is unit in B, we can assume that $f_i,g\in A_0$. Now we show $U\cap\mathrm{Spa}(A,A^+)(\frac{f_1,\ldots,f}{g})$ is rational, for this, it suffices to add a t^N to f_i, and this is possible, as $X(\frac{f_1,\ldots,f}{g})$ is quasi-compact by(17.8.2.23). (This is in fact similar to the proof that continuous bijection from compact to Hausdorff is homeomorphism). □

Remark (17.8.3.2). The proof goes through with complete replaced by Zariski or Henselian, because we only use item5 of(17.8.2.16), which is true for all Zariski pairs.

And by looking at the construction, if a rational subset U has a representation $X(\frac{f_1,\ldots,f_n}{g})$, then $f_i\in\mathcal{O}_X^+(U)$, and g is invertible in $\mathcal{O}_X(U)$. ⌟

Stalks

Def. (17.8.3.3) [Stalks]. The **stalks of an affinoid adic space** is defined as in the case of schemes, i.e. the colimit of the function ring of rational subsets containing x, without topology, and similarly for the **integral stalk**. notice that the function rings are defined by universal property w.r.t to complete Huber pairs, so the stalks only depend on the completion of (A,A^+). ⌟

Lemma (17.8.3.4). Let U be an open subset of $X=\mathrm{Spa}(A,A^+)$ and $f,g\in\mathcal{O}_X(U)$, then $V=\{x\in U||f|_x\leq |g|_x\neq 0\}$ is an open subset of X. ⌟

Proof: Cf. Morel P116.**?** □

Prop. (17.8.3.5) [Valuations on the Stalks]. Let $X=\mathrm{Spa}(A,A^+)$ be an affinoid adic space, and $x\in X$, then:

- There is a valuation x on $\mathcal{O}_{X,x}$ extending that on A, and $\mathcal{O}_{X,x}^+=\{f\in\mathcal{O}_{X,x}||f(x)|\leq 1\}$.

- $\mathcal{O}_{X,x}$ is local with maximal ideal $\mathfrak{m}_x = \ker x$, and $\mathcal{O}^+_{X,x}$ is local with maximal ideal $\{f \in \mathcal{O}_{X,x} | |f(x)| < 1\}$.
- If $\kappa(x)$ is the residue field of $\mathcal{O}_{X,x}$ and $\kappa(x)^+$ be the image of $\mathcal{O}^+_{X,x}$ in $\kappa(x)$, then $k^+(x)$ is naturally a valuation ring, and $(\kappa(x), \kappa^+(x))$ is an affinoid field over (A, A^+). In particular, there is an isomorphism between the residue fields of $\mathcal{O}^+_{X,x}$ and $k^+(x)$.
- If $\varphi : (A, A^+) \to (B, B^+)$ is a morphism of Huber pairs and $y \in \mathrm{Spa}(B, B^+)$ is a point that $\mathrm{Spa}(\varphi)(y) = x$, then the morphism of rings $\mathrm{Spa}(\varphi)^\flat_x : \mathcal{O}_{X,x} \to \mathcal{O}_{Y,y}$ induced by $\mathrm{Spa}(\varphi)$ is such that $|\cdot|_x \circ \mathrm{Spa}(\varphi)^\flat_x = |\cdot|_y$. In particular, $\mathrm{Spa}(\varphi)^\flat_x$ is a morphism of local rings. Also it sends $\mathcal{O}^+_{X,x}$ to $\mathcal{O}^+_{Y,y}$ and this is a morphism of local rings.

If moreover A is Tate, then we have:
- The ring $\mathcal{O}^+_{X,x}$ is t-adically Henselian, and $\mathcal{O}^+_{X,x} \to k^+(x)$ induces an isomorphism after t-adic completion.
- The pairs $(\mathcal{O}^+_{X,x}, \mathfrak{m}_x)$ and $(\mathcal{O}_{X,x}, \mathfrak{m}_x)$ are Henselian.

⌟

Proof: **?** Morel P115.

1: Consider the t-adic completion of the valuation ring R_x corresponding to x, then $(\widehat{k}(\mathfrak{p}_x), \widehat{R}_x)$ is an affinoid Tate ring over (A, A^+) that is mapped to x(and its generalizations), thus by universal property, there are unique maps from every rational subsets containing x to $(\widehat{k}_x, \widehat{R}_x)$, thus inducing a map $(\mathcal{O}_{X,x}, \mathcal{O}^+_{X,x}) \to (\widehat{k}_x, \widehat{R}_x)$, which induces the desired valuation. And also we have $\mathcal{O}^+_{X,x} \subset \{f \in \mathcal{O}_{X,x} | |f(x)| \le 1\}$, for the converse, if $|f(x)| \le 1$, then $U(\frac{f,1}{1})$ is rational subsets in U containing x, so by(17.8.3.2), $f \in \mathcal{O}_X(V)^+$, thus $f \in \mathcal{O}^+_{X,x}$.

2: for g not in $\mathfrak{m}_x$, $|g(x)| > |t(x)|^n$ for some n, so g is invertible in $U(\frac{t^n}{g})$ by(17.8.3.2), hence invertible in $\mathcal{O}_{X,x}$. Similarly for $\mathcal{O}^+_{X,x}$, as g is invertible in $U(\frac{1}{g})$.

3: This is clear from the construction of the valuation on $\mathcal{O}_{X,x}$ in item1.

4:

5: As filtered colimits of Henselian pair is Henselian(5.3.10.3) and the function ring is complete, the stalk is Henselian. As for the completion, notice $\mathfrak{m}_x \subset \mathcal{O}^+_{X,x}$ and is t-divisible, thus $\mathcal{O}^+_{X,x}$ has the same t-adic completion as $k^+(x)$.

6: We first prove $(\mathcal{O}^+_{X,x}, t)$ is Henselian, for this, it suffices to prove $(\mathcal{O}^+_X(U), t)$ is Henselian, by(5.3.10.3). And $\mathcal{O}^+_X(U)$ is a filtered colimits of rings of definitions(11.2.5.14) and they are t-adically complete hence Henselian, so we are done by(5.3.10.3) again. Then so does $(\mathcal{O}_{X,x}, \mathfrak{m}_x)$ because the property of being Henselian only depends on I(5.3.10.10). □

Cor. (17.8.3.6). By the construction of the valuation on the stalk, we have an inclusion of rings $k(\mathfrak{p}_x) \subset k(x) \subset \widehat{k}(x)$ that has the same completions, where the first is induced by the compatible map $A \to \mathcal{O}_X(X) \to \mathcal{O}_X(U)$. ⌟

Def. (17.8.3.7) [Huber's Presheaf]. Now by the universal property of function rings(17.8.3.1), we have a map between them induced by inclusion of rational subsets, so we can define the **structure presheaf** to be

$$\mathcal{O}_X(W) = \lim_{U \subset W \text{ rational}} \mathcal{O}_X(U),$$

and similarly for the **integral structure sheaf** $\mathcal{O}^+_X$.

Then there is a valuation of a point on $\mathcal{O}_X(W)$ by passing to the stalk, and

$$\mathcal{O}^+_X(W) = \{f \in \mathcal{O}_X(W) | |f(x)| \le 1, \forall x \in W\}.$$

because this is true for all rational subsets by adic nullstellensatz(17.8.2.16).

A Huber ring (A, A^+) is called **sheafy** iff the structure sheaf $\mathcal{O}_X$ on $X = \mathrm{Spa}(A, A^+)$ is a sheaf. In this case, $\mathcal{O}_X^+$ is also a sheaf by the above formula, so sheafyness is a property that only depends on A. ⌟

Criteria for Sheafyness

Def. (17.8.3.8) [Stably Uniform Huber Pair]. For $(A, A^+) \in \mathcal{H}\mathrm{ubPair}$ s.t. A is analytic and $X = \mathrm{Spa}(A, A^+)$, it is called **stably uniform** if $\mathcal{O}_X(U)$ is uniform for all rational subsets $U \subset X = \mathrm{Spa}(A, A^+)$. ⌟

Prop. (17.8.3.9). Let $A \to B$ be a continuous map of Huber rings which splits in the category of topological A-modules, then A is stably uniform. ⌟

Proof: The splitting means the map is strict(11.2.1.4), so A is also uniform. Also the splitting is preserved under completed tensor product with rational localization, so A is stably uniform. □

Prop. (17.8.3.10) [Examples of Sheafy Huber Rings]. Let (A, A^+) be a complete Huber pair,

1. (Schemes)If A is discrete, then A is sheafy.
2. (Formal Schemes)If A has a Noetherian ring of definition, then A is sheafy.
3. (Rigid Spaces, Fargues-Fontaine Curves)If A is Tate and strongly Noetherian(11.2.4.25), then A is sheafy.
4. (Perfectoid Spaces)If A is analytic and (A, A^+) is stably uniform(17.8.3.8), then A is sheafy and acyclic.

⌟

Proof: Cf. Hub94 T2.2, [Ked19]1.7.

We use the arguments following(17.8.4.30).

If A is analytic and (A, A^+) is stably uniform. Firstly the ideals $(f - gT), (g - fT)$ are closed in their rings, Cf.[Ked19]L1.5.26.

Then we have a diagram

$$\begin{array}{ccccccccc}
0 & \to & 0 & \to & B\langle T\rangle \oplus B\langle T^{-1}\rangle & \xrightarrow{(x,y)\mapsto x+T^{-1}y} & B\langle T,T^{-1}\rangle & \to & 0\\
 & & \downarrow & & \downarrow{\scriptstyle (f-gT,\,g-fT^{-1})} & & \downarrow{\scriptstyle \times(f-gT)} & & \\
0 & \to & B & \to & B\langle T\rangle\oplus B\langle T^{-1}\rangle & \xrightarrow{(x,y)\mapsto x-y} & B\langle T,T^{-1}\rangle & \to & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & B & \to & B\langle \frac{f}{g}\rangle \oplus B\langle\frac{g}{f}\rangle & \to & B\langle \frac{f}{g},\frac{g}{f}\rangle & \to & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where the columns and the first two rows are exact, thus the third row are exact in the middle and right by spectral sequence. Also it is exact at the left by(17.8.2.15). □

Remark (17.8.3.11). Notice that these contains nearly everything of interest, so Scholze comments that we can somehow pretend that non-sheafy Huber rings don't appear in nature. ⌟

Remark (17.8.3.12). Stably uniform is hard to check in practice, so a recent paper of Hansen-Kedlaya [Sheafyness Criterion for Huber Rings] studied another class of sousperfectoid rings which can be splitly embedded into a perfectoid ring, and another class of diamaintine rings, which involves a condition on the cohomology of pro-étale site of A, closely related to properties of diamonds. ⌟

Prop. (17.8.3.13) [Non-examples of Sheafy Huber Rings]. Cf. Hub94 end of section1.? ⌟

4 Adic Spaces

Def. (17.8.4.1) [Huber category]. The category $\mathcal{V}^{pre}$ is a category that the objects are triples $(X, \mathcal{O}_X, v_x)$ that X is a topological space, $\mathcal{O}_X$ is a , and $\mathcal{O}_X$ has the structure of sheaf of complete topological rings, and v_x are continuous valuations on the stalk $\mathcal{O}_{X,x}$ with support $\mathfrak{m}_x$.

And a morphism in V^{pre} is a pair $(f, f^\flat)$ where $f : X \to Y$ is a map of topological spaces and $f^\flat : \mathcal{O}_X \to f_*\mathcal{O}_Y$ is a morphism of presheaves of topological rings, and the induced morphism of $f^\flat$ on the stalks are compatible with the valuations.

The **Huber category** V is the full subcategory of V^{pre} whose objects are triples $(X, \mathcal{O}_X, v_x)$ in V^{pre} that $\mathcal{O}_X$ is a sheaf. ⌟

Def. (17.8.4.2)[Open Immersions]. An **open immersion** in V^{pre} is a homeomorphism onto an open subset that induces an isomorphism of presheaves. ⌟

Def. (17.8.4.3) [Adic Spaces]. The category of **affinoid adic spaces** is the full subcategory of the Huber category whose objects are isomorphic to $\mathrm{Spa}(A, A^+)$ for some Huber pair (A, A^+), and the category of **adic spaces** is the full subcategory of Huber category whose objects are locally isomorphic to an affinoid adic space. ⌟

Prop. (17.8.4.4) [Adic Spectrum Adjointness]. For any affinoid adic space $X = \mathrm{Spa}(R, R^+)$ and Y an arbitrary adic space, then there is a natural isomorphism

$$\mathrm{Hom}(Y, X) \cong \mathrm{Hom}((R, R^+), (\mathcal{O}_Y(Y), \mathcal{O}_Y^+(Y))).$$

⌟

Proof: It suffices to show for $Y = (S, S^+)$ affine, because an morphism from $Y \to X$ is glued from local morphisms, and $\mathcal{O}_Y$ is a sheaf.

For this, Cf.Huber94 Prop2.1(2).? □

Def. (17.8.4.5) [Uniform Adic Spaces]. An adic space X is called **uniform** if for all open affinoid $U = \mathrm{Spa}(R, R^+) \subset X$, the Huber ring R is uniform. ⌟

Cartier Divisors and Closed Immersions

Def. (17.8.4.6)[Cartier Divisors]. Let X be a uniform analytic adic space, then a (effective)**Cartier divisor** on X is an ideal sheaf $\mathcal{I} \subset \mathcal{O}_X$ that is locally free of rank 1. The support of a Cartier divisor is $\mathrm{Supp}(\mathcal{O}_X/\mathcal{I})$.

The support Z of a Cartier divisor is a nowhere dense closed subset of X, and the map $I \mapsto \mathcal{I} = i\mathcal{O}_X$ induces a bijection between invertible ideals $I \subset R$ that $V(I)$ is nowhere dense in X and Cartier divisors on X. ⌟

Proof: By(17.8.4.21), any Cartier divisor is of the form $I \otimes_R \mathcal{O}_X$ for some invertible ideal $I \subset R$. We need to show that $\varphi : I \otimes_R \mathcal{O}_X \to \mathcal{O}_X$ is injective iff $V(I) \subset X$ is nowhere dense.

By restriction, we can assume $I = (f)$ is principle, and if $V(f)$ contains an open subset, then on an open rational subset, $f = 0$ by uniformity(17.8.2.14), so φ is not injective. Conversely, if if $V(f)$ is nowhere dense, we show f is a nonzero-divisor: if $fg = 0$ and $g \neq 0$, then $U = U(\frac{g}{g})$ is contained in $V(f)$ and is open, so $U = 0$, which implies $g = 0$ by uniformity(17.8.2.14), contradiction. □

Prop. (17.8.4.7). Let X be a uniform analytic adic space and $\mathcal{I} \subset \mathcal{O}_X$ a Cartier divisor with support Z and $j : U = X \backslash Z \to X$. There are injective maps of sheaves

$$\mathcal{O}_X \hookrightarrow \varinjlim_n \mathcal{I}^{-n} \hookrightarrow j_* \mathcal{O}_U.$$

⌟

Proof: This is local, it suffices to check this is for any affine subscheme of X, so we can assume $X = \mathrm{Spa}(R, R^+)$ and $\mathcal{I} = f\mathcal{O}_X$ for some nonzero-divisor $f \in R$ whose vanishing locus Z is nowhere dense, and check the global sections:

$$R \to R[\frac{1}{f}] \to \Gamma(U, \mathcal{O}_U).$$

Then it suffices to show $R \to \Gamma(U, \mathcal{O}_U)$ is injective. But if g vanishes on U, then the vanishing locus of g is a closed subset containing U, which implies that it is all of X as Z is nowhere dense, so $g = 0$ by uniformity(17.8.2.14). □

Def. (17.8.4.8) [Meromorphic Along the Cartier Divisor]. A function $f \in H^0(U, \mathcal{O}_U)$ is **meromorphic along** the Cartier divisor $\mathcal{I} \subset \mathcal{O}_X$ if it lifts to $H^0(X, \varinjlim_n \mathcal{I}^{-n})$. ⌟

Def. (17.8.4.9) [Closed Cartier Divisors]. On a uniform analytic adic space X, a **closed Cartier divisor** is a Cartier divisor $\mathcal{I} \subset \mathcal{O}_X$ with support Z that $(Z, \mathcal{O}_X/\mathcal{I}, |\cdot|_x, x \in Z)$ is an adic space. ⌟

Prop. (17.8.4.10) [Closed Cartier Divisor and Closed Immersion]. On a uniform analytic adic space X, a Cartier divisor $\mathcal{I} \subset \mathcal{O}_X$ is closed iff the map $\mathcal{I}(U) \hookrightarrow \mathcal{O}_X(U)$ has closed image for all open affinoid $U \subset X$. In this case, for all open affinoid $U = \mathrm{Spa}(R, R^+) \subset X$, the intersection $U \cap Z = \mathrm{Spa}(S, S^+)$ is an affinoid adic space, where $S = R/I$ and S^+ is the integral closure of the image of R^+ in S. ⌟

Proof: The property of having closed image can be checked locally as affinoid subspace is quasi-compact. The fact $\mathcal{O}_X/\mathfrak{I}$ is a $(\mathcal{O}_X/\mathfrak{I})(U_i)$ is separated for an open covering $\{U_i\}$ of X, so at $\mathcal{I}(U_i)$ is closed in $\mathcal{O}_X(U_i)$.

Conversely, if $\mathcal{I}(U) \hookrightarrow \mathcal{O}_X(U)$ has closed image for all open affinoid $U \subset X$, we want to show $(Z, \mathcal{O}_X/\mathcal{I}, |\cdot|_x, x \in Z)$ is an adic space: We can construct this locally, so if $X = \mathrm{Spa}(R, R^+)$, $S = R/I$ is separated and complete, thus a complete Huber ring, and consider the quotient Huber ring(11.2.5.19) (S, S^+), then $\mathrm{Spa}(S, S^+) \to \mathrm{Spa}(R, R^+)$ is a closed immersion of topological spaces with image $V(I)$.

What's left to show is that the map of presheaves $\mathcal{O}_X/\mathcal{I} \to \mathcal{O}_Z$ is an isomorphism, and also $\mathcal{O}_X/\mathcal{I}(U) = \mathcal{O}_X(U)/\mathcal{I}(U)$. To show this, we first show the presheaf $\mathcal{O}_X/\mathcal{I}$ is a sheaf: this is by 3×3-lemma: $\mathcal{I}$ is locally (f), and for a rational covering $U_i \to X$,

$$\mathcal{O}_X(X)/f \to \prod_i \mathcal{O}_X(U_i)/f \rightrightarrows \prod_{ij} \mathcal{O}_X(U_{ij})/f$$

is exact.

And to show $\mathcal{O}_X/\mathcal{I} \to \mathcal{O}_Z$ is an isomorphism, it suffices to notice taking localization and taking quotient commutes, because they are both defined by universal properties.(11.2.5.19)(11.2.5.32). $\square$

Remark (17.8.4.11). Even if A is Tate and stably uniform, and $f \in A$ is a nonzero-divisor that $fA \subset A$ is closed, it may not be true that $\mathcal{O} = f\mathcal{O}_X \hookrightarrow \mathcal{O}_X$ is a closed Cartier divisor on $X = \mathrm{Spa}(A, A^+)$. This is because there may be rational localization $(A, A^+) \to (B, B^+)$ that fB is not closed in B. Cf. [Ked19]P16. ⌟

Examples of Adic Spaces

Prop. (17.8.4.12) [Examples of Adic Spaces].

- (Adic Closed Unit Disk) The space $\mathrm{Spa}(\mathbb{Z}[T]) = \mathrm{Spa}(\mathbb{Z}[T], \mathbb{Z}[T])$ represents the functor $X \mapsto \mathcal{O}_X^+(X)$.
- (Adic Affine Line) The functor $X \mapsto \mathcal{O}_X(X)$ is also representable, by $\mathrm{Spa}(\mathbb{Z}[T], \mathbb{Z})$. Notice for any non-Archimedean field K,
$$\mathrm{Spa}(\mathbb{Z}[T], \mathbb{Z}) \times \mathrm{Spa}\, K = \cup_{n\geq 1} \mathrm{Spa}\, K\langle \varpi^n T\rangle = \varinjlim_{n, T\mapsto \varpi T} \mathrm{Spa}\, K\langle T\rangle.$$
This is because For any Huber pair (R, R^+) over $(K, \mathcal{O}_K)$, $R = \cup_n \varpi^{-n} R^+$ because ϖ is topologically nilpotent.
- (The Open Unit Disk) Let $D = \mathrm{Spa}\, \mathbb{Z}[[T]]$, then for any non-Archimedean field K, $D_K = D \times \mathrm{Spa}\, K$ represents the functor that maps a K-algebra R to all its elements of norm ≤ 1. Then this the open disk over K. And D_K is also represented by
$$\cup_{n\geq 1} \mathrm{Spa}\, K\langle T, \frac{T^n}{\varpi}\rangle.$$
- (The Punctured Open Unit Disk) Let $D^* = \mathrm{Spa}\, \mathbb{Z}((T))$, then
$$D_K^* = D^* \times \mathrm{Spa}\, K = D_K\langle \frac{T}{T}\rangle = D_K \backslash \{0\}$$

⌟

Prop. (17.8.4.13) [The Open Unit Disk over $\mathbb{Z}_p$]. Consider $X = \mathbb{Z}_p[[T]]$ with the (p, T)-adic topology, there is exactly one non-analytic point $x = x_{\mathbb{F}_p}$. Let $X = \mathrm{Spa}(\mathbb{Z}_p[[T]])$ and $\mathcal{Y} = X\backslash\{x_{\mathbb{F}_p}\}$, then for a point $x \in \mathcal{Y}$, $T(x)$ and $p(x)$ cannot both be 0 by(11.2.6.2).

Then there exists a unique continuous map
$$\kappa : |\mathcal{Y}| \to [0, \infty]$$
characterized by the following property: For any rational number $m/n < r, |T(x)|^n > |p(x)|^m$, and for any rational number $m/n > r, |T(x)|^n < |p(x)|^m$. This map κ is surjective. ⌟

Proof: Let $\widetilde{x}$ be a maximal vertical generalization of x, then it has rank 1 and we can assume $\widetilde{x}$ is real valued by(11.2.3.8). Now we define
$$\kappa(x) = \frac{\log |T(\widetilde{x})|}{\log |p(\widetilde{x})|},$$

This is definable as $T(\widetilde{x})$ and $p(\widetilde{x})$ cannot both be 0.

The uniqueness of $\kappa(x)$ follows from the fact $|T(x)|^n > |p(x)|^m$ implies to $|T(\widetilde{x})|^n \geq |p(\widetilde{x})|^m$ because $\widetilde{x}$ is a generalization of x.

To show κ satisfies the condition, if $m/n < r$, then $|T(\widetilde{x})|^n > |p(\widetilde{x})|^m$, so $|T(x)|^n > |p(x)|^m$ because $x, \widetilde{x}$ define the same topology. And it is continuous because

$$\kappa^{-1}((-\infty, r)) = \cup_{m/n<r} U(\frac{T^n}{p^m}).$$

To show the surjectivity, if $\kappa = [x_0 : x_1]$, define the valuation as

$$v(\sum a_{ij} p^i T^j) = \sup_{a_{ij}\neq 0} e^{-x_0 i - x_1 j}$$

where $(a_{ij})^p = 1$. □

Construction of Adic Spaces

Def. (17.8.4.14) [Fiber Products of Adic Spaces and Schemes]. Cf.[Wed14]P91. ⌟

Def. (17.8.4.15) [Adic Spaces attached to Schemes]. ⌟

Def. (17.8.4.16) [Adic Spaces attached to Formal Schemes]. Cf.[Wed14]. ⌟

Def. (17.8.4.17) [Adic Spaces attached to Rigid Analytic Spaces]. Cf.[Wed14]. ⌟

Sheaves and Vector Bundles

Def. (17.8.4.18). Let (A, A^+) be a Huber pair and $X = \mathrm{Spa}(A, A^+)$, let $\widetilde{M} = M \otimes_A \mathcal{O}_X$ be the presheaf on X. ⌟

Prop. (17.8.4.19). If A is sheafy, then for any finite projective A-module M, the presheaf $\widetilde{M}$ is a sheaf on $X = \mathrm{Spa}(A, A^+)$, and $H^i(U, \mathcal{F}) = 0$ for any rational subset of X and $i > 0$. ⌟

Proof: Because M is a direct sum of a finite free A-module, then we reduce to the case $\mathcal{O}_X$ is sheafy. □

Remark (17.8.4.20). This is a partial analogy with Tate's acyclicity theorem in rigid analytic geometry(17.5.1.40)(17.5.3.10), but it only holds for f.p. modules, not even f.g. modules. One impediment is that the rational localization map are generally not flat. To get around this, Kedlaya defined a category of pseudo-coherent modules, with the property that even when flatness fails, tensoring is also exact in this category. ⌟

Prop. (17.8.4.21) [Vector Bundles]. Let (A, A^+) be a sheafy analytic Huber pair and $X = \mathrm{Spa}(A, A^+)$, then the functor $M \to \widetilde{M}$ from the category of finite projective A-modules to the category Vect_X of locally finite free $\mathcal{O}_X$-modules is an equivalence of categories. In particular, Vect_X only depends on A. ⌟

Proof: Cf.[Ked19].P40**?** □

Pre-Adic Spaces

Main references are [S-W20]L3 and [Ked19].

Def. (17.8.4.22) [Pre-Adic Spaces]. ⌟

Remark (17.8.4.23). Pre-adic spaces is an approach to work around the failure of sheafyness of general Huber pair, with techniques from algebraic stacks. ⌟

Analytic Points

Prop. (17.8.4.24) [Analytic and Tate Rings]. Let (A, A^+) be a complete Huber pair, then

- The Huber ring A is analytic iff all points of $\mathrm{Spa}(A, A^+)$ are analytic.
- A point $x \in \mathrm{Spa}(A, A^+)$ is analytic iff there is a rational nbhd $U \subset \mathrm{Spa}(A, A^+)$ that $\mathcal{O}_X(U)$ is Tate.

⌟

Proof: 1: x is non-analytic iff $A^{00} \subset \mathfrak{p}_x$ by(11.2.6.5), so all points are analytic iff $A^{00}A = A$, which means A is analytic.

2: Let x be an analytic point, then there exists $f \in I$ where I is an ideal of definition that $|f|_x \neq 0$. Now $\{g \in A||g(x)| \leq |f(x)\}$ is open(because $|\cdot|_x$ is continuous), so contains some I^n. Now let $I^n = (g_1, \ldots, g_k)$, then $U(\frac{g_1,\ldots,g_k}{f})$ is a rational subset. Then in $\mathcal{O}_X(U)$, f is a unit, but also it is topologically nilpotent, because it is contained in I.

Conversely, if $x \in X$ has a rational nbhd $U = U\langle\frac{T}{s}\rangle$ such that $\mathcal{O}_X(U)$ is Tate, and x is not analytic, then $\mathfrak{p}_x$ contains an ideal of definition $I \subset A_0$. Now let $f \in \mathcal{O}_X(U)$ be a topologically nilpotent unit, then there exists $m \geq 1$ that f^m lies in the closure of $IA_0[t/s|t \in T]$ in $\mathcal{O}_X(U)$. Since $x \in U$, the valuation $|\cdot|_x$ extends to $\mathcal{O}_X(U)$, and since $|\cdot|_x$ is continuous, $|f^m(x)| = 0$, contradiction, as f is a unit in $\mathcal{O}_X(U)$. □

Def. (17.8.4.25) [Analytic Points]. Let X be a pre-adic space, then a point $x \in X$ is called an **analytic point** if there is some open affinoid nbhd $U = \mathrm{Spa}(A, A^+) \subset X$ of x that A is Tate. And X is called **analytic** if all of its points are analytic. ⌟

Prop. (17.8.4.26). Let $f : X \to Y$ be a map of analytic pre-adic spaces, then $|f| : |X| \to |Y|$ is generalizing. If f is quasi-compact and surjective, then $|f|$ is a quotient map. ⌟

Proof: Cf.[Hub96]1.1.10. and [Étale Cohomology of Diamonds, L2.5].**?** □

Def. (17.8.4.27). A map $f : Y \to X$ of pre-adic spaces is called **analytic** if it carries analytic points to analytic points. ⌟

Proof of Acyclicity and Sheafyness by Cech Reduction

Def. (17.8.4.28) [Standard Rational Coverings]. Let $X = \mathrm{Spa}(A, A^+)$ and $f_1, \ldots, f_n \in A$ which generates the unit ideal, then the sets $X(\frac{f_1,\ldots,f_n}{f_i})$ covers X, called the **standard rational covering** of X. And if $n = 2$, it is called a **standard binary rational covering** of X.

There are special types of standard binary rational coverings: if $f_1 = f, f_2 = 1$, then it is called a **simple Laurent covering**. If $f_1 = f, f_2 = 1 - f$, then it is called a **simple balanced covering**. ⌟

Lemma (17.8.4.29) [Reduction of Coverings]. Let A be an analytic Huber ring,

- (Huber) Every open covering of X can be refined by some standard rational covering.
- (Gabber-Ramero) Every open covering of a rational subspace of X can be refined by some compositions of simple Laurent coverings and simple balanced coverings.

⌟

Proof: 1: Cf.[Ked19]P28.
2: Cf.[Ked19]P29. □

Prop. (17.8.4.30)[Cech Reduction]. By a Cech cohomological argument the same as Tate's acyclicity theorem in rigid geometry(17.5.1.40), it suffices to prove any presheaf is a sheaf or any sheaf is acyclic on simple Laurent coverings and simple balanced coverings.

That is, for every rational localization (B, B^+) over (A, A^+), every pair $f, g \in B$ that $g = f$ or $1 - f$, if the sequence

$$0 \to B \to B\langle \frac{f}{g}\rangle \oplus B\langle \frac{g}{f}\rangle \to B\langle \frac{f}{g}, \frac{g}{f}\rangle \to 0,$$

- is exact at exact at left and middle, then $\mathcal{O}_X$ is sheafy.
- is exact, then $\mathcal{O}_X$ is acyclic.

Also remember the following equations:

$$B\langle \frac{f}{g}\rangle = B\langle T\rangle/\overline{(f - gT)}, \quad B\langle \frac{g}{f}\rangle = B\langle T\rangle/\overline{(g - fT)}, \quad B\langle \frac{f}{g}, \frac{g}{f}\rangle = B\langle T, T^{-1}\rangle/\overline{(f - gT)}$$

⌟

Prop. (17.8.4.31) [Properties of (Finite)Étale Maps].

- (Finite)Étale maps are invariant under compositions and pullbacks.
- If g and gf are (finite)étale, then so is f.
- f is (finite)étale iff $f^\flat$ is (finite)étale.

⌟

Proof: Cf.[S-W20]P65. □

5 Perfectoid Spaces

Affinoid Perfectoid Spaces

Def. (17.8.5.1) [Perfectoid Spaces]. For any perfectoid affinoid algebra R, we associated to it an affinoid adic space $\mathrm{Spa}(R, R^+)$, called an **affinoid perfectoid space**.

Tate's acyclicity(17.8.6.19) shows that the adic spectra of perfectoid affinoid algebras are sheafy, so we can defined the category of **perfectoid spaces** $\mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$ to be the full subcategory of adic spaces that are locally isomorphic to affinoid perfectoid spaces. ⌟

Remark (17.8.5.2). Notice that it is not true that if $(A, A^+) \in \mathcal{H}\mathrm{ubPair}$ and $\mathrm{Spa}(A, A^+) \in \mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$, then $A \in \mathcal{P}\mathrm{erfd}$. Thus there is ambiguity to the term affinoid perfectoid spaces. But we always use this to mean the affinoid adic space associated to a perfectoid Huber pair. ⌟

Proof: Cf.[Ked19]P62. □

Prop. (17.8.5.3). The absolute product of two perfectoid spaces of char p is also a perfectoid space. ⌟

Proof: Cf.[Sch17]P71. □

Prop. (17.8.5.4) [Fiber Products of Perfectoid Spaces]. $\mathcal{P}\mathrm{erfd}_K$ admits fiber products. ⌟

Proof: Perfectoid spaces are constructed by glueing, thus it suffices to show that the category of perfectoid $K^\flat$-algebras has fiber pushouts, by tilting equivalence. For this, if $X = (A, A^+), Y = (B, B^+), Z = (C, C^+)$, define $X \otimes_Y Z = (D, D^+)$, where D is the completion of $A \otimes_B C$, and D^+ is the completion of the integral closure of $A^+ \otimes_{B^+} C^+$ in D. Then D is a perfect $K^\flat$-algebra, and it is truly the filtered colimits, by(11.2.5.23).

Notice that we don't even need a base field K, Cf.[Ked19]P57. □

Tiltings

Prop. (17.8.5.5) [Tilting Rational Subsets]. For a perfectoid affinoid K-algebra (R, R^+) over a perfectoid field K,

- The $\sharp$ map induces an isomorphism $X = \mathrm{Spa}(R, R^+) \cong X^\flat = \mathrm{Spa}(R^\flat, R^{\flat 0})$ that identifies rational open subsets.
- For a rational subset U with tilting $U^\flat$, the complete affinoid Tate algebra $(\mathcal{O}_X(U), \mathcal{O}_X^+(U))$ is perfectoid over R with tilt $(\mathcal{O}_{X^\flat}(U^\flat), \mathcal{O}_{X^\flat}^+(U^\flat))$.

⌟

Proof: This follows from(17.8.5.9). □

Lemma (17.8.5.6) [Huber's Presheaf in Char p]. Assume char$K = p$ and $U = X(\frac{f_1,\ldots,f_n}{g})$ is a rational subset that $f_i, g \in R^+$ and $f_n = \varpi^N$, then:

- Consider the subring $R^+[(\frac{f_i}{g})^{\frac{1}{p^\infty}}]$, its ϖ-adic completion $(R^+\langle(\frac{f_i}{g})^{\frac{1}{p^\infty}}\rangle)^a$ is a perfectoid K^{0a}-algebra.
- The map $R^+[X_i^{\frac{1}{p^\infty}}] \to R^+[(\frac{f_i}{g})^{\frac{1}{p^\infty}}]$ has kernel containing and almost equal to $I = (g^{\frac{1}{p^m}} X_i^{\frac{1}{p^m}} - f_i^{\frac{1}{p^m}})$.
- $\mathcal{O}_X(U)$ is a perfectoid K-algebra and $\mathcal{O}_X(U)^{0a} \cong (R^+\langle(\frac{f_i}{g})^{\frac{1}{p^m}}\rangle)^a$.

⌟

Proof: 1: The ring $R^+[(\frac{f_i}{g})^{\frac{1}{p^\infty}}]$ is perfect and ϖ-torsion-free, and R^+ is semi-perfect, thus its completion is clearly a perfectoid K^{0a}-algebra by(11.2.9.1).

2: Clearly $I \subset \ker$ and notice $R^+[(\frac{f_i}{g})^{\frac{1}{p^\infty}}][\varpi^{-1}] = R[g^{-1}]$ as $f_n = \varpi^N$, so $I[\varpi^{-1}] = \ker[\varpi^{-1}]$. Now consider the mapping

$$P_0 = R^+[X_i^{\frac{1}{p^\infty}}]/I \to R^+[(\frac{f_i}{g})^{\frac{1}{p^\infty}}]$$

Now this map is an isomorphism ofter inverting ϖ, so the kernel is ϖ^∞-torsion. But we have $I = I^{[p]}$ because R^+ is semi-perfect, so P_0 is perfect, so the kernel must be almost zero.

3: Consider the inclusion $R^+[\frac{f_i}{g}] \hookrightarrow R^+[(\frac{f_i}{g})^{\frac{1}{p^\infty}}]$, we show the cokernel is killed by ϖ^{nN}: as $f_n = \varpi^N$,

$$\varpi^{nN} \prod_{i=1}^n (\frac{f_i}{g})^{\frac{1}{p^{a_i}}} = \prod_{i=1}^n (f_i^{\frac{1}{p^{a_i}}} g^{1-\frac{1}{p^{a_i}}}) \frac{f_n}{g} \in R^+[\frac{f_i}{g}].$$

So these two ring has the same ϖ-adic completion, the first one is just $\mathcal{O}_X(U)$ by the construction(17.8.3.1), so $\mathcal{O}_X(U)$ is perfectoid K-algebra, and the isomorphism is by tilting equivalence $\mathrm{perf}_K \cong \mathrm{perf}_{K^{0a}}$(11.2.9.5). □

Lemma (17.8.5.7) [Huber's Presheaf in Char 0]**.** Let $U = X(\frac{f_1,\dots,f_n}{g})$ is a rational subset that f_i, g are perfect elements in R^+, $f_i = a_i^\sharp, g = b^\sharp$, and $f_n = \varpi^N$, so f_i, g have compatible p^n-th roots, then let $U^\flat = X^\flat(\frac{f_1,\dots,f_n}{g})$ be the tilting of U, U is the inverse image of $U^\flat$ along the map $X \to X^\flat$. Then the conclusion of(17.8.5.6) is also true, and moreover, $(\mathcal{O}_X(U), \mathcal{O}_X^+(U))$ tilts to $(\mathcal{O}_{X^\flat}(U^\flat), \mathcal{O}_{X^\flat}^+(U^\flat))$. ⌟

Proof: $1, 2$ of(17.8.5.6): Notation as before, there is a map $P_0 = R^+[X_i^{\frac{1}{p^\infty}}]/I \to R^+[(\frac{f_i}{g})^{\frac{1}{p^\infty}}]$, and an inclusion $R^+[(\frac{f_i}{g})^{\frac{1}{p^\infty}}] \to \mathcal{O}_X^+(U)$. Now write (S, S^+) for the untilt of the perfectoid $(R^\flat, R^{\flat+})$-algebra $(\mathcal{O}_{X^\flat}(U^\flat), \mathcal{O}_{X^\flat}^+(U^\flat))$, then by the tilting process(11.2.9.13), $\mathrm{Spa}(S, S^+)$ maps into U, so by the universal property, there is a map

$$\mu : (\mathcal{O}_X(U), \mathcal{O}_X^+(U)) \to (S, S^+).$$

Consider the composition

$$P_0 \xrightarrow{a_0} R^+[(\frac{f_i}{g})^{\frac{1}{p^\infty}}] \xrightarrow{d_0} S^+,$$

we prove their completion gives the same K^{0a}-algebras(notice S^+ is already complete): a_0 is surjective, thus so does its completion, the map $d_0 \circ a_0$ is almost isomorphism modulo ϖ by(17.8.5.6) item2 and tilting equivalence, so does its completion. Now(5.7.3.2) tells us the completion of $d_0 \circ a_0$ is almost isomorphism, so does a and d as a is surjective.

By the way, we know that $R^+\langle(\frac{f_i}{g})^{\frac{1}{p^\infty}}\rangle[\varpi^{-1}]$ is the untilt of $\mathcal{O}_{X^\flat}^+(U^\flat)$.

3 of(17.8.5.6) is proved as before.

For the tilting, by the above, we already know $R^+\langle(\frac{f_i}{g})^{\frac{1}{p^\infty}}$ tilts to the perfectoid $K^{\flat 0a}$-algebra $\mathcal{O}_{X^\flat}(U^\flat)^{0a}$, and by item3 $\mathcal{O}_X(U)$ tilts to the perfectoid $K^\flat$-algebra $\mathcal{O}_{X^\flat}(U^\flat)$. Now the question is the tilt of $\mathcal{O}_X^+(U)$, notice as in the proof of item1, there is a natural map

$$(R^+\langle(\frac{f_i}{g})^{\frac{1}{p^\infty}}\rangle[\varpi^{-1}], R^+\langle(\frac{f_i}{g})^{\frac{1}{p^\infty}}\rangle) \to (\mathcal{O}_X(U), \mathcal{O}_X^+(U)),$$

whose tilting gives by university of Huber's presheaf a map

$$\xi : (\mathcal{O}_{X^\flat}(U^\flat), \mathcal{O}_{X^\flat}^+(U^\flat)) \to (\mathcal{O}_X(U), \mathcal{O}_X^+(U))^\flat.$$

These two map μ, ξ are inverse to each other, showing that the tilting of $(\mathcal{O}_X(U), \mathcal{O}_X^+(U))$ is $(\mathcal{O}_{X^\flat}(U^\flat), \mathcal{O}_{X^\flat}^+(U^\flat))$. □

Lemma (17.8.5.8) [Approximation Lemma]. Assume $R = K\langle T_0^{\frac{1}{p^\infty}}, \dots, T_0^{\frac{1}{p^\infty}}\rangle$, $f \in R^0$ is homogenous of degree $d \in \mathbb{N}[p^{-1}]$, then for any $c > 0, \varepsilon > 0$, there exists some $g_{c,\varepsilon} \in R^{\flat 0}$ homogeneous of degree d that

$$|(f - g^\sharp)(x)| \le |\varpi|^{1-\varepsilon} \max\{|f(x)|, |\varpi|^c\}.$$

In particular, if $\varepsilon < 1$, then

$$\max\{|f(x)|, |\varpi|^c\} = \max\{|g_{c,\varepsilon}^\sharp(x)|, |\varpi|^c\}.$$

⌟

Proof: Cf.[Sholze Perfectoid Spaces, Lemma6.5]?. □

Prop. (17.8.5.9). For any $R \in \mathcal{P}\mathrm{erfd}_K$,

- The same conclusion of(17.8.5.8) holds.
- For $f, g \in R$, there exist $a, b \in R^\flat$ that $X(\frac{f,\varpi^c}{g}) = X(\frac{a^\sharp,\varpi^c}{b^\sharp})$. In particular, any rational subsets U of X comes from $X^\flat$, thus(17.8.5.7) applies for U.
- For any $x \in X$, the non-Archimedean field $\widehat{k(x)}$ is perfectoid.
- $X \to X^\flat$ is a homeomorphism preserving rational subsets.

⌟

Proof: 1: Using the tilting equivalence, we can write $f = g_0^\sharp + \varpi g_1^\sharp + \ldots + \varpi^c g_c^\sharp + f_{c+1}\varpi^{c+1}$, let $f_0 = g_0^\sharp + \varpi g_1^\sharp + \ldots + \varpi^c g_c^\sharp$. Then notice that the solution $g_{c,\varepsilon}$ for f_0 is suitable for f as well. So now if we consider the mapping

$$\mu : K\langle T_0^{\frac{1}{p^\infty}}, \ldots, T_n^{\frac{1}{p^\infty}}\rangle \to R : T_i \to g_i^\sharp,$$

together with its tilting

$$\mu^\flat : K^\flat\langle T_0^{\frac{1}{p^\infty}}, \ldots, T_n^{\frac{1}{p^\infty}}\rangle \to R^\flat.$$

Then for the approximation $g_{c,\varepsilon}^\sharp$ for $f' = \sum \varpi^i T_i$, $\mu^\flat(g)$ is what we are searching for.

2: Using 1, we find $a, b \in R^\flat$ that $|(g - b^\sharp)(x)| < \max\{|g(x)|, \varpi^c\}$ and $\max\{|f(x)|, |\varpi|^c\} = \max\{|a^\sharp(x)|, |\varpi|^c\}$ for all $x \in \mathrm{Spa}(R, R^+)$. Then it is routine to check that $X(\frac{f,\varpi^c}{g}) = X(\frac{a^\sharp,\varpi^c}{b^\sharp})$.

3: By(17.8.3.5), $\widehat{k^+(x)}$ equals the completion of the colimit $\mathrm{colim}\, \mathcal{O}_X^+(U)$ over rational subsets U containing x. As these are all perfectoid K^{0a}-algebras(11.2.9.14), and completion of the filtered limits of perfectoid K^{0a}-algebras is perfectoid(11.2.9.10), we know that $\widehat{k^+(x)}$ is perfectoid over K^{0a}, thus inverting ϖ shows $k(x)$ is also perfectoid over K.

4: this is injective because X is T_0 and a rational subset is the untilt of a ratinal subset of $X^\flat$ by item2. For surjectivity, a point of $X^\flat$ determines a continuous map $(R^\flat, R^{\flat+}) \to (\widehat{k(x)}, \widehat{k^+(x)})$, thus by untilting(11.2.9.13) corresponds to a map $(R, R^+) \to (L, L^+)$, then (L, L^+) is a perfectoid field, by(11.2.9.15), so it sorresponds to a point $y \in X$. Then it is clear that y maps to x, because the diagram $\begin{array}{ccc} R^\flat & \xrightarrow{\sharp} & R \\ \downarrow & & \downarrow \\ \widehat{k(x)} & \xrightarrow{\sharp} & L \end{array}$ is commutative. □

Prop. (17.8.5.10) [Tilting Equivalence for Perfectoid Spaces]. Fix a perfectoid field K, then for any perfectoid space X/K, there is a unique perfectoid space $X^\flat/K^\flat$ that satisfies: $X(R, R^+) \cong X^\flat(R^\flat, R^{\flat+})$ functorially, called the **tilt** of X. Moreover, this $X^\flat$ satisfies naturally $|X| \cong |X^\flat|$.

When X is an affinoid perfectoid space, this tilting coincides with that of(17.8.5.5).

And this tilting induces an equivalence between the category of perfectoid spaces over K and perfectoid spaces over $K^\flat$. ⌟

Proof: Firstly, the universal property truly determines the tilt $X^\flat$ uniquely: if there are two tilts X_1, X_2, as they are locally affinoid perfectoid like $\mathrm{Spa}(R^\flat, R^{\flat+})$ by(17.8.5.5), the immersion map $\mathrm{Spa}(R^\flat, R^{\flat+}) \to X_1$ determines via the functorial isomorphism a morphism $\mathrm{Spa}(R^\flat, R^{\flat+}) \to X_2$. Now X_1 has a sheaf structure, so these morphisms glue to give a morphism $X_1 \to X_2$. The same argument shows conversely there is a morphism $X_2 \to X_1$, and they are clearly converse to each other, so $X_1 \cong X_2$.

The construction of X is just the glueing of the tilting of the affinoid perfectoid spaces, as the tilting defined in(17.8.5.5) is a functor. The universal property is verified by just checking on the affinoid perfectoid spaces, as we can glue using the sheaf property. For the affinoid case, we should use(17.8.4.4). The last assertion is by(17.8.5.5). □

6 Properties of Perfectoid Spaces

Totally Disconnected Spaces

Def. (17.8.6.1) [Totally Disconnected Spaces]. A perfectoid space X is called **totally disconnected** if it is qcqs and any open covering $\{U_i \to X\}$ splits, i.e. $\coprod U_i \to X$ splits, or equivalently, there is a refinement covering $\{V_i \to X\}$ that $X \cong \coprod V_i$.

A perfectoid space X is called **strictly totally disconnected** if it is qcqs and every étale cover splits. ⌟

Prop. (17.8.6.2). Let X be a qcqs perfectoid spaces, then X is totally disconnected iff all its connected components are of the form $\mathrm{Spa}(K, K^+)$ where (K, K^+) are perfectoid affinoid fields. And it is strictly totally disconnected if moreover K are all alg.closed. ⌟

Proof: Cf.[Sch17].P29, P35. □

Prop. (17.8.6.3). if X is a totally disconnected perfectoid space, then X is affinoid. ⌟

Proof: Cf.[Sch17].P30.? □

Injections

Def. (17.8.6.4) [Injections]. A map $f : X \to Y$ of perfectoid spaces is called an injection if for any perfectoid space Z, $f_* : \mathrm{Hom}(Z, X) \to \mathrm{Hom}(Z, Y)$ is an injection. ⌟

Prop. (17.8.6.5) [Residue Field Map is Injection]. Let X be a perfectoid space and $x \in X$, giving rise to a map of residue fields

$$i_x : \mathrm{Spa}(\kappa(x), \kappa(x)^+) \to X,$$

then i_x is an injection of perfectoid spaces. ⌟

Proof: To show this, firstly we can replace X with an affinoid nbhd of X. Then notice that $\mathrm{Spa}(\kappa(x), \kappa(x)^+)$ is the filtered limit over all rational nbhds U of x in X, and for each U, $U \to X$ is an injection by definition(17.8.3.1), so i_x is also an injection. □

Prop. (17.8.6.6) [Characterizations of Injections]. Let $f : Y \to X$ be a map of perfectoid spaces, then the following conditions are equivalent:

- f is an injection.
- For any perfectoid adic field (K, K^+), the map of sets $f_* : Y(K, K^+) \to X(K, K^+)$ is an injection.
- The map $|f| : |Y| \to |X|$ is injective, and for all rank 1 point $y \in Y$ with image $f(y) = x \in X$, the map of completed residue fields $\kappa(x) \to \kappa(y)$ is an isomorphism.

- The map $|f|:|Y|\to|X|$ is injective, and f is final in the category of maps $Z\to X$ that $|Z|\to|X|$ factors through the map $|Y|\to|X|$.

In particular, by item4, an injection of perfectoid spaces is determined by its topological map. ⌟

Proof: $4\to1\to2$ is trivial. For the rest, Cf.[Sch17]P21. □

Prop. (17.8.6.7) [Injection and Base Change].

- Let $f:Y\to X$ be an injection of perfectoid spaces, and $X'\to X$ any map of perfectoid spaces, then the pullback $f':Y'=Y\times_X X'\to X'$ is also an injection, and the induced map

$$|Y'|\to|Y|\times_{|X|}|X'|$$

is a homeomorphism.

A map of perfectoids spaces is an injection iff it is universally injective. ⌟

Proof: Cf.[Sch17]P24. □

Immersions

Def. (17.8.6.8) [Immersions]. $f:Y\to X\in\mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$ is called an **immersion of perfectoid spaces** if f is an injection and $|f|:|Y|\to|X|$ is a locally closed immersion. If $|f|$ is moreover closed or open, then it is called closed/open immersion. ⌟

Def. (17.8.6.9) [Zariski-Closed Immersion]. For $f:Z\to X\in\mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$ where $X=\mathrm{Spa}(R,R^+)$ is affinoid,

- f is called a **Zariski-closed immersion of perfectoid spaces** if f is a closed immersion and $|Z|=V(I)\subset|X|$, where $I\subset R$ is an ideal.
- f is called a **strongly Zariski-closed immersion of perfectoid spaces** if $Z=\mathrm{Spa}(S,S^+)$ is affinoid, $R\to S$ is surjective, and S^+ is the closure of R^+ in S.

⌟

Prop. (17.8.6.10).

- If f is strongly Zariski-closed, then f is Zariski-closed, in particular a closed immersion.
- If f is Zariski-closed, then Z is affinoid.
- If X is of characteristic p, and f is Zariski-closed, then f is strongly Zariski-closed.

⌟

Proof: Cf.[Sch12] Section2.5. □

Prop. (17.8.6.11). For any map of perfectoid spaces $Y\to X$, the diagonal map $\Delta_f:Y\to Y\times_X Y$ is an immersion. ⌟

Proof: Clearly Δ_f is an injection, thus it suffices to show that $|\Delta_f|$ identifies Y with a locally closed subset of $|Y\times_X Y|$. This can be checked locally on the target, so we can assume $X=\mathrm{Spa}(R,R^+)$ and $Y=\mathrm{Spa}(S,S^+)$, then the diagonal map is strongly Zariski closed, as $S\widehat{\otimes}_R S\to S$ is surjective and maps the integral closure of $S^+\widehat{\otimes}_{R^+}S^+\to S^+$ onto S^+. Thus by(17.9.1.11), Δ_f is a closed immersion in this case. □

Def. (17.8.6.12) [Separated Map]. A map $f:Y\to X\in\mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$ is called separated if Δ_f is a closed immersion. ⌟

Prop. (17.8.6.13)[Valuation Criterion]. Let $f : Y \to X$ be a map of perfectoid spaces. The following are equivalent:

- f is separated.
- $|\Delta_f| : |Y| \to |Y \times_X Y|$ is a closed immersion.
- $|f|$ is quasi-separated, and for any perfectoid adic field (K, K^+) and any diagram

$$\begin{array}{ccc} \mathrm{Spa}(K, \mathcal{O}_K) & \longrightarrow & Y \\ \downarrow & \nearrow & \downarrow f \\ \mathrm{Spa}(K, K^+) & \longrightarrow & X \end{array},$$

⌟

Almost Acyclicity

Def. (17.8.6.14) [p-Finite Tate Ring]. Denote $L = \widehat{\mathbb{F}_p[[t]]_{\mathrm{perf}}}[t^{-1}]$, an $\mathbb{F}_p[t]$ algebra A^+ is called **algebraically admissible** if it is f.p., reduced, t-torsion-free, and integrally closed in $A^+[t^{-1}]$. A perfectoid affinoid L-algebra (R, R^+) is called p**-finite** if it is the completion of the perfection(17.8.2.27) of a uniform Tate ring of the form $(A^+[t^{-1}], A^+)$, where A^+ is algebraically admissible. ⌟

Lemma (17.8.6.15) [Tate's Acyclicity for Classical Affinoid Algebra]. If A^+ is an algebraically admissible $\mathbb{F}_p[t]$-algebra, then $(A^+[t^{-1}], A^+)$ is a uniform affinoid Tate algebra(because it is finite), and:

- For any rational subset $U \subset X$, the structure presheaf $(\mathcal{O}_X(U), \mathcal{O}_X^+(U))$ is also uniform, and it is a perfection of an algebraically admissible $\mathbb{F}_p[t]$-algebra, so $\mathcal{O}_X^+(U) = \mathcal{O}_X(U)^0$.
- For any covering $\mathfrak{U} : U_i \to X$ of rational subsets, the Čech cohomology groups $H^i(\mathfrak{U}, \mathcal{O}_X^+)$ are all killed by t^N for N large.
- (A, A^+) is sheafy, with $H^i(X, \mathcal{O}_X^+)$ being t^∞-torsion for all i.

⌟

Proof: ? □

Lemma (17.8.6.16) [Tate's Acyclicity for p-Finite Perfectoid Algebras]. Let (R, R^+) be a p-finite perfectoid L-algebra that comes from the completion of perfection of (A, A^+), then:

- The map $X = \mathrm{Spa}(R, R^+) \to Y = \mathrm{Spa}(R, R^+)$ is a homeomorphism.
- For rational subset $V \subset Y$ with preimage $U \subset X$, $(\mathcal{O}_X(U), \mathcal{O}_X^+(U))$ is the completion of the perfection of $(\mathcal{O}_Y(V), \mathcal{O}_Y^+(V))$.
- For any covering $\mathfrak{U} : U_i \to X$ of rational subsets, the Čech cohomology groups $H^i(\mathfrak{U}, \mathcal{O}_X^0)$ are all almost zero.
- (R, R^+) is sheafy, with $H^i(X, \mathcal{O}_X^+)$ almost zero for all $i > 0$.

⌟

Proof: 1: This is because the adic spectrum is insensitive for perfection(17.8.2.27) and completion(17.8.2.16).

2: This is by the universal property, as these two are both the universal elements for the complete and affinoid adic spaces mapping to X that factors through U.

3: The complex calculating $H^i(\mathfrak{U},\mathcal{O}_X^0)$ is just the complex calculating $H^i(\mathfrak{U},\mathcal{O}_Y^+)$ under completion of perfection((17.8.2.26) used). So(17.8.6.15) and(17.8.6.17)(applied to every element) shows that the perfection makes the complex almost acyclic, and this is preserved under completion as $(-)^a$ is exact.

4: The complex calculating $H^i(\mathfrak{U},\mathcal{O}_X)$ is just the complex calculating $H^i(\mathfrak{U},\mathcal{O}_X^+)$ inverting t, thus they are all 0 as localization is exact. For the second, it is because of item3 and the fact $\mathcal{O}_X^+$ is almost isomorphic to $\mathcal{O}_X^0$(11.2.9.14). □

Lemma (17.8.6.17). Let A be a ring with an element t that admits compatible p^n-th roots, then for an A-module M that $t^N M=0$, consider the Frobenius pushforward $M\to F_*M$, then the colimit $\operatorname{colim}_{F_*} F_*^n M$ is naturally a module over A_{perf}, and it is annihilated by $t^{\frac{1}{p^n}}$ for all n. ⌟

Proof: The A_{perf} structure is natural, and notice $F_*^k M$ is annihilated by $t^{\frac{N}{p^k}}$, thus naturally the colimit is annihilated by $t^{\frac{1}{p^n}}$ for all n. □

Prop. (17.8.6.18) [Noetherian Approximation in Char p]. If K is a perfectoid field of char$p$ with pseudo-uniformizer t, then K is an extension of $L=\widehat{\mathbb{F}_p[[t]]_{\mathrm{perf}}}[t^{-1}]$, and If A is an K^0-perfectoid algebra that is integrally closed in $A[t^{-1}]$, then:

- A is a completion of a filtered colimit $(\operatorname{colim}_i B_i)^\wedge$ that B_i are p-finite, that induces an homeomorphism
$$\mathrm{Spa}(A[t^{-1}],A)\cong\varprojlim_i \mathrm{Spa}(B_i[t^{-1}],B_i)$$
that each rational subset of $\mathrm{Spa}(A[t^{-1}],A)$ comes from a rational subset of some $\mathrm{Spa}(B_i[t^{-1}],B_i)$.
- If $U_i\subset\mathrm{Spa}(B_i[t^{-1}],B_i)$ is a compatible system of rational subsets that corresponds to $U\subset\mathrm{Spa}(A,A^+)=X$, then
$$(\mathcal{O}_X(U),\mathcal{O}_X^+(U))\cong\varinjlim_j(\mathcal{O}_j(U_j),\mathcal{O}_j^+(U_j))^\wedge.$$

⌟

Proof: 1: $A=\operatorname{colim}_i A_i$, where A_i are all the f.p. $\mathbb{F}_p[t]$-algebras in A. Then each A_i is reduced(as A is complete and integrally closed in $A[t^{-1}]$) and t-torsion-free, and we can assume they are integrally closed in $A_i[t^{-1}]$ because A does, by passing to their integral closure.

Then applying the $(-)_{\mathrm{perf}}$ functor gives $\operatorname{colim}_i(A_i)_{\mathrm{perf}}=A$, as A is perfect, and applying the completion gives
$$(\operatorname{colim}_i\widehat{A_i})^\wedge=A,$$
as A is already complete, so we are done.

2: This is immediate from 1 and(17.8.2.26).

3: This is because by universal property for Huber presheaves, there are pushouts diagrams

$$\begin{array}{ccccccc}(B_i[t^{-1}],B_i) & \longrightarrow & (B_j[t^{-1}],B_j) & \longrightarrow & \ldots & \longrightarrow & (A[t^{-1}],A)\\ \downarrow & & \downarrow & & & & \downarrow\\ (\mathcal{O}_{X_i}(U_i),\mathcal{O}_{X_i}^+(U_i)) & \longrightarrow & (\mathcal{O}_{X_j}(U_j),\mathcal{O}_{X_j}^+(U_j)) & \longrightarrow & \ldots & \longrightarrow & (\mathcal{O}_X(U),\mathcal{O}_X^+(U))\end{array}$$

So the conclusion follows as colimits commutes with colimits. □

Prop. (17.8.6.19) [Almost Acyclicity for Perfectoids]. Fix a perfectoid field K and a perfectoid affinoid K-algebra (R, R^+) with adic spectrum $X = \mathrm{Spa}(R, R^+)$, then

- (R, R^+) is sheafy, i.e. $\mathcal{O}_X$ and $\mathcal{O}_X^+$ are sheaves.
- $\mathcal{O}_X^+(X) = R^+$, and $H^i(X, \mathcal{O}_X^+)$ is almost zero for $i > 0$.
- $\mathcal{O}_X(X) = R$, and $H^i(X, \mathcal{O}_X) = 0$ all $i > 0$.

⌟

Proof: As in the proof of(17.8.6.16), it suffices to prove $\mathcal{O}_X^0$ is almost exact w.r.t any covering $\mathfrak{U}$. For this, notice each term is ϖ-adically complete and flat by(17.8.5.5), so it suffices to prove it is almost exact modulo ϖ(5.7.3.2). Then by the tilting equivalence, it suffices to prove for $X^\flat$. So we may assume at first that K is of char$p$. Then we may replace K by $L = \widehat{\mathbb{F}_p[[t]]_{\mathrm{perf}}}[t^{-1}]$.

But then Noetherian approximation(17.8.6.18) shows that the rational subrings are completion of filtered colimits of p-finite K-algebras((17.8.2.26) used), and then we reduced to the p-finite case, as in the proof of(17.8.6.16). □

7 Étale Sites of Perfectoid Spaces

Def. (17.8.7.1) [Finite Étale Maps of Adic Spaces]. A map of Huber pairs $(A, A^+) \to (B, B^+)$ is called **finite étale** if $A \to B$ is finite étale, and B^+ is the integral closure of A^+ in B.

A map $f : X \to Y$ of adic spaces is called a **finite étalemorphism of adic spaces** if there is a cover of Y by affinoids $V \subset Y$ that $U = f^{-1}(V)$ are all affinoids, and the map $(\mathcal{O}_Y(V), \mathcal{O}_Y^+(V)) \to (\mathcal{O}_X(U), \mathcal{O}_X^+(U))$ is finite étale. Write $Y_{\text{fét}}$ for the category of all such maps. ⌟

Def. (17.8.7.2) [Étale Maps]. A map $X = \mathrm{Spa}(A, A^+) \to Y = \mathrm{Spa}(B, B^+)$ of adic spaces is called **étale** iff for any $x \in X$, there exists an open $x \in U$ and open $f(U) \subset V$ together with an adic space W that $f : U \to V$ factors through an open immersion $U \to W$ and a finite étale map $W \to V$.

Cf.[S-W20]P65. ⌟

Def. (17.8.7.3) [Strongly Finite Étale]. For convenience, in case of perfectoid affinoid K-algebras, we call a map of Huber pairs $(A, A^+) \to (B, B^+)$ **strongly finite étale** if it is finite étale and B^{+a} is almost finite étale over A^{+a}.

A map $f : X \to Y$ of adic spaces is called **strongly finite étale** if there is a cover of Y by affinoids $V \subset Y$ that $U = f^{-1}(V)$ are all affinoids, and the map $(\mathcal{O}_Y(V), \mathcal{O}_Y^+(V)) \to (\mathcal{O}_X(U), \mathcal{O}_X^+(U))$ is strongly finite étale. Write $Y_{s\,\text{fét}}$ for the category of all such maps.

Finally we will prove that if (A, A^+) is perfectoid, then any finite étale map $(A, A^+) \to (B, B^+)$ is strongly finite étale. ⌟

Prop. (17.8.7.4) [Strongly Finite Étale Maps Form a Stack]. If $f : X \to Y$ is a strongly finite étale map that $Y = \mathrm{Spa}(A, A^+)$ is an affinoid perfectoid, then X is also affinoid perfectoid, and the structure map $(\mathcal{O}_X(X), \mathcal{O}_X^+(X)) \to (\mathcal{O}_Y(Y), \mathcal{O}_Y^+(Y))$ is strongly finite étale. ⌟

Proof: By(17.8.7.9), it suffices to prove in char$p$. Then we can replace K by $L = \widehat{\mathbb{F}_p[[t]]_{\mathrm{perf}}}[t^{-1}]$. Then by Noetherian approximation(17.8.6.18), we can assume that Y is a limit of p-finite affinoids $\mathrm{Spa}(B_i, B_i^+)$. As both rational subsets and finite étale algebras pass through filtered colimit, and adic spectrum is quasi-compact(17.8.2.23), we can assume that a finite étale cover of Y arises through base change of some $\mathrm{Spa}(B_i, B_i^+)$. So it suffices to prove the proposition in case of Y p-finite. Then Y is a completion of perfection of some algebraically admissible ring over $\mathbb{F}_p[t]$. Then by the above argument again, we can assume that Y is algebraically admissible.

Now a classical theorem(Cf.[Étale cohomology of rigid analytic varieties and adic spaces, Huber 1.6.6(2)]) shows that the finite étale cover of Y is global finite étale $\mathrm{Spa}(S,S^+)\to\mathrm{Spa}(R,R^+)$ in this case. Notice the strongness is not needed because we are working in char p, where almost purity theorem is already proven. □

Cor. (17.8.7.5). For an affinoid perfectoid space $Y=\mathrm{Spa}(R,R^+)$, the functor $X\mapsto\mathcal{O}_X^+(X)$ defined an equivalence of categories $Y_{s\,\text{fét}}\cong R^{+a}_{a\,\text{fét}}$, and the functor $X\mapsto\mathcal{O}_X(X)$ gives a fully faithful functor $Y_{s\,\text{fét}}\to R_{\text{fét}}$. ⌟

Def. (17.8.7.6) [Étale Sites of Perfectoid Spaces]. Let X be a perfectoid space, then the étale site of X is the category $X_{\text{ét}}$ of perfectoid spaces that is étale over X, and coverings are given by topological coverings. We also consider the following subcategories:

- $X_{\text{ét}}^{aff}$, the category of affinoid perfectoid spaces étale over X.
- $X_{\text{ét},qcqs}$, the full subcategory of qcqs perfectoid spaces étale over X.
- $X_{\text{ét},qc,sep}$, the full subcategory of qc separated perfectoid spaces étale over X.

⌟

Prop. (17.8.7.7) [Gabber-Ramero]. If A is a finite K^0-algebra that is ϖ-adically Henselian, then

$$A[\varpi^{-1}]_{\text{fét}}\cong\widehat{A}[\varpi^{-1}]_{\text{fét}}.$$

⌟

Proof: Cf.[Almost Ring Theory P5.4.53]. □

Cor. (17.8.7.8) [Finite Étale Covers and Direct Limits of Complete Uniform Rings]. Let (A_i,A_i^+) be a filtered system of complete uniform affinoid K-algebras, and (A,A^+) be their colimit in the category of complete uniform affinoid Tate rings, then

$$2-\mathrm{colim}_i\,A_{i,\text{fét}}\cong A_{\text{fét}}$$

as categories. ⌟

Proof: By(17.8.2.26), A^+ is the ϖ-adic completion of the algebraic colimit B^+ of A_i^+, and $A=A^+[\varpi^{-1}]$. Each A_i is complete and ϖ-torsion-free, thus the colimit is Henselian and ϖ-torsion-free(5.3.10.3)(5.3.10.6). Then the proposition(17.8.7.7) shows that $B^+[\varpi^{-1}]_{\text{fét}}\cong A_{\text{fét}}$. Now it remains to show that

$$2-\mathrm{colim}_i\,A_{i,\text{fét}}\cong B^+[\frac{1}{\varpi}]_{\text{fét}},$$

which is because étale sites commutes with taking filtered colimits □

Final Proof of Almost Purity Theorem

Prop. (17.8.7.9). There is an equivalence of categories $X_{s\,\text{fét}}\cong X^\flat_{s\,\text{fét}}$. ⌟

Proof: For this, use(17.8.7.5),(17.8.5.10) and the proven part of(11.2.10.1) and notice that

$$A^{+a}_{a\,\text{fét}}=A^{0a}_{a\,\text{fét}}\cong A^{\flat 0a}_{a\,\text{fét}}=A^{\flat+a}_{a\,\text{fét}},$$

and the integral closure clearly corresponds.(It get around the problem that $R^{0a}_{\text{fét}}\to R_{\text{fét}}$ hasn't been proven essentially surjective). □

Prop. (17.8.7.10)[Proof of Almost Purity Theorem]. Fix a perfectoid affinoid K-algebra (R, R^+), if $S \in R_{\text{fét}}$, then the integral closure of S^+ in R^+ lies in $R^{+a}_{a\,\text{fét}}$, and this gives an inverse to the morphism d in(11.2.10.1), thus finishing the proof of almost purity theorem. ⌟

Proof: Continuing the proof of(11.2.10.1), it suffices to show that $d : R^{+a}_{a\,\text{fét}} \to R_{\text{fét}}$ is essentially surjective, because $S^+ \to \overline{S} \subset R^+$ is the only possible inverse, by the almost purity theorem in char$p$ and tracing the tilting equivalence(11.2.9.6). Given(17.8.7.5), it suffices to prove that for $X = \mathrm{Spa}(R, R^+)$, the prestacks $X_{s\,\text{fét}} \cong X_{\text{fét}}$, where $X_{s\,\text{fét}}(U) = \mathcal{O}_X^{+a}(U)_{s\,\text{fét}}$, and $X_{\text{fét}}(U) = \mathcal{O}_X(U)_{\text{fét}}$.

We use(6.1.3.22), firstly $X_{s\,\text{fét}}$ is a stack, by(17.8.7.4), and for each U, $X_{s\,\text{fét}}(U) \to X_{\text{fét}}(U)$ is fully faithful by almost purity theorem(11.2.10.1). $X_{\text{fét}}$ is separated by(17.8.4.21), because the structure section of an element $S \in X_{\text{fét}}$ is determined its value on the stalk.

Its left to prove that their stalks are equal, for this, use the formula

$$\mathrm{colim}_{x\in U}(\mathcal{O}_X(U), \mathcal{O}_X^+(U)) = (\widehat{k(x)}, \widehat{k^+(x)})$$

in the category of complete uniform affinoid K-algebras(they are all perfectoids(17.8.5.5) thus uniform), by definition. So we get by(17.8.7.8):

$$\mathrm{colim}_{x\in U}\,\mathcal{O}_X(U)_{\text{fét}} \cong \widehat{k(x)}_{\text{fét}},$$

and by(17.8.7.8) together with the proven part of almost purity theorem(11.2.10.1):

$$\mathrm{colim}_{x\in U}\,\mathcal{O}_X^+(U)_{a\,\text{fét}} \cong \mathrm{colim}_{x^\flat\in U^\flat}\,\mathcal{O}_X^{\flat+}(U^\flat)_{a\,\text{fét}} \cong \kappa^+(x^\flat)_{a\,\text{fét}} \cong \kappa^+(x)_{a\,\text{fét}}.$$

Now we have already proved the almost purity over fields(11.2.10.1) which says $\kappa(x^\flat)_{a\,\text{fét}} \cong \kappa^+(x)_{a\,\text{fét}}$, so their stalks are the same. □

Cor. (17.8.7.11) [Invariance of Étale Site under Tilting]. There is a natural isomorphism of categories $X_{\text{ét}} \cong X^\flat_{\text{ét}}$, by almost purity theorem(11.2.10.1) and the localness of étale maps. ⌟

Prop. (17.8.7.12) [Almost Acyclicity]. For any $X \in \mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$, the functor $U \mapsto \mathcal{O}_X(U)$ is a sheaf on $X_{\text{ét}}$, and $H^i(X_{\text{ét}}, \mathcal{O}_X^+)$ is almost zero if X is affinoid perfectoid. ⌟

Proof: □

17.9 Pro-Étale Sites on $\mathcal{P}\mathrm{erfd}$ and Diamonds

References are [Sch17] and [Notes on Diamonds, David Hansen].

1 Properties of Perfectoid Spaces

Totally Disconnected Spaces

Def. (17.9.1.1) [Totally Disconnected Spaces]. $X \in \mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$ is called **totally disconnected** if it is qcqs and any open covering $\{U_i \to X\}$ splits, i.e. $\coprod U_i \to X$ splits, or equivalently, there is a refinement covering $\{V_i \to X\}$ that $X \cong \coprod V_i$.

A perfectoid space X is called **strictly totally disconnected** if it is qcqs and every étale cover splits. ⌟

Prop. (17.9.1.2). Let X be a qcqs perfectoid spaces, then X is totally disconnected iff all its connected components are of the form $\mathrm{Spa}(K, K^+)$ where (K, K^+) are perfectoid affinoid fields. And it is strictly totally disconnected if moreover K are all alg.closed. ⌟

Proof: Cf.[Sch17].P29, P35. □

Prop. (17.9.1.3). if X is a totally disconnected perfectoid space, then X is affinoid. ⌟

Proof: Cf.[Sch17].P30. □

Injections

Def. (17.9.1.4) [Injections]. $f : X \to Y \in \mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$ is called an injection if for any perfectoid space Z, $f_* : \mathrm{Hom}(Z, X) \to \mathrm{Hom}(Z, Y)$ is an injection. ⌟

Prop. (17.9.1.5) [Residue Field Map is Injection]. Let X be a perfectoid space and $x \in X$, giving rise to a map of residue fields

$$i_x : \mathrm{Spa}(\kappa(x), \kappa(x)^+) \to X,$$

then i_x is an injection of perfectoid spaces. ⌟

Proof: To show this, firstly we can replace X with an affinoid nbhd of X. Then notice that $\mathrm{Spa}(\kappa(x), \kappa(x)^+)$ is the filtered limit over all rational nbhds U of x in X, and for each U, $U \to X$ is an injection by definition(17.8.3.1), so i_x is also an injection. □

Cor. (17.9.1.6). In particular, if X is qcqs and has a unique closed point $x \in X$, then $X = \mathrm{Spa}(\kappa(x), \kappa(x)^+)$, as in this case X is the only quasi-compact open subset containing x. ⌟

Prop. (17.9.1.7) [Characterizations of Injections]. For $f : X \to Y \in \mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$, the following are equivalent:

- f is an injection.
- For any perfectoid adic field (K, K^+), the map of sets $f_* : Y(K, K^+) \to X(K, K^+)$ is an injection.
- The map $|f| : |Y| \to |X|$ is injective, and for all rank 1 point $y \in Y$ with image $f(y) = x \in X$, the map of completed residue fields $\kappa(x) \to \kappa(y)$ is an isomorphism.
- The map $|f| : |Y| \to |X|$ is injective, and f is final in the category of maps $Z \to X$ that $|Z| \to |X|$ factors through the map $|Y| \to |X|$.

In particular, by item4, an injection of perfectoid spaces is determined by its topological map. ⌟

Proof: Cf.[Sch17]P21. $4 \to 1 \to 2$ is trivial. □

Prop. (17.9.1.8) [Injection and Base Change].

- Let $f : Y \to X$ be an injection of perfectoid spaces, and $X' \to X$ any map of perfectoid spaces, then the pullback $f' : Y' = Y \times_X X' \to X'$ is also an injection, and the induced map
$$|Y'| \to |Y| \times_{|X|} |X'|$$
is a homeomorphism.
- A map of perfectoids spaces is an injection iff it is universally injective.

⌟

Proof: Cf.[Sch17]P24. □

Immersions

Def. (17.9.1.9) [Immersions]. $f : Y \to X \in \mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$ is called an immersion if f is an injection and $|f| : |Y| \to |X|$ is a locally closed immersion. If $|f|$ is moreover closed or open, then it is called closed/open immersion. ⌟

Def. (17.9.1.10) [Zariski-Closed Immersions]. Let $f : Z \to X = \mathrm{Spa}(R, R^+) \in \mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$, then

- f is called a Zariski-closed immersion if f is a closed immersion and $|Z| = V(I) \subset |X|$, where $I \subset R$ is an ideal.
- f is called a strongly Zariski-closed immersion if $Z = \mathrm{Spa}(S, S^+)$ is affinoid perfectoid, $R \to S$ is surjective, and S^+ is the closure of R^+ in S.

⌟

Prop. (17.9.1.11).

- If f is strongly Zariski closed, then f is Zariski closed, in particular a closed immersion.
- If f is Zariski closed, then Z is affinoid.
- If X is of characteristic p, and f is Zariski closed, then f is strongly Zariski closed.

⌟

Proof: Cf.[Sch17] Section2.5. □

Prop. (17.9.1.12). For any map of perfectoid spaces $Y \to X$, the diagonal map $\Delta_f : Y \to Y \times_X Y$ is an immersion. ⌟

Proof: Clearly Δ_f is an injection, thus it suffices to show that $|\Delta_f|$ identifies Y with a locally closed subset of $|Y \times_X Y|$. This can be checked locally on the target, so we can assume $X = \mathrm{Spa}(R, R^+)$ and $Y = \mathrm{Spa}(S, S^+)$, then the diagonal map is strongly Zariski closed, as $S\widehat{\otimes}_R S \to S$ is surjective and maps the integral closure of $S^+\widehat{\otimes}_{R^+} S^+ \to S^+$ onto S^+. Thus by(17.9.1.11), Δ_f is a closed immersion in this case. □

Def. (17.9.1.13) [Separated Map]. $f : Y \to X \in \mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$ is called separated if Δ_f is a closed immersion. ⌟

Prop. (17.9.1.14) [Valuation Criterion]. For $f : Y \to X \in \mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$, the following are equivalent:

- f is separated.
- $|\Delta_f| : |Y| \to |Y \times_X Y|$ is a closed immersion.
- $|f|$ is quasi-separated, and for any perfectoid adic field (K, K^+) and any diagram

$$\begin{array}{ccc} \mathrm{Spa}(K, \mathcal{O}_K) & \longrightarrow & Y \\ \downarrow & \nearrow & \downarrow f \\ \mathrm{Spa}(K, K^+) & \longrightarrow & X \end{array},$$

there exists at most one dotted arrow making the diagram commutative.

⌟

Proof: The equivalence of 1 and 2 is by(17.9.1.12).

2 $\to$ 3: If $|\Delta_f|$ is a closed immersion, then it is in particular quasi-compact, thus f is quasi-separated. Now if there are two dotted-arrow making this diagram commutative, they define a point $z \in (Y \times_X Y)(K, K^+)$ s.t. $z|_{\mathrm{Spa}(K,\mathcal{O}_K)} \in \Delta_f(Y)(K, \mathcal{O}_K)$. But $|\Delta_f|(|Y|)$ is closed in $|Y \times_X Y|$, so z maps $\mathrm{Spa}(K, K^+)$ into $|\Delta_f|(|Y|)$ iff it maps $\mathrm{Spa}(K, \mathcal{O}_K)$ into $|\Delta_f|(|Y|)$, as $\mathrm{Spa}(K, \mathcal{O}_K) \subset \mathrm{Spa}(K, K^+)$ is dense**??**. Now Δ_f is an injection, so by(17.9.1.7), z factors through Δ_f thus the two maps are equal.

3 $\to$ 2: The condition implies that $|\Delta_f| : |Y| \to |Y \times_X Y|$ is a quasi-compact locally closed immersion of locally spectral spaces which is moreover specializing. But because $|\Delta_f|$ is quasi-compact, the image of $|\Delta_f|$ is pro-constructible, and it is also closed under specialization, thus it is closed, Cf.[Sch17]P25. □

2 Pro-Étale Site and v-Site

Prop. (17.9.2.1). if (R, R^+) is the completed filtered colimit of perfectoid Huber pairs (R_i, R_i^+), $X_i = \mathrm{Spa}(R_i, R_i^+)$, $X = \mathrm{Spa}(R, R^+)$, then base change induce equivalences of categories:

- $2 - \lim_i X_{i,\text{fét}} \cong X_{\text{fét}}$.
- $2 - \lim_i X_{i,\text{ét}}^{\text{aff}} \cong X_{\text{ét}}^{\text{aff}}$.
- $2 - \lim_i X_{i,\text{ét},qcqs} \cong X_{\text{ét},qcqs}$.
- $2 - \lim_i X_{i,\text{ét},qc,sep} \cong X_{\text{ét},qc,sep}$.

⌟

Proof: Cf.[Sch17]P27.

1 follows from almost purity theorem. □

Def. (17.9.2.2)[Pro-étale Morphism]. A map of perfectoid Huber pairs $(A, A^+) \to (B, B^+)$ is called **pro-étale** iff it is the completed filtered colimit of étale ring maps $(A, A^+) \to (A_i, A_i^+)$.

A morphism of perfectoid spaces is **pro-étale** if there is an affinoid covering $V_i = \mathrm{Spa}(R_i, R_i^+)$ of X that $f^{-1}(V_i)$ have coverings $U_{ij} = \mathrm{Spa}(R_{ij}, R_{ij}^+)$ that $(R_i, R_i^+) \to (R_{ij}, R_{ij}^+)$ are all pro-étale.

In fact, by(17.9.2.7), if this is true for one affinoid covering V_i of X, then this is true for any affinoid covering of X. ⌟

Prop. (17.9.2.3). If S is a profinite set and X is a perfectoid space, then we can define a new perfectoid space $X \times \underline{S}$ as the inverse limit of $X \times \underline{S_i}$, where $S = \varprojlim S_i$. Then $X \times \underline{S}$ is pro-étale over X. ⌟

Prop. (17.9.2.4) [Immersion are Pro-Étale]. If $f : Z \hookrightarrow X$ be a Zariski closed immersion with image $V(I)$, then f is affinoid pro-étale. Then $f(Z)$ can be written as the intersection of rational subsets

$$U_{f_1,\ldots,f_n} = \{|f_1|, \ldots, |f_n| \le |\varpi|\}$$

for various n and $f_1, \ldots, f_n \in I$. Then $Z = \varprojlim U_{f_1,\ldots,f_n} \to X$, as it is a closed immersion thus an injection(17.9.1.11), which shows $Z \to X$ is pro-étale.

In particular, an immersion is also pro-étale because pro-étale can be checked analytically locally. ⌟

Cor. (17.9.2.5) [Diagonal Map is Pro-Étale]. If $f : Y \to X$ is a map of perfectoid spaces, then $\Delta_f : Y \to Y \times_X Y$ is pro-étale, by(17.9.1.12). ⌟

Prop. (17.9.2.6). If X is an affinoid perfectoid space, then the functor

$$\mathrm{Pro}(X^{\mathrm{aff}}_{\text{ét}}) \to X^{\mathrm{aff}}_{pro\,\text{ét}} : \varprojlim_i (X_i) \mapsto \varprojlim_i X_i$$

is an equivalence of categories. ⌟

Proof: This map is essentially surjective by definition, To show it is fully faithful, it suffices to show that for $Y = \varprojlim_i \mathrm{Spa}(Y_i, Y_i^+), Z = \varprojlim_j \mathrm{Spa}(Z_j, Z_j^+)$,

$$\mathrm{Hom}_X(Y, Z) = \varprojlim_j \varinjlim_i \mathrm{Hom}(Y_i, Z_j).$$

We need to show for any $Z \to X$,

$$\mathrm{Hom}_X(Y, Z) = \varinjlim_i \mathrm{Hom}(Y_i, Z).$$

Because $2 - \lim_i X_{i,\text{ét},qcqs} \cong X_{\text{ét},qcqs}$(17.9.2.1), we have

$$\mathrm{Hom}_X(Y, Z) = \mathrm{Hom}_Y(Y, Y \times_X Z) = \varinjlim_i \mathrm{Hom}_{Y_i}(Y_i, Y_i \times_X Z) = \varinjlim_i \mathrm{Hom}_X(Y_i, Z).$$

□

Prop. (17.9.2.7) [Properties of Pro-Étale Morphisms].

- (Affinoid)Pro-Étale maps are stable under composition and pullbacks.
- Let $f : Y \to X, f' : Y' \to X$ be (affinoid)pro-étale, then any map $g : Y \to Y'$ over X is also (affinoid)pro-étale.
- For any affinoid perfectoid space X, the category $X^{\mathrm{aff}}_{pro-\text{ét}}$ has all finite limits.

⌟

Proof: 1: Composition is obvious. pro-étale maps are stable under pullbacks because étale maps do.

2: We can factor g as a section of the map $Y \times_X Y' \to Y$ and the projection map $Y \times_X Y' \to Y'$. Thus it suffices to show a section of a pro-étale map is pro-étale. But if $Y = \varprojlim_i Y_i \to X$ is pro-étale, then a section is given by compatible sections $s_i : X \to Y_i$. Then $X = \varprojlim_i (X \times_{Y_i} Y) \to X$ is pro-étale.

3: This is because $X^{\mathrm{aff}}_{\text{ét}}$ has finite limits, because it has a final object and fiber products(11.2.9.17). □

Def. (17.9.2.8) [Big Pro-Étale Sites]. Consider the following categories:

- $\mathcal{P}$erfd$\mathcal{S}$pa, the category of perfectoid spaces.
- $\mathcal{P}$erf, the category of perfectoid spaces of characteristic p.
- $X_{pro\,\text{ét}}$, the category of perfectoid spaces pro-étale over X, where X is a perfectoid space.
- $X^{\text{aff}}_{pro\,\text{ét}}$, the category of affinoid perfectoid spaces pro-étale over X.

The **big pro-étale site** is the category Perfd endowed with the topology that a family of maps $\{f_i : Y_i \to X\}$ is a covering if all f_i are pro-étale and for any quasi-compact open subset $U \subset X$, there is a finite set $J \subset I$ and quasi-compact opens $V_j \subset Y_j$ that $U = \cup_{j\in J} f_j(V_j)$.

These truly form sites by(17.9.2.7). ⌟

Cor. (17.9.2.9). The presheaf $\mathcal{O} : X \mapsto \mathcal{O}_X(X), \mathcal{O}^+ : X \mapsto \mathcal{O}^+_X(X)$ on the big étale site are sheaves. If X is affinoid perfectoid, then $H^i(X_{pro\,\text{ét}}, \mathcal{O}) = 0$ for $i > 0$, and $H^i(X_{pro\,\text{ét}}, \mathcal{O}^+)$ is almost zero for $i > 0$. Moreover, the big pro-étale site is subcanonical. ⌟

Proof: Firstly we can assume X is affinoid because we already know $\mathcal{O}, \mathcal{O}^+$ are sheaves w.r.t. the analytic topology. Let $Y \to X$ be an affinoid pro-étale covering of X, where $Y = \text{Spa}(R_\infty, R^+_\infty)$, $(R_\infty, R^+_\infty) = (\varinjlim_i (R_i, R^+_i))^\wedge$. Then fixing a pseudo-uniformizer ϖ of R, the complexes

$$0 \to R^+/\varpi \to R^+_j/\varpi \to \cdots$$

is almost exact, because $H^i(X_{\text{ét}}, \mathcal{O}^+_X/\varpi)$ is almost zero for $i > 0$. Now take a direct limit over i, then

$$0 \to R^+/\varpi \to R^+_\infty/\varpi \to \cdots$$

is almost exact. Now by induction on n, we can prove

$$0 \to R^+/\varpi^n \to R^+_\infty/\varpi^n \to \cdots$$

is almost exact. Then by passing to the direct limit ,

$$0 \to R^+ \to R^\infty_\infty \to \cdots$$

is almost exact. Then by inverting ϖ,

$$0 \to R \to R_\infty \to \cdots$$

is exact. These give us the desired results. Notice $\mathcal{O}^+$ is a sheaf because it is the elements of valuations≤ 1 everywhere by(17.8.3.7).

For the final assertion, if $\{Y_i \to Y\}$ is a pro-étale covering of Y, and $g_i : Y_i \to X$ are maps that agree on $Y_i \times_X Y_j$, then firstly we can glue these maps together topologically to a map $|Y| \to |X|$. So this problem can be considered locally on X, so we may assume $X = \text{Spa}(R, R^+)$ is affinoid, and maps $(R, R^+) \to (\mathcal{O}(Y_i), \mathcal{O}^+(Y_i))$ that agree on the overlap(17.8.4.4), then they glue to a map $(R, R^+) \to (\mathcal{O}(Y), \mathcal{O}^+(Y))$, as $\mathcal{O}, \mathcal{O}^+$ are all sheaves, and this gives a morphism $Y \to X$. □

Prop. (17.9.2.10) [Strictly Totally Disconnected Pro-Étale Cover]. Let X be an affinoid perfectoid space, then there is an affinoid perfectoid space $\widetilde{X}$ with an affinoid pro-étale surjective and universally open map $\widetilde{X} \to X$ that $\widetilde{X}$ is strictly totally disconnected. ⌟

Proof: Cf.[Sch17]P35. □

Prop. (17.9.2.11). The presheaf $\mathcal{O}, \mathcal{O}^+$ are sheaves w.r.t. the v-topology. Moreover, the v-site is subcanonical. ⌟

Proof: Cf.[Sch17]P40. □

Prop. (17.9.2.12). Let X be an affinoid perfectoid space, then $H^i_v(X, \mathcal{O}) = 0$ for $i > 0$, and $H^i_v(X, \mathcal{O}^+)$ is almost zero for $i > 0$. ⌟

Proof: Cf.[Sch17]P41. □

Descent on Pro-Étale Site

Prop. (17.9.2.13) [Descent May Fail]. The question is whether the fibered category over Perfd:

$$X \mapsto \{\text{Perfectoid Spaces } Y \to X\}$$

is a stack for the pro-étale toplogy. This fails in general. An evidence is that the fibered category

$$X \mapsto \{\text{Affinoid Perfectoid Spaces } Y \to X\}$$

is not a stack on the category of affinoid Perfectoid spaces with the analytic topology, let along the pro-étale topology:

Let $X = \operatorname{Spa} K\langle x, y\rangle$, and $V \subset X$ be $\{(x, y) \mid |x| = 1 \text{ or } |y| = 1\}$, then V is covered by two affinoids, but is not an affinoid itself: $H^1(V, \mathcal{O}_V) = \widehat{\bigoplus}_{m,n>0} K x^{-m} y^{-n} \neq 0$. But there is a standard rational covering $X = \cup_i X(\frac{f_1, f_2, f_3}{f_i})$, where $f_1 = \varpi$, $f_2 = x$, $f_3 = y$, and

$$U_0 \cap V = \varnothing, \quad U_1 \cap V = \{|x| = 1\} \subset U_1, \quad U_2 \cap V = \{|y| = 1\} \subset U_2$$

are all affinoid. There is a similar example in the perfectoid case, thus

$$X \mapsto \{\text{Affinoid Perfectoid Spaces } Y \to X\}$$

is not a stack. ⌟

Prop. (17.9.2.14) [Pro-étale is not Pro-étale Local]. There is an example of a non-pro-étale map that is pro-étale locally pro-étale. ⌟

Proof: Cf.[S-W20]P66. □

Prop. (17.9.2.15) [Characterization of Locally pro-étale Maps]. For $f : X \to Y \in \mathcal{A}\text{ff}\,\mathcal{P}\text{erfd}\mathcal{S}\text{pa}$, the following are equivalent:

- There exists an affinoid pro-étale cover $Y' \to Y$ s.t. the base change $X' = X \times_Y Y' \to Y'$ is pro-étale.
- For all geometric points $\operatorname{Spa} C \to Y$, $X \times_Y \operatorname{Spa} C = \operatorname{Spa} C \times \underline{S}$ for some profinite set S.

⌟

Proof: Cf.[S-W20]P66. □

Prop. (17.9.2.16) [Descent]. Descent data of the the fibered category

$$X \mapsto \{\text{Perfectoid Spaces } Y \to X\}$$

of a perfectoid space $Y' \to X'$ along a pro-étale cover $X' \to X$ is effective in the following cases:

- If X, X', Y' are affinoids and X is totally disconnected.
- if f is separated and pro-étale and X is strictly totally disconnected.
- If f is separated and étale. In particular, the fibered category

$$X \mapsto \{\text{separated étale } X \to Y\}$$

is a stack over the category of perfectoid spaces with the pro-étale topology.
- If f is finite étale. In particular, the fibered category

$$X \mapsto \{\text{finite étale } X \to Y\}$$

is a stack over the category of perfectoid spaces with the pro-étale topology.

⌟

Proof: Cf.[Sch17]P9.3, 9.6, 9.7. □

3 Morphisms of v-Stacks

Def. (17.9.3.1)[Étale Morphisms of Stacks]. Let $f: Y' \to Y$ be a map of pro-étale stacks on $\mathcal{P}$erfd,

- Assume f is locally separated(i.e. there is an open cover of Y' over which f becomes separated), then f is called **quasi-pro-étale** if for any strictly totally disconnected perfectoid space X and a map $X \to Y$, the pullback $Y' \times_Y X$ is representable and $Y' \times_Y X \to X$ is pro-étale.
- Assume f is locally separated, then f is called **étale** if for any perfectoid space X and a map $X \to Y$, the pullback $Y' \times_Y X$ is representable and $Y' \times_Y X \to X$ is étale.
- f is called **finite étale** if for any perfectoid space X and a map $X \to Y$, the pullback $Y' \times_Y X$ is representable and $Y' \times_Y X \to X$ is finite étale.

⌟

4 Diamonds

Remark (17.9.4.1) [Motivation of Diamonds]. The idea of diamonds is that there should be a functor

$$\diamond : \{\text{analytic adic spaces over } \mathbb{Z}_p\} \to \{\text{diamonds}\}$$

that forgets the structure morphism to $\mathbb{Z}_p$. For a perfectoid space X, $X \mapsto X^f lat$ has this property, so this functor should coincides on these objects. Now any analytic adic space X over $\mathbb{Z}_p$ is pro-étale locally perfectoid:

$$X = \mathrm{Coeq}(\widetilde{X} \times_X \widetilde{X} \rightrightarrows X),$$

where $\widetilde{X} \to X$ is a pro-étale perfectoid cover. The equivalence relations $R = \widetilde{X} \times_X \widetilde{X}$ is also perfectoid, so this functor should send X to $\mathrm{Coeq}(R^\flat \rightrightarrows \widetilde{X}^\flat)$.

For example, if $X = \mathrm{Spa}(\mathbb{Q}_p)$, then a pro-étale cover of X is $\mathrm{Spa}((\mathbb{Q}_p^{\mathrm{cycl}})^\wedge)$, and then $R = \widetilde{X} \times_X \widetilde{X} = \widetilde{X} \times \underline{\mathbb{Z}_p^*}$ by Galois theory, and then $\mathbb{Q}_p^\diamond$ should be defined as the coequalizer of $\mathrm{Spa}((\mathbb{Q}_p^{\mathrm{cycl}})^\flat)/\underline{\mathbb{Z}_p^*}$, whose meaning is explained in(17.9.4.11). ⌟

Def. (17.9.4.2) [Diamonds]. A **diamond** is a pro-étale sheaf $\mathcal{D}$ on $\mathcal{P}$erfd that can be written as $\mathcal{D} = X/R$, where

- $X \in \mathcal{P}$erfd,

- R is a pro-étale equivalence relation in $X \times X$(i.e. an equivalence relation that the maps $s, t : R \to X$ are pro-étale),
- R is representable.

⌟

Prop. (17.9.4.3). Let $X \in \mathcal{P}\mathrm{erfd}$ and $R \subset X \times X$ a representable pro-étale equivalence relation, then

- The quotient sheaf $Y = X/R$ is a diamond.
- The natural map of sheaves $R \to X \times_Y X$ is an isomorphism.
- Let $\widetilde{X} \to X$ be a pro-étale cover by a perfectoid space $\widetilde{X}$, and $\widetilde{R} = R \times_{X \times X} (\widetilde{X} \times \widetilde{X})$ the induced equivalence relation, then $\widetilde{R}$ is a representable pro-étale equivalence relation of $\widetilde{X}$, and the natural map $\widetilde{Y} = \widetilde{X}/\widetilde{R} \to Y = X/R$ is an isomorphism.
- The map $X \to Y$ is quasi-pro-étale(17.9.3.1).

⌟

Proof: 1 is by definition.

For 2, firstly $R \to X \times_Y X$ is injective as subsheaves of $X \times X$. Next, if $Z \to X \times_Y X$ is any map from a perfectoid space Z, then we have two maps $a, b : Z \to X$ that their composition with $X \to Y$ agree. This means after passing to a pro-étale covering $\widetilde{Z} \to Z$, the composition map $\widetilde{Z} \to Z \to X \times X$ factors through R. Now this map $\widetilde{Z} \to R$ descends to a map $Z \to R$, because pro-étale site is subcanonical and the two projection maps $\widetilde{Z} \times_Z \widetilde{Z} \to R$ coincides because they do after compositing with $R \hookrightarrow X \times X$.

3: Firstly $\widetilde{R}$ is representable as fiber products of representable objects(17.8.5.4), and the two projections are pro-étale, as they are compositions of base changes of pro-étale morphisms. Also the mop $\widetilde{Y} \to Y$ of pro-étale sheaves is surjective, as the composition $\widetilde{X} \to X \to Y$ is.

To show $\widetilde{Y} \to Y$ is injective, let Z be a perfectoid space with two maps $Z \to \widetilde{Y}$ that coincide after compositing with $\widetilde{Y} \to Y$, we need to show $a = b$. Now because pro-étale site is subcanonical, it suffices to show this after replacing Z with a pro-étale cover $\widetilde{Z}$, such that a, b factors over $\widetilde{a}, \widetilde{b} : Z \to \widetilde{X}$. The associated map $Z \to \widetilde{X} \times \widetilde{X} \to X \times X$ factors through R by item2, so we get a map $Z \to R \times_{X \times X} (\widetilde{X} \times \widetilde{X}) = \widetilde{R}$, which means $\widetilde{a}, \widetilde{b}$ induces the same map $Z \to \widetilde{Y}$. So we are done.

4: By 3, we can replace X by $\widetilde{X} = \coprod_i U_i \to X$, where U_i is an affinoid cover of $\widetilde{X}$, and R by the the induced equivalence relation in $\widetilde{X} \times \widetilde{X}$, and to pro-étale is analytically local. In this way, we may assume $R \subset X \times X$ and $X \times X \to X$ are separated.

Let X' be a strictly totally disconnected perfectoid space and $X' \to X$ be a map. Because $X \to Y$ is surjective as sheaves on Perf, there is a pro-étale cover $\widetilde{X'} \to X'$ and a map $\widetilde{X'} \to X$ lying over $X' \to Y$. We can assume $\widetilde{X'}$ is affinoid. Let $W = X' \times_Y X \to X'$ be the fiber product, then

$$\widetilde{X'} \times_{X'} W = \widetilde{X'} \times_X (X \times_Y X) = \widetilde{X'} \times_X R$$

is representable and pro-étale over $\widetilde{X'}$, and also separated. So by(17.9.2.16), W is also representable, pro-étale and separated over X. □

Cor. (17.9.4.4) [Equivalent Characterization of Diamonds]. Let Y be a pro-étale sheaf on Perf, then Y is a diamond iff there is a surjective quasi-pro-étale morphism $X \to Y$ from a perfectoid space X. If X is a disjoint union of strictly totally disconnected spaces, then $R \subset X \times_Y X \subset X \times X$ is a representable pro-étale equivalence relation with $Y = X/R$. ⌟

Proof: If Y is a diamond, then $X \to Y$ is quasi-pro-étale by(17.9.4.3). Conversely, if there is a quasi-pro-étale morphism $X \to Y$, by(17.9.2.10), we can assume that X is a disjoint union of strictly disconnected spaces. In this case, by the definition of auasi-pro-étale, R is representable and the projections $R = X \times_Y X \to X$ is pro-étale, and $X/R \cong Y$: it suffices to show this map is injective: if $a, b : Z \to X$ are two maps that coincide after composing with $X \to Y$, then after replacing to a pro-étale covering $\widetilde{Z} \to Z$, we can lift to maps $(\widetilde{a}, \widetilde{b}) : \widetilde{Z} \to R$. And this map descend to a map $Z \to R$, because the pullback to $\widetilde{Z} \times_Z \widetilde{Z} \to R$ coincides as they do after composing with $R \hookrightarrow X \times X$. So $X/R \to Y$ is injective. □

Cor. (17.9.4.5).

- Let Y be a pro-étale sheaf on $\mathcal{P}$erfd and there is a quasi-pro-étale map $Y' \to Y$, where Y' is a diamond, then Y is also a diamond.
- Let $f : Y' \to Y$ be a quasi-pro-étale map of pro-étale sheaves on $\mathcal{P}$erfd and Y is a diamond, then Y' is also a diamond.

⌟

Proof: 1: By(17.9.4.4), we can choose a quasi-pro-étale map $X \to Y'$ where X is a perfectoid space, then $X \to Y' \to Y$ is also quasi-pro-étale, so Y is a diamond by(17.9.4.4) again.

2: Choose a surjective quasi-pro-étale map $X \to Y$ where X is a perfectoid space, then $X' \times_X Y$ is representable and $X' \to Y'$ is quasi-pro-étale and surjective, thus Y' is a diamond by(17.9.4.4). □

Lemma (17.9.4.6) [Product of Perfectoid Spaces]. The product of two perfectoid spaces of char p is also a perfectoid space. ⌟

Proof: Cf.[Sch17]P71. □

Prop. (17.9.4.7) [Absolute Product of Diamonds]. Let $\mathcal{D}, \mathcal{D}'$ be diamonds, then the product sheaf $\mathcal{D} \times \mathcal{D}'$ is also a diamond. ⌟

Proof: Let $\mathcal{D} = X/R$ and $\mathcal{D}' = X'/R'$, then $R \times R', X \times X'$ are also representable by(17.9.4.6), $R \times R' \to (X \times X') \times (X \times X')$ is also an injection, and the projections are pro-étale. Thus $\mathcal{D} \times D' = (X \times X')/(R \times R')$ is a diamond, by(17.9.4.3). □

Prop. (17.9.4.8) [Fiber Products]. Fiber products exist in the category of diamonds. ⌟

Proof: Let $Y_1 \to Y_2 \leftarrow Y_3$ be a diagram of diamonds. Choose representations $Y_i = X_i/R_i$, and after replacing X_1, X_2 with a pro-étale covering using(17.9.4.3), we can assume there are maps $X_i \to X_3$ lying over $Y_i \to Y_3$. Moreover, we can replace X_i by $X_i \times_{Y_3} X_3$ to assume that $X_i \to Y_1 \times_{Y_3} X_3$ is surjective in the pro-étale topology.

In this case, the map $X_1 \times_{X_3} X_2 \to Y_1 \times_{Y_3} Y_2$ is surjective in the pro-étale topology, and the equivalence relation $R_4 = X_4 \times_{Y_4} X_4$ can be calculated to be $R_4 = R_1 \times_{R_3} R_2$, which is representable. It remains to see that $R_4 \to X_4$ is pro-étale. But $R_1 \times R_2 \to X_1 \times X_2$ is pro-étale, so does its base change $R_1 \times_{X_3} R_2 \to X_1 \times_{X_3} X_2 = X_4$, and also $R_4 = R_1 \times_{R_3} R_2 \to R_1 \times_{X_3} R_2$ is pro-étale because it is the base change of $R_3 \to R_3 \times_{X_3} R_3$, which is pro-étale by(17.9.2.5). □

Prop. (17.9.4.9). Let Y be a diamond, then Y is a sheaf for the v-topology. ⌟

Proof: Cf.[Sch17]P54. □

Def. (17.9.4.10) [Underlying Spaces of Diamonds]. Any diamond has an underlying space $|\mathcal{D}| = |X|/|R|$. ⌟

Proof: ? □

Spd($\mathbb{Q}_p$)

Prop. (17.9.4.11). Let Spd($\mathbb{Q}_p$) be defined as

$$\mathrm{Spa}((\mathbb{Q}_p^{\mathrm{cycl}})^\flat)/\mathbb{Z}_p^* = \mathrm{Spa}(\mathbb{F}_p((t^{1/p^\infty})))/\mathbb{Z}_p^*,$$

where $\mathbb{Z}_p^*$ acts on $\mathbb{F}_p((t^{1/p^\infty}))$ via $\gamma(t) = (1+t)^\gamma - 1$(11.2.8.17), i.e. it is the coequalizer of

$$\underline{\mathbb{Z}_p}^* \times \mathrm{Spa}(\mathbb{F}_p((t^{1/p^\infty}))) \rightrightarrows \mathrm{Spa}(\mathbb{F}_p((t^{1/p^\infty}))),$$

where one map is projection and the other map is the group action. To show this is diamond, we first need to verify this is an injection thus an equivalence relation, which follows from(17.9.4.12). ⌟

Lemma (17.9.4.12). Consider the map

$$g : \underline{\mathbb{Z}_p}^* \times \mathrm{Spa}(\mathbb{F}_p((t^{1/p^\infty}))) \rightrightarrows \mathrm{Spa}(\mathbb{F}_p((t^{1/p^\infty}))) \times \mathrm{Spa}(\mathbb{F}_p((t^{1/p^\infty})))$$

where the first map is group action and the second map is projection, then this is an injection map. ⌟

Proof: For any adic point (K, K^+), $\mathbb{Z}_p^*$ acts freely on K^{00}, thus the map is an injection, by(17.9.1.7). □

Prop. (17.9.4.13) [Torsor over Affinoid Perfectoid Space]. Let G be a profinite group and $f : \mathcal{F}' \to \mathcal{F}$ be a $\underline{G}$-torsor, with G profinite, then for any affinoid $X = \mathrm{Spa}(B, B^+)$ and any morphism $X \to \mathcal{F}$, the pullback $\mathcal{F}' \times_{\mathcal{F}} X$ is representable by a perfectoid affinoid $X' = \mathrm{Spa}(A, A^+)$, where (A, A^+) is the completed filtered colimit of (A_H, A_H^+), where for each open normal subgroup H of G, A_H/B is a finite étale G/H-torsor. ⌟

Proof: If H is an open normal subgroup of G, then $\mathcal{F}'/\underline{H} \to \mathcal{F}$ is a G/H-torsor, and $\mathcal{F}' = \varprojlim_H \mathcal{F}'/\underline{H}$, thus we reduce to the case G is finite. But for this case, we use the fact {perfectoid spaces finite étale over X} is a stack(17.9.2.16), and the definition of G-torsor. □

Prop. (17.9.4.14) [Description of Spd($\mathbb{Q}_p$)]. If $X = \mathrm{Spa}(R, R^+)$ is an affinoid perfectoid space of characteristic p, then $(\mathrm{Spd}\,\mathbb{Q}_p)(X)$ is the set of isomorphism classes of data of the following shape.

- A $\mathbb{Z}_p^*$-torsor $R \to \widetilde{R}$, i.e. $\widetilde{R} = (\varinjlim_i R_i)^\wedge$, where R_n/R is finite étale with Galois group $(\mathbb{Z}/p^n\mathbb{Z})^*$.
- A topological nilpotent unit $t \in \widetilde{R}$ s.t. for all $\gamma \in \mathbb{Z}_p^*$, $\gamma(t) = (1+t)^\gamma - 1$.

⌟

Proof: Notice $\mathrm{Spa}(\mathbb{Q}_p^{\mathrm{cycl}})^\flat \to \mathrm{Spd}(\mathbb{Q}_p)$ is a $\mathbb{Z}_p^*$-torsor by definition, so for any morphism $X \to \mathrm{Spd}(\mathbb{Q}_p)$, the pullback $\mathrm{Spa}(\mathbb{Q}_p^{\mathrm{cycl}})^\flat \times_{\mathrm{Spd}(\mathbb{Q}_p)} X \to X$ is also a $\mathbb{Z}_p^*$-torsor, so it is isomorphic to a torsor $\mathrm{Spa}(\widetilde{R}, \widetilde{R}^+) \to \mathrm{Spa}(R, R^+)$ by(17.9.4.13), and the map $\mathrm{Spa}(\mathbb{Q}_p^{\mathrm{cycl}})^\flat \times_{\mathrm{Spd}(\mathbb{Q}_p)} X \to X \to \mathrm{Spa}(\mathbb{Q}_p^{\mathrm{cycl}})^\flat$ is an $\mathbb{Z}_p^*$-equivariant map, which is equivalent to a topologically nilpotent element $t \in \widetilde{R}$ that is equivariant, i.e. $\gamma(t) = (1+t)^\gamma - 1$.

Conversely, for any such a $\mathbb{Z}_p^*$-torsor $R \to \widetilde{R}$, an equivariant element $t \in \widetilde{R}$ descends to a map $X \to \mathrm{Spd}(\mathbb{Q}_p)$. □

Prop. (17.9.4.15). $\mathcal{P}$erf$\mathrm{d}\mathcal{S}$pa $/\mathbb{Q}_p$ is equivalent to the category of perfectoid spaces $X \in \mathcal{P}\mathrm{erf}_p$ together with a map $X \to \mathrm{Spd}(\mathbb{Q}_p)$. ⌟

Proof: Consider the category of triples $(X^\sharp, X, \iota)$, where $X^\sharp$ is a perfectoid space over $\mathbb{Q}_p$, X is a perfectoid space of characteristic p, $\iota : X^{\sharp\flat} \cong X$ is an isomorphism. A map of triples is a tuple $(f^\sharp, f) : (X^\sharp, X, \iota) \to (Y^\sharp, Y, \iota')$ that $\iota' \circ f^{\sharp\flat} = f \circ \iota$.

This category is equivalent to the category of perfectoid spaces over $\mathbb{Q}_p$ by the forgetful functor, where the quasi-inverse is given by $X^\sharp \mapsto (X^\sharp, X^{\sharp\flat}, \mathrm{id}_{X^{\sharp\flat}})$. And this category is also fibered in equivalent relations over Perf. So it is equivalent to a presheaf $\mathrm{Untilt}_{\mathbb{Q}_p}$ which maps X to the isomorphism classes of untilts $(X^\sharp, \iota)$ over $\mathbb{Q}_p$, where $\iota : X^{\sharp\flat} \cong X$ is an isomorphism, by(4.2.3.31).

Similarly we can show define a functor Untilt which maps X to the isomorphism classes of untilts $(X^\sharp, \iota)$(of whatever characteristic), where $\iota : X^{\sharp\flat} \cong X$ is an isomorphism.

Let $X = \mathrm{Spa}(R, R^+)$ be an affinoid perfectoid space of characteristic p. If $X^\sharp = \mathrm{Spa}(R^\sharp, R^{\sharp+})$ is an untilt. Let $\widetilde{X}^\sharp = X^\sharp \widetilde{\otimes}_{\mathbb{Q}_p} \mathbb{Q}_p^{\mathrm{cycl}}$, then $\widetilde{X}^\sharp \to X^\sharp$ is a pro-étale $\underline{\mathbb{Z}_p^*}$-torsor, whose tilt $\widetilde{X} \to X$ is a pro-étale $\underline{\mathbb{Z}_p^*}$-torsor equipped with a $\underline{\mathbb{Z}_p^*}$-equivariant map $\widetilde{X} \to \mathrm{Spa}(\mathbb{Q}_p^{\mathrm{cycl}})^\flat$ this is a morphism $X \to \mathrm{Spd}(\mathbb{Q}_p)$ by(17.9.4.14).

Conversely, let $\widetilde{X} \to X$ be a pro-étale $\underline{\mathbb{Z}_p^*}$-torsor and $\widetilde{X} \to \mathrm{Spa}(\mathbb{Q}_p^{\mathrm{cycl}})^\flat$ a $\underline{\mathbb{Z}_p^*}$-equivariant map, then by tilting equivalence there exists a morphism $\widetilde{X}^\sharp \to \mathrm{Spa}(\mathbb{Q}_p^{\mathrm{cycl}})$ which is also $\underline{\mathbb{Z}_p^*}$-equivariant. The equivariance means that it is a descent datum along $\widetilde{X} \to X$, so it descends to an untilt $X^\sharp$ of X over $\mathbb{Q}_p$.

Finally, for general affinoid perfectoid space X, as $\mathrm{Untilt}_{\mathbb{Q}_p}$ and $\mathrm{Spd}(\mathbb{Q}_p)$ are all sheaves on Perf, the above construction can be glued to give an isomorphism between them. □

Prop. (17.9.4.16) [Untilts is a Sheaf]. Untilt is a v-sheaf on $\mathcal{P}\mathrm{erfd}$. So does $\mathrm{Untilt}_{\mathbb{Q}_p}$, because the invertibility of p can be verified locally as $\mathcal{O}$ is sheaf. ⌟

Proof: Firstly Untilt is clearly an analytic sheaf, so it suffices to show that if $X = \mathrm{Spa}(R, R^+)$ is a perfectoid space of characteristic p with a v-cover $Y = \mathrm{Spa}(S, S^+) \to X$ and $Y^\sharp = \mathrm{Spa}(S^\sharp, S^{\sharp+})$ is an untilt of Y that the corresponding two untilts of $Z = Y \times_X Y$ agree, then there is a unique untilt $X^\sharp = \mathrm{Spa}(R^\sharp, R^{\sharp+})$ whose pullback to Y is $Y^\sharp$.

Cf.[Sch17]P86. □

Spatial Diamonds

Def. (17.9.4.17) [Spatial Diamonds]. A **spatial diamond** is a qcqs diamond D s.t. $|D|$ has a basis of opens $|U|$ s.t. $U \subset D$ is a qc open immersion. ⌟

Proof: □

Diamonds associated to Perfectoid Spaces

Def. (17.9.4.18). For $Y \in \mathcal{P}\mathrm{erfd}\mathcal{S}\mathrm{pa}$, $Y^\diamond$: is the map $X \mapsto$ untilts of X with a map to Y.

It is a locally spatial diamond, s.t. $|Y^\diamond| = |Y|$. ⌟

Example (17.9.4.19). $\mathrm{Spa}(R, R^+)^\diamond = \mathrm{Spa}(R^\sharp, R^{+\sharp})$. ⌟

17.10 Untilts and Fargues-Fontaine Curves

References are [FF curves, Lurie], [FF Curve, Johannes], [The Fargues-Fontaine Curve and Diamonds Mathew Morrow], [Laurent Fargues and Jean-Marc Fontaine. Courbes et fibrés vectoriels en théorie de Hodge p-adique].

1 Schematic F-F Curve

Def. (17.10.1.1) [Fargues-Fontaine Curve]. The sum $\oplus_n B^{\varphi=p^n}$ is a graded ring. In fact, it is non-negatively graded(17.10.1.33), and we define the **Fargues-Fontaine curve** as the scheme

$$\mathrm{Proj}(\oplus_{n\geq 0}B^{\varphi=p^n}).$$

⌟

Def. (17.10.1.2)[Formal Logarithm]. For $x\in 1+\mathfrak{m}_{C^\flat}$, $[x]-1=[x-1]+\sum_{n>0}[c_n]p^n$, thus $|[x]-1|_\rho\geq |x-1|>0$, thus the formal logarithm

$$\log([x])=\sum_{k>0}\frac{(-1)^{k+1}}{k}([x]-1)^k$$

converges for every Gauss norm $|\cdot|_\rho$, thus converges to some element in B. And clearly $\varphi(\log([x]))=p\log([x])$, thus $\log([x])\in B^{\varphi=p}$. And $\log([xy])=\log([x])\log([y])$. ⌟

Prop. (17.10.1.3) [Artin-Hasse Exponential]. There is another way of constructing elements in $B^{\varphi=p}$, which is

$$T:a\in\mathfrak{m}_{C^\flat}\mapsto\sum_n\frac{[a^{p^n}]}{p^n}.$$

We want to relate this one to the formal logarithm:

There is a bijection of sets $\mathfrak{m}_{C^\flat}\cong 1+\mathfrak{m}^b_{C^\flat}$ that $\log([E(a)])=T(a)$, which is defined by the **Artin-Hasse exponential**

$$E(x)=\prod_{(d,p)=1}(\frac{1}{1-x^d})^{\frac{\mu(d)}{d}}.$$

⌟

Proof: Firstly, it has coefficients in $\mathbb{Z}_{(p)}$, because $(1-x^d)^{\frac{1}{d}}=\sum(-1)^kC^k_{\frac{1}{n}}x^{kd}$ has coefficient in $\mathbb{Z}_{(p)}$. And $[1-x]=\lim_k(1-[x^{p^{-k}}])^{p^k}$, so

$$\log([\prod_{(d,p)=1}(\frac{1}{1-x^d})^{\frac{\mu(d)}{d}}])=\sum_{(d,p)=1}\frac{\mu(d)}{d}\log(\frac{1}{[1-d]})=\sum_{(d,p)=1}\mu(d)\sum_{\alpha\in p^{-n}\mathbb{Z}}\frac{[x^{d\alpha}]}{d\alpha}$$

Notice the right hand side stablizes for any term $[x^\beta]$, and if $\beta\neq\frac{1}{p^k}$, it will vanish, thus for $x\in\mathfrak{m}_{C^\flat}$, it converges, and the sum equals $\sum_n\frac{[x^{p^n}]}{p^n}$. □

Cor. (17.10.1.4). The set of elements of the form $\sum_n\frac{[a^{p^n}]}{p^n}$ is closed under addition. ⌟

Valuation Function

Def. (17.10.1.5) [Exponential Valuation]. For any positive real number s, define a valuation on $A_{\inf}[\frac{1}{p},\frac{1}{[t]}]$ by the formula $v_s(f) = -\log|f|_{\exp(-s)}$, then it is a valuation by(17.11.1.8).

If f has a Teichmuller expansion $\sum_{n>>-\infty}[c_n]p^n$, then

$$|f|_\rho = \sup\{|c_n|_{C^\flat}\rho^n\}, \quad v_s(f) = \inf\{v(c_n) + ns\}.$$

⌟

Prop. (17.10.1.6). For any $f \neq 0 \in A_{\inf}[\frac{1}{p},\frac{1}{[t]}]$, $s \mapsto v_s(f)$ is a concave function in s which is piecewise linear with integral slopes. ⌟

Proof: Consider the Newton Polygon. □

Lemma (17.10.1.7). If $s > 0$ and f_n is a Cauchy sequence in $A_{\inf}[\frac{1}{p},\frac{1}{[t]}]$ for the norm $|\cdot|_{\exp(-s)}$ and doesn't converge to 0, then the sequences

$$v_s(f_n), \quad \partial_- v_s(f_n), \quad \partial_+ v_s(f_n)$$

stablize. ⌟

Proof: Easy, Cf.[ff Curve Lurie P44]. □

Prop. (17.10.1.8). If $0 < a \leq b < 1$, and f_n is a Cauchy sequence in $A_{\inf}[\frac{1}{p},\frac{1}{[t]}]$ and doesn't converge to 0 for either the norm $|\cdot|_a$ or $|\cdot|_b$, then the sequence of functions $s \mapsto v_s(f)$ stablizes on $[-\log(b), -\log(a)]$. ⌟

Proof: Assume f_n doesn't converge to 0 for the form $|\cdot|_b$, then by(17.10.1.7), the sequences $v_s(f_n), \partial_+ v_s(f_n)$ converges, thus $v_s(f_n)$ is bounded uniformly, thus $v_s(f)$ is bounded.

Then choose N large that $|f - f_m|_\rho$ very small for any $m > N$ and $a \leq \rho \leq b$, then $v_s(f) = v_s(f_m)$ for any $a \leq s \leq b$, thus it stablizes. □

Cor. (17.10.1.9). Let f be a non-zero element in B, then the construction $s \mapsto v_s(f)$ is a concave function in s with piecewise linear function with integral slopes. This is analogous to the Hadamard three circle theorem(11.5.2.13). ⌟

Proof: This is true for $f \in B_{[a,b]}$, because any f is a limit of a sequence f_n in both the norm $|\cdot|_a$ and $|\cdot|_b$, so by the proposition, there for n large, $v_s(f) = v_s(f_n)$ on $[-\log(b), -\log(a)]$, thus the conclusion is true by(17.10.1.6). And for $f \in B$, for any interval $[a,b]$ we can do the same, thus the conclusion is true on each interval, thus it is true. □

Metric Structures on Y

Def. (17.10.1.10) [Metric on $\overline{Y}$]. Let $\overline{Y} = Y \cup \{0\}$ be the isomorphism classes of untilts of $C^\flat$, where 0 corresponds to $C^\flat$ itself.

(17.11.1.5) show $\overline{Y}$ corresponds to distinguished elements in $A_{\inf}$ up to units. So for any $x, y \in \overline{Y}$, we let $d(x,y) = |\xi_x(y)|_{K_y} \leq 1$. Then this is a metric, and it is non-Archimedean. ⌟

Proof: Firstly, if $d(x,y)=0$, then ξ_x divides ξ_y, which is equivalent to $(\xi_x)=(\xi_y)$, by(5.5.4.21).

Secondly, for any x,y, since $C^\flat$ is alg.closed, we can assume $\xi_x(y)=c^\sharp$ for some $c\in C^\flat$. Notice $\xi(y)=t^\sharp+pu(y)$ is in $\mathfrak{m}_K$, thus $c\in\mathfrak{m}_{C^\flat}$. So $\xi_x-[c]$ is also a distinguished element and vanishes at y, so we may assume that $\xi_y=\xi_x-[c]$ by(5.5.4.21) again. Then

$$d(y,x)=|\xi_y(x)|_{K_x}=|c^\sharp|_{K_x}=|c|_{C^\flat}=|c^\sharp|_{K^y}=d(x,y).$$

Finally it is non-Archimedean because any valuation field K is non-Archimedean. □

Prop. (17.10.1.11) [$\overline{Y}$ is Complete]. $\overline{Y}$ is complete w.r.t this metric. ⌟

Proof: Given a Cauchy sequence of points y_n in $\overline{Y}$, as in the proof of(17.10.1.10), we can assume that $\xi_{y_n}=\xi_{y_{n-1}}+[c_n]$ for some $c_n\in\mathfrak{m}_{C^\flat}$, and $|c_n|_{C^\flat}=d(y_{n-1},y_n)$. Now A_{inf} is $[t]$-adically complete for a uniformizer $t\in C^\flat$, thus $\sum[c_n]$ is definable in A_{inf}, and $\xi=\xi_0+\sum[c_n]$ is also distinguished, and corresponds to a point y which y_n clearly converges to. □

Divisors

Lemma (17.10.1.12). $B_{[a,b]}$ is an integral domain. ⌟

Proof: By(17.10.1.9), the valuation function $v_s(f)$ and $v_s(g)$ are bounded, thus it is clear that $v_s(fg)$ is also finite, so $fg\neq 0$. □

Prop. (17.10.1.13) [Divisors]. Assume $C^\flat$ is alg.closed, then for any $f\in B_{[a,b]}$ and $y=(K,\iota)\in Y_{[a,b]}$, we define the **order of vanishing** $\mathrm{ord}_K(f)\in\mathbb{Z}\cup\{\infty\}$ as the valuation of $e_K(f)\in B^+_{\mathrm{dR}}(K)$. Then

- if $f\neq 0\in B_{[a,b]}$, then $\mathrm{ord}_K(f)<\infty$ for each $K\in Y_{[a,b]}$, and there are only f.m. K that $\mathrm{ord}_K(f)\neq 0$. In particular, $B_{[a,b]}$ is an integral domain.
- if $x,y\neq 0\in B_{[a,b]}$, then x divides y iff $\mathrm{ord}_K(x)\geq\mathrm{ord}_K(y)$ for each $K\in Y_{[a,b]}$.

Thus for each $f\in B_{[a,b]}$, we can define the **divisor** of K as the formal sum $\sum_{K\in Y_{[a,b]}}\mathrm{ord}_K(f)K$, and this is also definable for $f\in B$, but it may be an infinite but locally finite sum. ⌟

Proof: Firstly, by(17.10.1.17) and(17.10.1.18), if $\mathrm{div}(f)\cap Y_{[a,b]}\neq 0$, then there is a distinguished element ξ that $f=\xi f_1$. And we can iterate this, and eventually end up with $f=\xi_1\ldots\xi_n f_n$ that $\mathrm{div}(f_n)\cap Y_{[a,b]}=0$, by(17.10.1.19), so by(17.10.1.20), f_n is invertible in f, so $\mathrm{div}(f)$ is finite. And if $\mathrm{div}(g)\geq\mathrm{div}(f)$, then g also divides $\xi_1\ldots\xi_n$, so g divides f. □

Remark (17.10.1.14). Notice by(17.11.1.22), for a $f\in B_{[a,b]}$, $\mathrm{ord}_K(f)>0$ iff $f(y)=0\in K$. ⌟

Cor. (17.10.1.15) [B is Integral Domain]. B is an integral domain, and if $C^\flat$ is alg.closed, then x is divisible by y if and only if $\mathrm{div}(x)\geq\mathrm{div}(y)$. ⌟

Cor. (17.10.1.16). B is integrally closed. ⌟

Proof: B is an integral domain by(17.10.1.15), it is integrally closed because if f/g is integral over B, then there image in $B^+_{\mathrm{dR}}(y)$ is integral over $B^+_{\mathrm{dR}}(y)$ for all $y\in Y$, thus in $B^+_{\mathrm{dR}}(y)$ because it is a valuation ring, and then f is divisible by g by(17.10.1.15). □

Prop. (17.10.1.17) [Examples of Divisors].

- For a distinguished element ξ, if $\xi=up$, then ξ is invertible in B, thus $\mathrm{div}(\xi)=0$. Otherwise ξ defines a char0 untilts K of $C^\flat$, and ξ is a uniformizer of $B^+_{\mathrm{dR}}(K)$, and it doesn't divides other distinguished elements(5.5.4.21), thus $\mathrm{div}(\xi)=K$.

- $\mathrm{div}(\log([x])) = \sum_{n\in Z} \varphi^n(K)$.

⌟

Proof: 2: $\log([x])$ vanishes at a single φ-orbits of Y, and one of them is given by the distinguished element $\xi = 1 + [x^{1/p}] + \ldots + [x^{p-1/p}] = \frac{[x]-1}{[x^{1/p}]-1}$. Notice $[x^{1/p}] - 1$ is mapped to an invertible element in K, thus it is invertible in $B^+_{\mathrm{dR}}(K)$, so $[x] - 1$ is associated to ξ, and notice

$$\log([x]) = \sum_{k>0} \frac{(-1)^{k+1}}{k}([x]-1)^k \equiv [x] - 1 \mod ([x]-1)^2,$$

so $\mathrm{ord}_K(\log([x])) = 1$, and because $\varphi(\log([x])) = p\log([x])$, $\mathrm{ord}_{\varphi^n(K)}(\log([x])) = 1$ for any n, so we are done. □

Lemma (17.10.1.18). Let $C^\flat$ be alg.closed. If ξ is a distinguished element of A_{inf} vanishes at a point $y \in Y_{[a,b]}$ and $g \in B_{[a,b]}$ also vanishes at y, then g is divisible by ξ in $B_{[a,b]}$. ⌟

Proof: If $g \in A_{\mathrm{inf}}[\frac{1}{p}, \frac{1}{[\pi]}]$, then this is easy by(17.10.1.14) and $A_{\mathrm{inf}}/(\xi) = \mathcal{O}_K$(17.11.1.4).

Now generally g is a limit of $g_n \in A_{\mathrm{inf}}[\frac{1}{p}, \frac{1}{[\pi]}]$, so $g(y)$ is the limit of $g_n(y) \in K$. Now $g(y) = 0$, so $\lim_n g_n(y) = 0$. Now K is alg.closed by(11.2.8.16), so we can let $g_n(y) = c_n^\sharp$, so c_i converges to 0 in $C^\flat$. So $\{[c_n]\}$ converges to 0 in norm $|\cdot|_a$ and $|\cdot|_b$, so we can replace g_n by $g_n - [c_n]$ and assume $g_n(y) = 0$.

Now the first part shows $g_n = \xi h_i$, and now h_i is a Cauchy sequence for both $|\cdot|_a$ and $|\cdot|_b$, so converges to some h, and then $g = \xi h$. □

Lemma (17.10.1.19). Given this lemma(17.10.1.18), we have a strategy of proving(17.10.1.13), that is, decomposing f, g into distinguished elements, but we need to show this decomposition is finite. And this is true:

If $f \neq 0 \in B_{[a,b]}$, denote $\beta = -\log(b), \alpha = -\log(a)$ and let $N = \partial_- v_\beta(f) - \partial_+ v_\alpha(f) \geq 0$, then f cannot be divisible by a product of $\xi_1, \ldots, \xi_{N+1}$ of $N+1$ distinguished elements. ⌟

Proof: By(5.5.4.20), if ξ is distinguished, then $v_s(\xi) = \max\{s, v(v_0)\}$. Now $v(v_0) = v(t^\sharp) = v(|p|_K)$ in $\mathcal{O}_K = A_{\mathrm{inf}}/([t] - up)$, so if K corresponding to ξ belongs to $Y_{[a,b]}$, then $v(v_0) \in [\beta, \alpha]$, so $\partial_- v_\beta(\xi) = 1, \partial_+ v_\alpha(\xi) = 0$.

So if $f = \xi_1, \ldots, \xi_{N+1} u$, then $N(f) \geq \sum N(\xi_i) \geq N+1$. □

Lemma (17.10.1.20) [Valuation Funtion And Invertibility]. Let $C^\flat$ be alg.closed and $f \neq 0 \in B_{[a.b]}$, then the following are equivalent:

- f is invertible.
- $\partial_- v_\beta(f) = \partial_+ v_\alpha(f)$.
- $\mathrm{div}(f) \cap Y_{[a,b]} = \varnothing$.

⌟

Proof: 2 → 3: by(17.10.1.19).

1 → 2: Because $N(f) + N(f^{-1}) = 0$, and $N(f) \geq 0, N(f^{-1}) \geq 0$, so $N(f) = 0$.

2 → 1: Assume first that $f = \sum_{n>>-\infty} [c_n] p^n \in A_{\mathrm{inf}}[\frac{1}{p}, \frac{1}{[\pi]}]$, then the hypothesis just says that $s \to v_s(f)$ is linear in a small nbhd of $[\beta, \alpha]$, that is, there is a n_0 that $v(c_n) + ns > v(c_{n_0}) + n_0 s$ for all $n \neq n_0$ and $s \in [\beta, \alpha]$.

Now we can normalize f that $n_0 = 0$ and $c_0 = 1$, so $|f-1|_\rho < 1$ for all $\rho \in [\beta, \alpha]$, so $f-1$ is topologically nilpotent in $B_{[a,b]}$, and thus f is invertible.

Generally, f is a limit of a sequence $f_n \in A_{\inf}[\frac{1}{p}, \frac{1}{[\pi]}]$, and by(17.10.1.8) we can assume the hypothesis holds for all f_n. Then f_n is invertible, and it is easily shown that f_n^{-1} is a Cauchy sequence in $B_{[a,b]}$, so converges to some f^{-1}.

$3 \to 2$: Firstly, if $\partial_- v_\beta(f) > \partial_+ v_\alpha(f)$, then we must have $\partial_- v_\rho(f) > \partial_+ v_\rho(f)$ for some s, so wlog, we can assume $a = b = s$, and we need to show f vanishes at some point in $Y_{\exp(s)}$. Now combining with(17.10.1.18) and(17.10.1.19), this is equivalent to another statement that any element $y \in B_{[\rho,\rho]}$ has a decomposition $y = g\xi_1 \ldots \xi_n$ where ξ_k corresponds to points in Y_ρ and g is invertible in B_ρ. The proof is finished at(17.10.1.30). □

Primitive Elements and the Proof of $3 \to 2$ of The Lemma on Valuation Function and Invertibility

Def. (17.10.1.21). Let $C^\flat$ be alg.closed, an element in $B_{[\rho,\rho]}$ is called **good** iff it has a decomposition as in the proof of $3 \to 2$ of(17.10.1.20). ⌟

Prop. (17.10.1.22) [Approximating Zero]. If f is a good element having n-zeros on Y_ρ, and $g \in B_\rho$ that $|f-g|_\rho < |f|_\rho$, then for any zero y of g on Y_ρ, there exists a zero y' of f on Y_ρ that $d(y', y) < \rho(\frac{|f-g|_\rho}{|g|_\rho})^{1/n}$. ⌟

Proof: $|f-g|_\rho \geq |(f-g)(y)|_K = |f(y)|_K$. Now $f = g\xi_1 \ldots \xi_n$, and ξ corresponds to y_i, then

$$|f(y)|_K = |g(y)|_K |\xi_1(y)|_K \ldots |\xi_n(y)|_K = \frac{|f|_\rho}{\prod_i |\xi_i|_\rho} \prod_i d(y_i, y) = |f| \prod_i \frac{d(y_i, y)}{\rho}.$$

(Notice $|g|_\rho = |g(y)|_K$ because g is invertible(17.11.1.10)) and $d(y_i, y) \leq \rho$. So at least one ξ satisfies the desired inequality. □

Cor. (17.10.1.23). If $f \in B_\rho$ is given by a Cauchy sequence of good elements, and $\partial_- v_\rho(f) > \partial_+ v_\rho(f)$, then f has a root on Y_ρ. ⌟

Proof: By(17.10.1.7), passing to a subsequence, we may assume

$$v_s(f) = v_s(f_n), \quad \partial_- v_s(f) = \partial_- v_s(f_n), \quad \partial_+ v_s(f) = \partial_+ v_s(f_n), \quad |f_{n+1} - f_n|_\rho < |f|_\rho.$$

Let $n = \partial_- v_s(f) - \partial_+ v_s(f) > 0$, then each f_i has exactly n roots on Y_ρ, and applying(17.10.1.22), we can find successively roots y_n of f_n that $d(y_{n+1}, y_n) \leq \rho(\frac{|f_{n+1}-f_n|_\rho}{|f|_\rho})^{1/n}$, so the sequence $\{y_n\}$ is Cauchy and converges to some point $y \in \overline{Y}$, so

$$|f_i(y)|_K \leq |f_i|_\rho \frac{d(y_i, y)}{\rho} = |f|_\rho \frac{d(y_i, y)}{\rho} \to 0.$$

so $f(y) = 0$. □

Def. (17.10.1.24) [Primitive Elements]. An element $f = \sum_{n \geq 0} [c_n] p^n \in A_{\inf}$ is called **primitive of degree** d if $c_0 \neq 0, |c_d| = 1$ for some smallest element d.

Clearly an element is distinguished of degree 1 iff it is distinguished and corresponds to an untilts of $X^\flat$ of char0. ⌟

Prop. (17.10.1.25).

- Any element $f \in A_{\inf}$ of finite Teichmuller expansion can be written uniquely as a $f = p^m[c]g$, where $c \in C^\flat$ and g is primitive.
- For an element $f \in A_{\inf}[\frac{1}{p}, \frac{1}{[t]}]$, f can be written as $p^m[c]g$ iff $v_s(f)$ consists of f.m. line segments iff $\sup\{|c_n|\}$ is achieved by some n.
- If $f = gh$ in $A_{\inf}$ is primitive, then g, h are also primitive, and $\deg(f) = \deg(g) + \deg(h)$.

⌟

Prop. (17.10.1.26). Let $f = \sum [c_n]p^n \in A_{\inf}$ be primitive of degree $d > 0$, and let $\lambda \in (0, 1)$ be the number that $s = -\log(\lambda)$ is the minimal number that $v_s(f)$ is non-differentiable at, i.e. s is -1 times the slope of the line segment on the left of $v(c_d)$. Then f has a zero on Y_λ. ⌟

Proof: By(17.10.1.27) there is a $y \in Y_\lambda$ that $|f(y_1)| \le \lambda^{d+1}$, and then(17.10.1.28) shows we can find successively y_n that

$$d(y_n, y_{n+1}) \le \lambda^{1+\frac{d}{n}}, \quad |f(\lambda_n)| \le \lambda^{d+m}.$$

So y_n is a Cauchy sequence thus converges to some y, and then $f(y) = 0$. □

Lemma (17.10.1.27) [Lemma for Approaching a Zero]. If $C^\flat$ is alg.closed and $f \in A_{\inf}$ is primitive of degree $d > 0$, and let λ as in(17.10.1.26), then there is a point $y \in Y_\lambda$ that $|f(y)|_{K_y} \le \lambda^{d+1}$. ⌟

Proof: Let $f = \sum [c_n]p^n$, we may assume $c_d = 1$, and let $F = x^d + c_{d-1}x^{d-1} + \ldots + c_0$, then the largest valuation of the roots of F on $C^\flat$ is λ, by Newton polygon. Let r be such a root, then c_i is divisible by r^{d-i}, and let $\xi = p - [r]$ be a distinguished element of $A_{\inf}$ and corresponds to an untilt K, then $|p|_K = \lambda$, and

$$p^{-d}f(y) = \sum_{n \ge 0} c_n^\sharp p^{n-d} \equiv \sum_{i=0}^{d} (\frac{c_i}{r^{d-i}})^\sharp \mod p = (r^{-d}F(r)) \mod p = 0$$

thus $f(y)$ is divisible by p^{d+1}, which is equivalent to $|f(y)|_K \le \lambda^{d+1}$. □

Lemma (17.10.1.28) [Lemma for Approaching a Zero]. Situation as in(17.10.1.27), if $y \in Y_\lambda$ and $|f(y)| = \lambda^d \cdot \alpha$, then there is a y' that $d(y, y') \le \lambda \cdot \alpha^{1/d}$ that $|f(y')| \le \lambda^{d+1}\alpha$. ⌟

Proof: Since $A_{\inf}$ is ξ-complete and every element of $A_{\inf}/\xi \cong \mathcal{O}_K$ belongs to the image of $\sharp : \mathcal{O}_C^\flat \to \mathcal{O}_K$, thus by induction, we can write $f = \sum_{n \ge 0} [c_n]\xi^n$. Because f is primitive of degree d, we may assume $c_d = 1$, and $|c_0|_{C^\flat} = |f(y)|_K = \lambda^d\alpha$.

Let $F(x) = c_0 + c_1x + \ldots + c_{d-1}x^{d-1} + x^d$, because $C^\flat$ is alg.closed, let r be a root of minimal absolute value, then $|r|^m_{C^\flat}|c_m|_{C^\flat} \le \lambda^n\alpha$, in particular $|r|_{C^\flat} \le \lambda\alpha^{1/n}$. So let $\xi' = \xi - [r]$, then ξ is also distinguished, and $d(y', y) = |r|_{C^\flat} \le \lambda\alpha^{1/n}$(17.10.1.10), and $d(0, y') = \lambda$, and $\xi(y') = r^\sharp$.

Now

$$\frac{(f(y'))^\sharp}{c_0^\sharp} = \sum_{n \ge 0} \frac{c_n^\sharp}{c_0^\sharp}\xi(y')^n = \sum_{n \ge 0} (\frac{c_n r^n}{c_0})^\sharp \equiv \sum_{i=0}^{n} (\frac{c_n r^n}{c_0})^\sharp \mod p = (\frac{F(r)}{c_0})^\sharp = 0,$$

So $|f(y')|_{K'} \le |c_0^\sharp|_{K'}|p|_{K'} = |c_0|_{C^\flat}\lambda = \lambda^{d+1}\alpha$. □

Cor. (17.10.1.29) [Primitive Elements Decompose as Distinguished Elements]. If $f \in A_{\inf}$ is a primitive element of degree $d > 0$, then f admits a factorization as products of distinguished elements ξ corresponding to points in Y. ⌟

Proof: Use induction on d. If $d = 1$, then f is distinguished by(17.10.1.24), and if $d > 1$, then by(17.10.1.26), $f = \xi g$, so g is primitive of degree $d-1$ by(17.10.1.25), so induction is finished. □

Prop. (17.10.1.30) [Finite Teichmuller Expansion is Good]. Any element of finite Teichmuller expansion is good.

In particular, because any element of B_ρ can be approximated by elements in $A_{\mathrm{inf}}[\frac{1}{p}, \frac{1}{[t]}]$, and such element can be approximated by elements of finite Teichmuller expansion, by(17.10.1.23), we finishes the proof of $3 \to 2$ of(17.10.1.20). ⌟

Proof: If f has finite Teichmuller expansion, then $f = p^m[c]g$, where g is primitive of degree d. If $d = 0$, then g is invertible in A_{inf}, thus f is invertible in B_ρ. Otherwise, we can use(17.10.1.29) to factorize g into distinguished elements, and the elements that corresponds to points outside Y_ρ is invertible in B_ρ because $v_s(\xi) = \max\{s, v(v_0)\}$ and $2 \to 1$ of(17.10.1.20), so f is good. □

Bounded Meromorphic Functions

Prop. (17.10.1.31). If $f \in B$, then $f \in A_{\mathrm{inf}}$ iff $|f|_\rho \le 1$ for any $0 < \rho < 1$.

Easily we can get characterization of f being in $A_{\mathrm{inf}}[\frac{1}{p}], A_{\mathrm{inf}}[\frac{1}{[t]}]$ or $A_{\mathrm{inf}}[\frac{1}{p}, \frac{1}{[t]}]$. ⌟

Proof: One direction is trivial, for the other, by(17.10.1.32), we can find successively f_n that $f = \sum_{i<n}[c_i]p^i + f_n$, and $|f_n|_\rho \le \rho^n$ for all $0 < \rho < 1$. So f_n converges to 0 in any norm ρ, thus it converges to 0 in B, and $f = \sum_{n\ge 0}[c_n]p^n \in A_{\mathrm{inf}}$. □

Lemma (17.10.1.32). If $f \in B$ satisfies $|f|_\rho \le \rho^m$ for all $0 < \rho < 1$, then there is a $c \in \mathcal{O}_{C^\flat}$ that $f = [c]p^m + g$ that $|g|_\rho \le \rho^{m+1}$ for all $0 < \rho < 1$. ⌟

Proof: Replace f by $\frac{f}{p^m}$, we may assume $m = 0$. Choose a sequence f_i in $A_{\mathrm{inf}}[\frac{1}{p}, \frac{1}{[t]}]$ converging to f in B, where $f_i = \sum_{n>>-\infty}[c_{n,i}]p^n$.

Firstly we want to truncate f_i with the positive part f_i^+. Notice for each ρ and any $0 < \varepsilon < 1$, because $\lim |f_i - f|_{\varepsilon\rho} = 0$, thus for i large, $|f_i|_{\varepsilon\rho} = |f|_{\varepsilon\rho} \le 1$, thus $|c_{-n,i}|_{C^\flat}\rho^{-n} \le \varepsilon^n < \varepsilon \le \varepsilon$, so $|f_i - f_i^+|_\rho < \varepsilon$ for i large, so $\lim f_i^+ = f$ also in B.

Secondly, $|c_{0,i} - c_{0,j}|_{C^\flat} \le |f_i - f_j|_\rho$ for each ρ, thus $c_{0,i}$ is Cauchy in $C^\flat$ thus converges to some $c \in C^\flat$, and when i is large, $|c_{0,i}|_{C^\flat} \le |f_i|_\rho = |f|_\rho \le 1$, so $c \in \mathcal{O}_{C^\flat}$. Now let $g_i = \sum_{n>0}[c_{n,i}]p^n$, then g_i is also Cauchy in B for any norm $|\rho|$ and converges to some g, and $f = g + [c]$.

It's left to check $|g|_\rho \le \rho$: each $v_s(g_i)$ has positive slopes, then so does $v_s(g)$ because by(17.10.1.7), $v_s(g_i)$ stablizes to $v_s(g)$ uniformly on compact intervals. So if $v_s(g) < s - \varepsilon$ for some s, then $v_\varepsilon(g) \le v_s(g) - (s - \varepsilon) < 0$, but this cannot happen because $v_\varepsilon(g) \le \max\{v_\varepsilon(f), -\log |c|_{C^\flat}\} \ge 0$. □

Eigenspaces of Frobenius

Prop. (17.10.1.33).

- The vector space $B^{\varphi=p^n}$ vanish for $n < 0$.
- The canonical map $\mathbb{Q}_p \to B^{\varphi=\mathrm{id}}$ is an isomorphism.

⌟

Proof: 1: Consider $v_{ps}(\varphi(f)) = pv_s(f)$(17.11.1.14), $v_s(p^n f) = ns + v_s(f)$, so if $\varphi(f) = p^n f$, then

$$pv_{s/p}(f) = v_s(\varphi(f)) = v_s(p^n f) = ns + v_s(f).$$

Let $h(s) = \partial_+ v_s(f)$, then $h(s/p) = n + h(s)$, but h must by non-increasing(17.10.1.6), so $n \ge 0$.

2: Firstly we prove $B^{\varphi=\mathrm{id}}$ is a field: by(17.10.1.15), it suffices to show that $\mathrm{div}(f) = 0$ for $f \neq 0 \in B^{\varphi=\mathrm{id}}$. If $\mathrm{div}(f) \neq 0$, because f is fixed by φ, so $\mathrm{div}(f) \geq \sum_{n\in\mathbb{Z}} \varphi^n(y)$ for some y, and $\sum_{n\in\mathbb{Z}} \varphi^n(y) = \mathrm{div}(\log([\varepsilon])$ for some $\varepsilon \in 1 + \mathfrak{m}_{C^\flat}$ because K is alg.closed and by (17.11.1.16). So by(17.10.1.15) again $f = g\log([\varepsilon])$, and $g \in B^{\varphi=p^{-1}}$ by(17.10.1.2), then $g = 0$ by item1.

3: From(17.10.1.34) and(17.10.1.31), $f \in A_{\mathrm{inf}}[\frac{1}{p}]$, thus $f = \sum_{n>>\infty}[c_n]p^n$, so $\varphi(f) = f$ shows $c_n^p = c_n$, which is equivalent to $c_n \in \mathbb{F}_p$. So $f \in W(\mathbb{F}_p)[\frac{1}{p}] = \mathbb{Q}_p$. □

Lemma (17.10.1.34). If $f \neq 0 \in B^{\varphi=\mathrm{id}}$, then there is an integer n that $|f|_\rho = \rho^n$. ⌟

Proof: Notice $|f|_\rho^p = |\varphi(f)|_{\rho^p} = |f|_{\rho^p}$, so $v_{ps}(f) = pv_s(f)$, differentiation shows that $\partial_- v_{ps}(f) = \partial_- v_s(f)$. This is for all $s < 0$, and $\partial_- v_s(f)$ is non-decreasing, thus it is constant, and $v_{ps}(f) = pv_s(f)$ shows $v_s(f) = ns$ for some integer n. □

Cor. (17.10.1.35). For $n \geq 0$, any element $f \in B^{\varphi=p^n}$ factors uniquely up to action of $\mathbb{Q}_p^*$ as $\lambda\log([\varepsilon_1])\ldots\log([\varepsilon_n])$ where $\lambda \in B^{\varphi=\mathrm{id}}$, $0 < |\varepsilon_i - 1| < 1$. ⌟

Proof: The existence is by(17.10.1.30)

For the uniqueness: it suffices to prove $\log([\varepsilon])$ is a prime element in $\oplus_{n\geq 0}B^{\varphi=p^n}$. For this, notice for any $f \in B^{\varphi=p^n}$, $\mathrm{div}(f)$ is fixed by φ, and $\mathrm{div}(\log([\varepsilon]))$ is a single orbit of φ, thus by(17.10.1.15), if $\log([\varepsilon])$ divides fg, then $\log([\varepsilon])$ divides f or g. □

Applications

Cor. (17.10.1.36). If $C^\flat$ is alg.closed, then every untilts K of $C^\flat$ belongs to the vanishing locus of $\log([x])$ for some $x \in C^\flat$ that $0 < |x - 1| < 1$, and the map

$$\psi : 1 + \mathfrak{m}_{C^\flat} \to K : y \mapsto \log(y^\sharp)$$

is surjective with kernel generated by x (as a $\mathbb{Q}_p$-subspace of $1 + \mathfrak{m}_{C^\flat}$). ⌟

Proof: By(11.2.8.16), any untilts of $C^\flat$ is alg.closed, thus it has a compatible p^n-th roots of unity. So it belongs to some locus of $\log([x])$ by(17.11.1.16). Now if $|z| < |p|_K^{1/(p-1)}$, then $z = \log(\exp(z))$, and $\exp = y^\sharp$ for some y because K is alg.closed. So ψ contains sufficiently small elements, but it is a map of $\mathbb{Q}_p$-vector spaces, thus it is surjective. For the kernel, if $\log(y^\sharp) = 0$, then $\log([y])$ vanish on K, thus by(17.11.1.16), y, x is in the same $\mathbb{Q}_p$-vector space. □

Cor. (17.10.1.37). If $C^\flat$ is alg.closed, then the map

$$1 + \mathfrak{m}_{C^\flat} \xrightarrow{\log([x])} B^{\varphi=p}$$

is an isomorphism. ⌟

Proof: Firstly any untilts of $C^\flat$ is alg.closed by(11.2.8.16). It is injective because of the correspondence(17.11.1.16), and for the surjectivity, for each $f \in B^{\varphi=\mathrm{id}}$, if $f = 0$, then $f = \log([1])$, and if $f \neq 0$, then notice $\mathrm{div}(f) \neq \varnothing$, because in this case f is invertible in B by(17.10.1.15), thus $f^{-1} \in B^{\varphi=p^{-1}}$, so $f^{-1} = 0$ by(17.10.1.33), contradiction.

Now if $\mathrm{ord}_K(f) \geq 1$, then $\mathrm{ord}_{\varphi^n(K)}(f) \geq 1$ for any $n \in \mathbb{Z}$ since $\varphi(f) = pf$. Consider $\mathrm{div}(\log([x])) = \sum_{n\in\mathbb{Z}} \varphi^n(K)$(17.10.1.17), then f is divisible by $\log([x])$ by(17.10.1.15), $f = \log([x])g$, then $g \in B^{\varphi=\mathrm{id}}$, then $g \in \mathbb{Q}_p^*$ by(17.10.1.33), thus $f = \log([x^g])$. □

Cor. (17.10.1.38) [Filtration on B_{dR}]. By(17.10.1.17) and(17.10.1.36), we see that for any untilt K of $C^\flat$, there is a unique up to $\mathbb{Q}_p$-constant ε that $t = \log([\varepsilon])$ is the uniformizer of $B_{\mathrm{dR}}(y)$. In fact, this ε can be to be $\varepsilon = (1, \xi_p, \ldots, x_{p^n}, \ldots)$, where ξ_{p^n} is a compatible roots of unity in the alg.closed field K.

Now we prefer to use the filtration $Fil^n = t^{-n} B^+_{\mathrm{dR}}$ on B_{dR} because it is $G_{\mathbb{Q}_p}$ invariant, as ε does. ⌟

Prop. (17.10.1.39). Let $C^\flat$ be alg.closed, then any point x of the Fargues-Fontaine curve X_{FF} that is not the generic point corresponds to the prime $x_K = (\log([\varepsilon]))$(17.10.1.35) where $K \in \mathrm{div}(\log([\varepsilon]))$(17.10.1.36). And the residue field of x_K can be identified to K. ⌟

Proof: By(17.10.1.35), we can cover X_{FF} by affine schemes of the form $\mathrm{Spec}(R_f = B[f^{-1}]^{\varphi=\mathrm{id}})$ for $f \in B^{\varphi=p}$, now for any prime $\mathfrak{p} \subset R_f$, let $\frac{g}{f^n} \in \mathfrak{p}$, then $g = \lambda \log([\varepsilon_1]) \ldots \log([\varepsilon_n])$, thus some $\frac{\log([\varepsilon])}{f} \in \mathfrak{p}$. Let K be a point that $\log([\varepsilon])$ vanish(17.11.1.16), then we claim $(\log([\varepsilon])/f)$ is maximal.

In fact, we may assume f doesn't vanish on K, otherwise $\log([\varepsilon])/f$ is a unit, then there is a map $\rho : B[f^{-1}]^{\varphi=1} \subset B[f^{-1}] \to K$, and this map is surjective with kernel $(\log([\varepsilon])/f)$: it is surjective even on $f^{-1}B^{\varphi=p}$ by(17.10.1.36), and if $\log([\varepsilon_1])/f$ is mapped to 0, then $\log([\varepsilon_1])$ differs from $\log([\varepsilon])$ by some Q_p^* by(17.11.1.16). □

Cor. (17.10.1.40). If $C^\flat$ is alg.closed, there is a bijection of sets:

$$Y/\varphi_{C^\flat}^{\mathbb{Z}} \cong \{\text{Closed points of } X_{FF}\}.$$

by(17.11.1.16). ⌟

Cor. (17.10.1.41). X_{FF} is a Dedekind scheme(6.4.2.14). ⌟

Proof: Let $\mathrm{Spec}(R_f = B[f^{-1}]^{\varphi=\mathrm{id}})$, two elements $f = \log([\varepsilon]), g = \log([\mu])$ can cover it. The proof of(17.10.1.39) shows that every prime ideals of R_f is maximal principal, in particular f.g, thus by(5.1.1.48), it is Noetherian. And it has Krull dimension 1 and it is regular because all of its maximal ideals are principal, hence normal(5.3.5.32). So X_{FF} is a Dedekind scheme. □

2 Line Bundles and Filtrations

Def. (17.10.2.1). By(17.10.1.35), the graded algebra $\oplus_{n\geq 0} B^{\varphi=p^n}$ is generated over $\mathbb{Q}_p$ by $B^{\varphi=p}$, so we can define the Serre twisting sheaf $\mathcal{O}(1)$ on X_{FF}, which is a line bundle, and on an open affine scheme $U = X - \{x\}$, where x corresponds to $\log([\varepsilon])$, $\mathcal{O}(1)(U) = (B[\frac{1}{\log([\varepsilon])}])^{\varphi=p}$. Similarly we can define $\mathcal{O}(m)$, and $\mathcal{O}(m) = \mathcal{O}(1)^m$. ⌟

Lemma (17.10.2.2). There is an isomorphism $\mathrm{Div}(X) \to \mathrm{Pic}(X)$ that maps each x to the inverse of its ideal sheaf(6.5.3.15)(5.3.5.20). And there is also a degree map $\mathrm{Div}(X) \to \mathbb{Z}$. Then:

$$\begin{array}{ccc} \mathrm{Div}(X) & \xrightarrow{\deg} & \mathbb{Z} \\ & \searrow & \downarrow \rho \\ & & \mathrm{Pic}(X) \end{array}$$

commutes. ⌟

Proof: It suffices to show that any $\mathcal{O}(x)$ is isomorphic to $\mathcal{O}(1)$. As $\log([\varepsilon])$ is a global section of $\mathcal{O}(1)$ that vanishes of order 1 at x, it induces an isomorphism $\mathcal{O}(1) \cong \mathcal{O}(x)$ by(6.5.3.15). □

Lemma (17.10.2.3) [Cohomology of Line Bundles]. For any integer m, $B^{\varphi=p^m} \to H^0(X, \mathcal{O}(m))$ is an isomorphism and $H^i(X, \mathcal{O}(m)) = 0$ for $i > 0, m > 0$. ⌟

Proof: This is trivial using Cech cohomology, as $\oplus_{n\geq 0} B^{\varphi=p^n}$ is PID, so X is separated. □

Prop. (17.10.2.4). The construction induces an isomorphism $\rho : \mathbb{Z} \cong \mathrm{Pic}(X) : m \mapsto \mathcal{O}(m)$. ⌟

Proof: By lemma(17.10.2.2), ρ is surjective because $\mathrm{Div}(X) \to \mathrm{Pic}(X)$ does, and it is injection because if $\mathcal{O}(m) \cong \mathcal{O}(n)$, then tensoring $\mathcal{O}(-m)$, we can assume $\mathcal{O} \cong \mathcal{O}(-k)$, but they have different global sections by lemma(17.10.2.3) and(17.10.1.33)(17.10.1.35). □

Harder-Narasimhan Filtration of Vector Bundles

Prop. (17.10.2.5) [Harder Narasimhan Formalism for Bun_X]. For a vector bundle L on X, we can define $\deg(L) = n$ iff $L \cong \mathcal{O}(n)$(17.10.2.2), and for a vector bundle E, define $\deg(E) = \deg(\wedge(E))$. And define the generic rank on the category of coherent sheaves on X. Then this is a Harder-Narasimhan formalism on $\mathcal{C} = \mathrm{Bun}_X$ with $\mathcal{A} = \mathcal{V}\mathrm{ect}_{K(X)}$. ⌟

Proof: Only the last axiom needs proof, but if $\mathcal{E}' \subsetneq \mathcal{E}$, notice $\wedge\mathcal{E}' \subsetneq \wedge\mathcal{E}$(The stalks are PID), so by taking their top exterior power product, we reduce to the case of line bundles.

But $\mathcal{O}(m)$ cannot map into $\mathcal{O}(n)$ if $m > n$ and must by isomorphism if $m = n$, by tensoring $\mathcal{O}(-m)$ and looking at global sections(17.10.2.3), so the assertion is true. □

Cor. (17.10.2.6). Every vector bundle $\mathcal{E}$ on X has a unique functorial Harder-Narasimhan filtration, by(4.3.4.22). ⌟

3 Base Change of Fields

Prop. (17.10.3.1) [Base Change]. Let $C^\flat$ be alg.closed. For any finite extension E of $\mathbb{Q}_p$ of degree n, $\mathrm{Spec}\, E \to \mathrm{Spec}\, \mathbb{Q}_p$ is finite étale, and finite locally free of degree n, so does $X_E = X \otimes_{\mathbb{Q}_p} E \to X$(6.6.2.24).

In particular, X_E is also a Dedekind scheme**?**. For any closed point x of X corresponding to an untilt K of $C^\flat$, which is alg.closed, the fiber of X_E over x is identical to the spectrum of $E \otimes_{\mathbb{Q}_p} K \cong K^n$ as K is alg.closed.

In this situation and use(17.10.1.40), we see that the closed points of X_E are in bijection with isomorphism classes of (K, ι, u) module φ-actions, where (K, ι) is an untilt of $C^\flat$, and $u : E \to K$ is an embedding of E into K over $\mathbb{Q}_p$, isomorphism classes of these triples are denoted by Y_E. ⌟

Prop. (17.10.3.2). By(17.10.3.1) and flat base change(6.7.5.1), we know $H^0(X_E, \mathcal{O}_{X_E}) = E$, in particular X_E is connected. ⌟

Lemma (17.10.3.3). If E is unramified of degree n over $\mathbb{Q}_p$, then $E \cong W(\mathbb{F}_{p^n})[\frac{1}{p}]$. In particular,

$$\mathrm{Hom}_{\mathbb{Q}_p}(E, K) \cong \mathrm{Hom}_{\mathbb{Z}_p}(W(\mathbb{F}_{p^n}), \mathcal{O}_K) \cong \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_{p^n}, \mathcal{O}_K/p) \cong \mathcal{O}_{C^\flat}/[t]) \cong \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_{p^n}, C)$$

where the last isomorphism is by Henselian lemma.

Therefore, $Y_E \cong Y \otimes \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_{p^n}, C)$, and

$$\text{Closed points of } Y_E \cong Y_E/\varphi^{\mathbb{Z}} \cong (Y \otimes \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_{p^n}, C))/\varphi^{\mathbb{Z}} \cong Y/\varphi^{n\mathbb{Z}}.$$

⌟

Prop. (17.10.3.4). If E is unramified of degree n over $\mathbb{Q}_p$ and $U \neq X$ is an affine open defined by a homogenous element t, then

$$U_E = \mathrm{Spec}((B[t^{-1}] \otimes_{\mathbb{Q}_p} E)^{\varphi=\mathrm{id}}) = \mathrm{Spec}(B[t^{-1}]^{\varphi^n=1}).$$

where φ acts trivially on E. ⌟

Proof: Each $u \in \mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_{p^n}, C^\flat)$ induces a map $W(\mathbb{F}_p) \to W(\mathcal{O}_{C^\flat}) = A_{\mathrm{inf}} \to B$, which extends to a map $\overline{u} : E \to B[t^{-1}]$. and induces a map $q_u : B[t^{-1}] \otimes_{\mathbb{Q}_p} E \to B[t^{-1}]$. Now

$$B[t^{-1}] \otimes_{\mathbb{Q}_p} E \to \prod_{\mathrm{Hom}_{\mathbb{F}_p}(\mathbb{F}_{p^n}, C)} B[t^{-1}]$$

is an isomorphism, which is just because $x^{p^n} - x$ splits in $B[t^{-1}]$.

And under this isomorphism, the action of φ is

$$\varphi((f_0, \ldots, f_{n-1}) = (\varphi(f_{n-1}), \varphi(f_0), \ldots, \varphi(f_{n-2})),$$

so proposition is clear. □

Cor. (17.10.3.5). Fix now a finite extension $E/\mathbb{Q}_p$ with uniformizer π that has ramification degree e and inertia degree d, and E_0 is the maximal unramified subextension, then there are maps $E_0 \to B$ by(17.10.3.4), fix forever one of them p_u, this induces a map

$$B[\frac{1}{t}] \otimes_{\mathbb{Q}_p} E \to B[\frac{1}{t}] \otimes_{E_0} E$$

and this induces an isomorphism

$$(B[\frac{1}{t}] \otimes_{\mathbb{Q}_p} E)^{\varphi=\mathrm{id}} = (B[\frac{1}{t}] \otimes_{\mathbb{Q}_p} E_0)^{\varphi=\mathrm{id}} \otimes_{E_0} E = (B[\frac{1}{t}] \otimes_{E_0} E)^{\varphi^d=\mathrm{id}}$$

⌟

Def. (17.10.3.6)[Y_E^0]. Define $Y_E^0 \subset Y_E =$ triples (K, ι, u), where (K, ι) is an untilt of $C^\flat$, and $u : E \to K$ is an embedding that $u|_{E_0}$ is identical to $e_K \circ p_u : E_0 \to B \to K$. Notice Y_E^0 is not stable under the Frobenius, but it is stable under φ^d, and induces an isomorphism

$$Y_E^0/\varphi^{d\mathbb{Z}} \cong Y_E/\varphi^{\mathbb{Z}}.$$

⌟

Prop. (17.10.3.7). Notice for an element y of Y_E^0, the map $u : E \to K_y = B_{dR}^+(y)/\xi$ extends uniquely to a map $E \to B_{dR}^+(y)$ that is compatible with $e_K \circ p_u : E_0 \to B_{\mathrm{dR}}^+(y)$, because E is separable over E_0. i.e.

$$\begin{array}{ccc} E_0 & \xrightarrow{e_K \circ p_u} & B_{\mathrm{dR}}^+(y) \\ \downarrow & \overset{\widetilde{u}}{\nearrow} & \downarrow \\ E & \xrightarrow{u} & K \end{array}$$

Then this defines a map $B \otimes_{E_0} E \to B_{\mathrm{dR}}^+(y)$, also called the stalk map. ⌟

Prop. (17.10.3.8). For any finite extension $E/\mathbb{Q}_p$, the degree map $\deg : \mathrm{Pic}(X_E) \cong \mathbb{Z}$ is an isomorphism. ⌟

Proof: It suffices to show that $\mathcal{O}_{X_E}(x) \cong \mathcal{O}_{X_E}(x')$ for each pair of closed points x, x' of X_E.

We attempt to construct a line bundle $\mathcal{O}_{X_E}(1)$ on X_E that $\mathcal{O}_{X_E}(1)(U_E) = (B[\frac{1}{t}] \otimes_{E_0} E)^{\varphi^d=\pi}$, because $\mathcal{O}_{X_E}(U_E) = (B[\frac{1}{t}] \otimes_{E_0} E)^{\varphi^d=1}$.

We show simultaneously that $\mathcal{O}_{X_E}(1)$ is a line bundle and it is isomorphic to $\mathcal{O}_{X_E}(x)$ for any closed point $x \in X_E$: For any $x \in X_E$ corresponding to a φ^d-orbit of Y_E^0, let f be the element constructed by lemma(17.10.3.9) below, we show that for any affine open $U = D(t)$, multiplying by $f : \mathcal{O}_{X_E}(x)(U_E) \to \mathcal{O}_{X_E}(1)(U_E)(\star)$ is an isomorphism:

Notice $B \otimes_{E_0} E$ is free over B, let $N(f) \in B$ be its norm, the norm is local, so for each $y \in Y$, $N(f)_y = \prod_{\overline{y}} f_{\overline{y}}$, where $\overline{y} \in Y_E$ are over y, so it vanishes with order 1 in a φ^d-orbit of Y(order 1 because f only vanishes at $\overline{y}$ in the orbit corresponding to x), and then $N(f)\varphi(N(f))\dots\varphi^{d-1}(N(f))$ vanishes at a single φ-orbit of Y with order 1, thus equals $u\log([\varepsilon])$ for some $\varepsilon \in \mathfrak{m}_{C^\flat}$, by(17.10.1.17)(17.10.1.13). In particular, y divides $\log([\varepsilon])$.

Now if $x \notin U_E$, then $\log([\varepsilon])$ divides t, so f divides t, thus f is invertible in $B[\frac{1}{t}] \otimes_{E_0} E$, thus $(\star)$ is an isomorphism.

Otherwise if $x \in U_E$, then choose some x' not in U_E, then the same argument shows that f' is invertible in $B[\frac{1}{t}] \otimes_{E_0} E$, so $f/f' \in (B[\frac{1}{t}] \otimes_{E_0} E)^{\varphi=\mathrm{id}}$ that vanishes with a single zero at x, so multiplying by f'/f defines an isomorphism $\mathcal{O}_{X_E}(U_E) \cong \mathcal{O}_{X_E}(x)(U_E)$, so it suffices to show the composition

$$\mathcal{O}_{X_E}(U_E) \xrightarrow{f'/f} \mathcal{O}_{X_E}(x)(U_E) \xrightarrow{f} \mathcal{O}_{X_E}(1)(U_E)$$

is an isomorphism, but this reduces to the first case. □

Lemma (17.10.3.9)[Uniformizer Existence]. If x be a closed point of X_E corresponding to an orbit of φ in Y_E thus an orbit S of φ^d in Y_E^0, then there is an element $f \in (B \otimes_{E_0} E)^{\varphi^d=\pi}$ that $\mathrm{ord}_{\overline{y}}(f) = 1$ if $\overline{y} \in S$, and 0 otherwise. ⌟

Proof: The map defined (17.10.3.18) composed with the Teichmuller section(17.10.3.16) in fact has image in $(B \otimes_{E_0} E)^{\varphi^n=\pi}$ because $[\pi] = \pi t + t^{p^n} = \varphi^n$ on $\mathcal{O}_{C^\flat}$, and it is an isomorphism of $\mathcal{O}_E$ modules. Now there are commutative diagrams:

$$\begin{array}{ccccc} G_{LT}(\mathcal{O}_{C^\flat}) & \xrightarrow{\sigma} & G_{LT}(A_{\mathrm{inf}} \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E) & \xrightarrow{\log_G} & B \otimes_{E_0} E \\ & & \downarrow & & \downarrow \\ & & G_{LT}(\mathcal{O}_K) & \xrightarrow{\log_G} & K \end{array}$$

The map $G_{LT}(\mathcal{O}_{C^\flat}) \to G_{LT}(\mathcal{O}_K)$ has kernel $\mathcal{O}_E u$ for some u, thus we can let $f = \log_G(\sigma(u))$, then the image of $f \in K$ is 0, which means f has a zero at the point $y \in Y_E^0$. And(17.10.3.13) shows the the zeros of f is just the φ^d-orbit containing y. □

Lubin-Tate Formal Groups and the Proof of the Lemma of Uniformizer

Prop. (17.10.3.10). The ring $B \otimes_{E_0} E$ is an integral domain. ⌟

Proof: Cf.[Lurie P95]. In fact this is the ramified Witt vector, which is by the same reason as before an integral domain, Cf.[FF Curve Johannes]. □

Cor. (17.10.3.11). If $f \neq 0 \in B \otimes_{E_0} E$, then $N_{E/E_0}(f) \neq 0 \in B$, in particular, the vanishing locus of f is finite. ⌟

Cor. (17.10.3.12). If $f, g \in B \otimes_{E_0} E$, then f is divisible by g iff for each $\overline{y} \in Y_E^0$, $\mathrm{ord}_{\overline{y}}(f) \geq \mathrm{ord}_{\overline{y}}(g)$. ⌟

Proof: If $\mathrm{ord}_{\overline{y}}(f) \geq \mathrm{ord}_{\overline{y}}(g)$, suppose $N_{E/E_0}(g) = gh$, then multiplying by h, we can assume $g \in B$. Now f is written uniquely as $f_0 + f_1\pi + \ldots + f_{e-1}\pi^{e-1}$ where $f_k \in B$, thus it suffices to show f_i is divisible by g, which is equivalent to $\mathrm{ord}_y(f) \geq \mathrm{ord}_y(g)$ for each $y \in Y$, by(17.10.1.15). Now if $\mathrm{ord}_y(g) = n$, the hypothesis shows f vanishes in

$$\prod_{\overline{y}\to y} B_{\mathrm{dR}}^+(y)/\xi^n = (B_{\mathrm{dR}}^+(y)/\xi^n) \otimes_{E_0} E = B_{\mathrm{dR}}^+(y)/\xi^n + \pi B_{\mathrm{dR}}^+(y)/\xi^n + \ldots + \pi^{e-1} B_{\mathrm{dR}}^+(y)/\xi^n$$

thus $\mathrm{ord}_y(f) \geq n = \mathrm{ord}_y(g)$. □

Cor. (17.10.3.13). If $f \in (B \otimes_{E_0} E)^{\varphi^n = \pi}$, then the vanishing locus of f is a single φ^d-orbit, and all zeros are simple. ⌟

Proof: Set $N_{E/E_0}(f) = f'$ and $N_{E/E_0}(\pi) = \pi'$, then f belongs to $B^{\varphi^d = \pi'}$, and its divisor is just the image of divisor of f in Y_E^0. So it suffices to show that f' vanishes on a single $\varphi^{d\mathbb{Z}}$-orbit.

Now for $0 < \rho < 1$,

$$\rho^{p^d} |f'|_{\rho^{p^d}} = |\pi' f'|_{\rho^{p^d}} = |f'^{\varphi^d}|_{\rho^{p^d}} = |f'|_\rho^{p^d},$$

thus

$$p^d s + v_{p^d s}(f') = p^d v_s(f')$$

for each $s > 0$, differentiating, we get

$$1 + \partial_- v_s(f') = \partial_- v_s(f')$$

Now the divisor of f' is $\varphi^{d\mathbb{Z}}$-invariant, and it has exactly one zero on any annulus $(\rho^n, \rho]$(17.10.1.19), thus its divisor is a single φ^d-orbit. □

Def. (17.10.3.14) [Universal Lubin-Tate Formal Group]. Recall that if E is a finite extension of Q_p with uniformizer π, for a $\mathcal{O}_E$-algebra A complete w.r.t π, $G_{LT}(A)$ is the Lubin-Tate formal group, with elements the topological nilpotent elements of A3.

Now we define the **universal cover of Lubin-Tate formal group** $\widetilde{GT}$ as the functor

$$A \mapsto \lim\{\cdots \xrightarrow{[\pi]} G_{LT}(A) \xrightarrow{[\pi]} G_{LT}(A)\}.$$

⌟

Prop. (17.10.3.15).

- Notice for K an alg.closed extension of E, $G_{LT}(\mathcal{O}_K)$ is in bijection with $\mathfrak{m}_K$, and the kernel of $[\pi^n]$ on $G_{LT}(\mathcal{O}_K)$ has order $\mathcal{O}_E/\pi^n$, thus the kernel of $\widetilde{G}_{LT}(\mathcal{O}_K) \to G_{LT}(\mathcal{O}_K)$ is a 1-dimensional $\mathcal{O}_E$-module.
- If π vanishes on A and A is perfect, then $[\pi] = \pi t + t^q = t^q$ on A, so it is just the Frobenius, and $\widetilde{G}_{LT}(A) \to G_{LT}(A)$ is a bijection.
- $\widetilde{G}_{LT}(A) \to \widetilde{G}_{LT}(A/I)$ is an isomorphism for $\pi \in I$ and A is I-adic.
- $\widetilde{G}_{LT}(A) \to \widetilde{G}_{LT}(A/I)$ is an isomorphism for any ideal I that $I + (\pi) \neq (1)$, because both of them is isomorphic to $\widetilde{G}_{LT}(A/(I + (\pi))$.

⌟

Proof: For 3, it suffices to prove that $\widetilde{G}_{LT}(A/I^{n+1}) \to \widetilde{G}_{LT}(A/I^n)$ for $n \geq 1$. Notice $F(u,v) \equiv u+v \mod I^{2n}$, so we have an exact sequence

$$0 \to I^n/I^{n+1} \to G_{LT}(A/I^{n+1}) \to G_{LT}(A/I^n) \to 0.$$

In particular the kernel is annihilated by π, so there is a commutative diagram

$$\begin{array}{ccccc} \cdots & \xrightarrow{\pi} & G_{LT}(A/I^{n+1}) & \xrightarrow{\pi} & G_{LT}(A/I^{n+1}) \\ & \nearrow & \downarrow & \nearrow & \downarrow \\ \cdots & \xrightarrow{\pi} & G_{LT}(A/I^{n+1}) & \xrightarrow{\pi} & G_{LT}(A/I^{n+1}) \end{array}$$

which show that $\widetilde{G}_{LT}(A/I^{n+1}) \cong \widetilde{G}_{LT}(A/I^n)$. □

Cor. (17.10.3.16) [Teichmuller Section]. Consider the $\mathcal{O}_E$-algebra $A_{\inf} \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E$. Because there are isomorphism $\mathcal{O}_{E_0}/p \cong \mathcal{O}_E/\pi$, we have an isomorphism

$$C^\flat \cong A_{\inf}/p \cong (A_{\inf} \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E)/\pi$$

Now(17.10.3.15) shows the diagram

$$\begin{array}{ccc} \widetilde{G}_{LT}(A_{\inf} \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E) & \xrightarrow{\cong} & \widetilde{G}_{LT}(\mathcal{O}_{C^\flat}) \\ \downarrow & & \downarrow \cong \\ G_{LT}(A_{\inf} \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E) & \longrightarrow & G_{LT}(\mathcal{O}_{C^\flat}) \end{array}$$

So the lower horizontal map is surjective, and it even has a canonical section σ, called the **Teichmuller section**. ⌟

Cor. (17.10.3.17). Given a point of Y_E^0 which corresponds to an untilt of $C^\flat$ together with a E_0-map $E \to K$, then this gives a commutative diagram

$$\begin{array}{ccc} \widetilde{G}_{LT}(A_{\inf} \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E) & \xrightarrow{\cong} & \widetilde{G}_{LT}(\mathcal{O}_K) \\ \downarrow & & \downarrow \\ G_{LT}(A_{\inf} \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E) & \longrightarrow & G_{LT}(\mathcal{O}_K) \end{array}$$

where the right vertical arrow is surjective with kernel free of rank 1 over $\mathcal{O}_E$. So this together with(17.10.3.16) shows there is a surjection $G_{LT}(\mathcal{O}_{\mathcal{O}_{C^\flat}}) \to G_{LT}(\mathcal{O}_K)$ with kernel a rank-1 $\mathcal{O}_E$-module. ⌟

Prop. (17.10.3.18). There is a canonical $\mathcal{O}_E$-module map

$$G_{LT}(A_{\inf} \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E) \xrightarrow{\log_G} B \otimes_{E_0} E.$$

and it is equivariant w.r.t φ. ⌟

Proof: $G_{LT}(A_{\inf} \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E)$ are in bijection with the maximal ideal of $A_{\inf} \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E$, and $\log_G(x)$ is of the form $x + \frac{c_2}{2}x^2 + \ldots + \frac{c_n}{n}x^n + \ldots$, with $c_n \in \mathcal{O}_E$.

Now for $x \in G_{LT}(A_{\inf} \otimes_{\mathcal{O}_{E_0}} \mathcal{O}_E)$, we show that $\log_G(x)$ converges in $B \otimes_{E_0} E = B + \pi B + \ldots + \pi^{e-1}B$: Let $c_n x^n = \sum a_{n,i}\pi^i$, then we need to show $a_{n,i}/n$ converges to 0 for each of the norm $|\cdot|_\rho$. And this is because if $x = x_0 + \pi y_0$, then for $n \geq em$, $|x|_\rho \leq \max\{|x_0|_\rho^{em}, \rho^m$, which decays exponential in n, and $|\frac{1}{n}|_\rho$ decays linearly in n. □

Prop. (17.10.3.19). The map $\log_G(\sigma(\cdot)) : G_{LT}(\mathcal{O}_{C^\flat}) \to (B \otimes_{E_0} E)^{\varphi^n=\pi}$ as in(17.10.3.9) is an isomorphism. ⌟

Proof: For surjectivity, as any $f \in (B \otimes_{E_0} E)^{\varphi^n=\pi}$ vanishes at a single $\varphi^{d\mathbb{Z}}$-orbit, then by(17.10.3.9) we can find a $\log_G(u)$ that vanishes at the same locus, so $f = \log(u)\lambda$ where λ is a unit in $B \otimes_{E_0} E$(17.10.3.12), so

$$\lambda \in (B \otimes_{E_0} E)^{\varphi^n=\mathrm{id}} = (B \otimes_{\mathbb{Q}_p} E)^{\varphi=\mathrm{id}}(17.10.3.5) = B^{\varphi=\mathrm{id}} \otimes_{\mathbb{Q}_p} E = E.$$

For injectivity, we proved in(17.10.3.9) that each $\log_G(\sigma(u))$ only vanishes at a single φ^d-orbit in Y_E^0, so it cannot by 0, which vanishes at all points. □

Cor. (17.10.3.20). There are canonical bijections

$$\{\text{Closed Points of } X_E\} \cong \{\varphi^{d\mathbb{Z}}\text{orbits of } Y_E^0\} \cong ((B \otimes_{E_0} E)^{\varphi^n=\pi} - \{0\})/E^* \cong (G_{LT}(\mathcal{O}_{C^\flat}) - \{0\}/E^*$$

by(17.10.3.9)(17.10.3.19),(17.10.3.12). ⌟

Vector Bundles and Base Change

Prop. (17.10.3.21) [Vector Bundles on the Cover]. Let $\pi : X_E \to X$ be the covering map, for any vector bundle $\mathcal{E}$ on X_E, $\pi_*(\mathcal{E})$ is a vector bundle on X, and this induces an isomorphism

$$\{X_E\text{-Bundles}\} \cong \{X - \text{Bundles with an } E\text{-action}\}.$$

Now define $\deg(\mathcal{E}) = \deg(\pi_*\mathcal{E})$, and $\mathrm{slope}(\mathcal{E}) = \frac{\deg(\mathcal{E})}{\mathrm{rank}(\mathcal{E})} = \frac{1}{n}\mathrm{slope}(\pi_*\mathcal{E})$.

Then $\mathcal{E}$ is semistable of slope λ iff $\pi_*\mathcal{E}$ is semistable of slope λ/n. ⌟

Proof: One direction is clear, for the other, if $\mathcal{F} = \pi_*\mathcal{E}$ is not semistable, choose its HN-filtration, then $\lambda_1 > \lambda/n$. Now the action of E on $\mathcal{F}$ preserves the HN-filtration, thus $\mathcal{F}_1$ is an E-vector bundle, thus by the correspondence above, $\mathcal{F}_1 = \pi_*\mathcal{E}'$ for some subbundle $\mathcal{E}' \subset \mathcal{E}$, and clearly this contradicts the semistablity of $\mathcal{E}$. □

Cor. (17.10.3.22). For any integral number d, n with $n > 0$, there exists a semistable vector bundle on X with rank n and degree d. ⌟

Proof: Let E be an extension of $\mathbb{Q}_p$ of degree n, then $\pi_*(\mathcal{O}_{X_E}(d))$ is semistable of rank n and degree d, by(17.10.3.1)(6.6.2.23), because $\mathcal{O}_{X_E}(d)$ is a line bundle(17.10.3.8) so clearly semistable, and it is of degree d because **?**. □

Isocrystals and Classification of Semistable Vector Bundle over X

Remark (17.10.3.23). Recall the Dieudonné-Manin Classification(8.8.4.10)(8.8.4.13): Any isocrystal over k is a finite sum of modules pure of slopes λ_i. And if k is alg.closed, then any isocrystal over k has a unique decomposition as sums of E_{λ_i}. ⌟

Prop. (17.10.3.24). Let $k = \overline{\mathbb{F}}_p \in C^\flat$, then there is an inclusion $W(k) \to A_{\mathrm{inf}}$, which extends to a map $K \to B$. Now given an isocrystal V over k, denote $\mathcal{E}_V$ the coherent sheaf on X defined by the graded module $\oplus_{n\geq 0} \mathrm{Hom}_K(V, B)^{\varphi=p^n}$. In other words, on an affine open subscheme $U = D(t)$, $\mathcal{E}_V(U) = \{\varphi - \text{equivariant } K\text{-linear maps } V \to B[\frac{1}{t}]\}$.

And when $V = E_{m/n}$ is the simple isocrystal, then $\mathcal{E}_V$ is denoted by $\mathcal{O}(\frac{m}{n})$. ⌟

Prop. (17.10.3.25). In fact we have $\mathcal{O}(\frac{m}{n})(U) \cong (B[t^{-1}])^{\varphi^n = p^m} = (\rho_* \mathcal{O}(m))(U)$, where $\rho : X_E \to X$, and E is an unramified extension of $\mathbb{Q}_p$. ⌟

Prop. (17.10.3.26) [Classification of Semistable Vector Bundles over X]. For every vector bundle on X, the HN-filtration splits non-canonically, and the construction $V \to \mathcal{E}_V$ induces an equivalence of categories between

$$\{\text{Isoclinic Isocrystals of slope } \mu\}^{\text{op}} \to \{\text{Semistable vector bundles on } X \text{ of slope } \mu\}$$

⌟

Proof: Cf.[FF Curve Johannes].**?** □

Cor. (17.10.3.27). Any two semistable vector bundles of slope λ over X is isomorphic, and a semistable vector bundle of slope 0 is trivial. ⌟

Prop. (17.10.3.28). If $\mathcal{E}, \mathcal{E}'$ be semistable vector bundles on X of slopes μ, μ', then $\mathcal{E} \otimes \mathcal{E}'$ is semistable of slope $\mu + \mu'$. ⌟

Proof: We can assume $\mathcal{E} = \rho_* \mathcal{O}_{X_E}(d)$ for an unramified extension $E/\mathbb{Q}_p$ by(17.10.3.27), and then $\mathcal{E} \otimes \mathcal{E}' = \rho_*(\mathcal{O}_X(d) \otimes \rho^* \mathcal{E}')$. Since ρ_*, ρ^* preserves semistability(by(17.10.3.21) and**?**). So it suffices to prove $\mathcal{O}(d) \otimes -$ preserves semistablity, but this is clear, as $\mathcal{O}(d)$ shifts degree. □

Diamonds Definitions

Def. (17.10.3.29) [Diamond]. Let Perf denote the site of perfectoid spaces of characteristic p equipped with the pro-étale topology. A **diamond** X is a sheaf (of sets) on Perf of the form $X = Hom_{Perf}(,Z)/R$, where $Z \in Perf$ and $R \in Z \times Z$ is a reasonable representable equivalence relation. ⌟

Prop. (17.10.3.30) [Scholze]. Let $\underline{R} = (R, R^+)$ be a Huber pair, then

$$\text{Spd}(\underline{R}) = \mathcal{Z} \mapsto \{\text{untilts of}\text{Spa}(\underline{R}) \text{ over } Z\}$$

is a diamond.

And this construction can be glued to give diamond $X^\diamond$ of any adic space X, which is a sheaf. ⌟

Def. (17.10.3.31) [Adic Fargues-Fontaine Curve]. Let $\mathcal{Y}$ be the adic space $\text{Spa}(A_{\text{inf}})$ removing the vanishing locus of p and $[t]$, then by what we proved, the Frobenius act totally discontinuous on $\mathcal{Y}$, thus the quotient $\mathcal{X}^{FF}$ is an adic space, the FF-curve. ⌟

Prop. (17.10.3.32). There is an isomorphism of diamonds:

$$\mathcal{Y}^\diamond \cong \text{Spd}(C^\flat) \times \text{Spd}(\mathbb{Q}_p), \quad \mathcal{X}^{FF,\diamond} \cong \text{Spd}(C^\flat)/\varphi^{\mathbb{Z}} \times \text{Spd}(\mathbb{Q}_p)$$

More generally, over any Huber pair $\underline{R}$, there is a relative FF-curve which is defined by

$$\text{Spd}(\underline{R}) \times \text{Spd}(\mathbb{Q}_p)/\varphi^{\mathbb{Z}}$$

⌟

Proof: $C^\flat$ is a perfectoid of char$p$, so for a perfect Huber pair, $\underline{S}$ point of $C^\flat$ is just a morphism $u:(C^\flat,\mathcal{O}_{C^\flat}\to(S,S^+)$. And a $\mathbb{Q}_p$ point is just a char0 untilts $\underline{T}$ of $\underline{S}$.

So for each pairs (T,u), we need to find a morphism $A_{\inf}[\frac{1}{p},\frac{1}{[t]}\to T$. For this, consider

$$A_{\inf}=W(\mathcal{O}_{C^\flat})\to W(S^+)\cong W(T^\flat)\xrightarrow{\theta_T}T$$

This is a bijection, as we proved in the beginning(17.11.1.2). □

Prop. (17.10.3.33). There is a morphism of ringed spaces $\mathcal{X}^{FF}\to X^{FF}$ that regard $\mathcal{X}^{FF}$ as the rigid analytification of $\mathcal{X}$, so they have the same category of vector bundles and cohomology, prove by Kedlaya-Liu. ⌟

4 Applications

Prop. (17.10.4.1). The FF curve X is geometrically simply connected, i.e. the projection defines an isomorphism of étale groups $\pi_1(X)\to\pi_1(\operatorname{Spec}\mathbb{Q}_p)=\mathrm{Gal}_{Q_p}$.

Equivalently, the pullback defines an equivalence of étale sites. ⌟

Proof: Let $\widetilde{X}\to X$ be an finite étale morphism, we want to prove that $\widetilde{X}=X\otimes_{\operatorname{Spec}\mathbb{Q}_p}\operatorname{Spec}(E)$ for some étale $\mathbb{Q}_p$-algebra. Let $\mathcal{A}=\rho_*\mathcal{O}_{\widetilde{X}}$, and $E=H^0(X,\mathcal{A})=H^0(\widetilde{X},\mathcal{O}_{\widetilde{X}})$. Now it suffices to show $\mathcal{A}=E\otimes_{\mathbb{Q}_p}\mathcal{O}_X$, which shows $\widetilde{X}=X\otimes_{\operatorname{Spec}\mathbb{Q}_p}\operatorname{Spec}(E)$, and forces E be an étale $\mathbb{Q}_p$-algebra by fpqc descent**?**. Equivalently, $\mathcal{A}$ is trivial, and this is equivalent to $\mathcal{A}$ being semistable of slope 0 by(17.10.3.27).

Because ρ is finite étale, the trace pairing $\mathcal{A}\times\mathcal{A}\to\mathcal{A}\xrightarrow{tr}\mathcal{O}_X$ is non-degenerate(check on stalks), which induces an isomorphism $\mathcal{A}\cong\mathcal{A}^\vee$, so $\deg(\mathcal{A})=0$, and if $\mathcal{A}$ is not semistable, let $\mathcal{A}'$ be the first term of the HN-filtration of $\mathcal{A}$, then it is of slope $\lambda>0$, So $\mathcal{A}'\otimes\mathcal{A}'$ is of slope 2λ by(17.10.3.28), so the composite $\mathcal{A}'\otimes\mathcal{A}'\hookrightarrow\mathcal{A}\otimes\mathcal{A}\to\mathcal{A}$ must by 0(4.3.4.32), which is impossible, because if U is an affine open that $\mathcal{A}$ has a section, then this says $U\otimes_X\widetilde{X}$ has a section s that $s^2=0$. But $U\otimes_X\widetilde{X}$ is reduced(check on stalks). □

Cor. (17.10.4.2).

- The projection map induces equivalence of categories between Finite Abelian groups with $Gal(Q_p)$-action and étale Local system on X.
- If M is a finite Abelian group with a $Gal(\mathbb{Q}_p)$-action, then

  $$H^*(Gal(\mathbb{Q}_p),M)\to H^*_{ét}(X,u^*M)$$

  is an isomorphism for $*=0,1$.

⌟

Proof: 1 is trivial, and 2 Cf. [Lurie P102]. □

5 Weakly Admissible⇒Admissible

Def. (17.10.5.1) [Notations]. Let K be a finite extension of $\mathbb{Q}_p$, and $K_0=W(k)[\frac{1}{p}]$ be the maximal unramified subextension in K, let $C=\widehat{\overline{K}}$ and $F=C^\flat$. Denote by $\infty\in X$ the closed point determined by C, which is just the vanishing locus of the Galois stable line $\mathbb{Q}_pt$, where $t=\log([\varepsilon])$ and $\varepsilon=(1,\xi_p,\xi_{p^2},\dots)\in C^\flat$(17.10.1.36).

Notice G_K acts on $\mathbb{Q}_p\log([\varepsilon])$ by the cyclotomic character χ_{cycl}. Recall

$$B_{\mathrm{dR}}^+=\widehat{\mathcal{O}}_X(\infty),\quad B_{\mathrm{crys}}^+,\quad B_{\mathrm{crys}}=B_{\mathrm{crys}}^+[t^{-1}],\quad B_e=H^0(X-\{\infty\},\mathcal{O}_X)=(B_{crys})^{\varphi=\mathrm{id}}$$

⌟

Def. (17.10.5.2) [Equivariant Action of G_K on Vector Bundles]. Recall an equivariant action of G_K on a bundle $\mathcal{E}$ on X is a data of isomorphisms $\sigma^*(\mathcal{E})\cong E$ that $c_{\sigma\tau}=c_\tau\circ\tau^*(c_\sigma)$. Notice any equivariant action of G_K on $\mathcal{E}$ induces a semilinear G_K action on $\mathcal{E}_\infty^\wedge=\mathcal{E}\otimes_{\mathcal{O}_X}B_{\mathrm{dR}}^+$, and here we require this action is continuous. The category of equivariant G_K-bundles are denoted by $Bun_X^{G_K}$. ⌟

Cor. (17.10.5.3). By the slope 0 case of the classification of vector bundles on X(17.10.3.26) and(18.4.5.1), we see that the functor:

$$\mathrm{Rep}_{\mathbb{Q}_p}G_K\to\mathrm{Bun}_X^{G_K}:V\mapsto V\otimes_{\mathbb{Q}_p}\mathcal{O}_X$$

is fully faithful with essential image the category $\mathrm{Bun}_X^{G_K,sst,0}$ of all G_K vector bundles on X that the underlying bundle is semistable of slope 0, i.e. trivial(17.10.3.27). ⌟

Prop. (17.10.5.4). There is a pullback diagram of categories:

$$\begin{array}{ccc}\varphi-FilMod_{K/K_0} & \longrightarrow & \varphi-Mod_{K_0}\\ \downarrow{\scriptstyle\mathcal{E}(-)} & & \downarrow{\scriptstyle\mathcal{V}}\\ \mathrm{Bun}_X^{G_K} & \longrightarrow & \mathrm{Rep}_{B_e}G_K\end{array}$$

Where $\mathcal{E}(-)$ maps a φ-filtered module (D,φ_D,Fil) to the bundle that is the bundle $\widetilde{(D,\varphi_D)}$ modified so that the fiber at ∞ is $Fil^0(D_K\otimes_K B_{\mathrm{dR}})$. ⌟

Proof: 1: By lemma(18.4.4.9), $\varphi-FilMod_{K/K_0}$ is equivalent to a φ-module V with a G_K-stable B_{dR}^+-lattice in $(V\otimes_{K_0}K)\otimes_K B_{\mathrm{dR}}^+=V\otimes_{K_0}B_{\mathrm{dR}}^+$.

2: By(18.4.6.5), φ-Mod is a full subcategory of $\mathrm{Rep}_{B_e}G_K$, where the G_K-stable B_{dR}^+-lattice is choose to be $V\otimes_{K_0}B_{\mathrm{dR}}^+$.

3: Clearly there is a functor

$$Bun_X^{G_K}\to\mathrm{Rep}_{B_e}G_K:\mathcal{E}\to H^0(X-\{\infty\},\mathcal{E}).$$

, and(6.4.2.15) says in this case $Bun_X^{G_K}$ is equivalent to a B_e-module with continuous G_K-actions and and a B_{dR}^+-module with continuous G_K-actions that they corresponds as a B_{dR}-module with continuous G_K-actions.

4: The compatibility in 3 just says that the B_{dR}^+-lattice choosen in the definition of(18.4.4.11) just comes from that of 2, so this diagram is clearly a pullback. □

Lemma (17.10.5.5). Let $FilV\in VectFil_K$ and $W=Fil(V\otimes_K B_{\mathrm{dR}})$, if $V\otimes B_{\mathrm{dR}}^+=\{e_1,\ldots,e_n\}$ and $Fil^0(V\otimes_K B_{\mathrm{dR}})=\{t^{-a_1}e_1,\ldots,t^{-a_n}e_n\}$, then the Hodge polygon of $FilV$ has slopes $(a_1,\ldots,a_n)$. ⌟

Proof: Use(18.4.4.9), notice $(t^aB_{\mathrm{dR}}^+)^{G_K}=0$ for $a>0$, as in the proof of(18.4.4.8). □

Lemma (17.10.5.6). The functor

$$\mathcal{E}(-) : \varphi - FilMod_{K/K_0} \to Bun_X^{G_K}$$

defined in(17.10.5.4) preserves degree and HN-filtration, where the HN-filtration on the RHS is induces by the HN-filtration on Bun_X by canonicity. ⌟

Proof: $\deg(\mathcal{E}((D,\varphi_D,Fil)) = \deg(\mathcal{E}(D,\varphi_D)) - \dim_K[D\otimes_{K_0} B_{\mathrm{dR}}^+ : Fil^0(D_K \otimes_K B_{\mathrm{dR}})]$ $= \deg(D_K, Fil) - \deg(D,\varphi_D)$.

Now the degree correspond, for the invariance of HN-filtration, it suffices to prove the subobjects are in bijection: Given a subobjects of $\mathcal{E}(V)$, we want to show it is a $\mathcal{E}(V')$, but this is because on the affine open $\mathrm{Spec}(B_e)$, by(18.4.6.5) any subbundle is also crysatalline, i.e. comes from $\varphi - Mod_{K_0}$. □

Prop. (17.10.5.7) [Weakly Admissible implies Admissible]. The category of crystalline Galois representations of G_K is equivalent to the category $\varphi - FilMod_{K/K_0}^{wa}$ of weakly admissible filtered φ-modules for K. ⌟

Proof: By definition of weakly admissible and(17.10.5.6), there is a pullback diagram

$$\begin{array}{ccc} \varphi - FilMod_{K/K_0}^{wa} & \longrightarrow & \varphi - FilMod_{K/K_0} \\ \downarrow & & \downarrow \mathcal{E}(-) \\ \mathrm{Rep}_{\mathbb{Q}_p} G_K \cong Bun_X^{G_K,sst,0} & \longrightarrow & Bun_X^{G_K} \end{array}$$

Adjunction with(17.10.5.4), we get another pullback diagram

$$\begin{array}{ccccc} \varphi - FilMod_{K/K_0}^{wa} & \longrightarrow & \varphi - FilMod_{K/K_0} & \longrightarrow & \varphi - Mod_{K_0} \\ \downarrow & & \downarrow \mathcal{E}(-) & & \downarrow \mathcal{V} \\ \mathrm{Rep}_{\mathbb{Q}_p} G_K \cong Bun_X^{G_K,sst,0} & \longrightarrow & Bun_X^{G_K} & \longrightarrow & \mathrm{Rep}_{B_e} G_K \end{array}$$

But this pullback is just the category of crystalline representations: by(17.10.5.3), for $V \in \mathrm{Rep}_{\mathbb{Q}_p} G_K$, the condition $\mathcal{V}(\mathcal{D})(M) \cong M$ in(18.4.6.5) is just saying that V is in the image of $\mathcal{V}$ iff

$$(V \otimes_{\mathbb{Q}_p} B_{crys})^{\varphi=\mathrm{id}} \otimes_{B_e} B_{crys} \cong V \otimes_{\mathbb{Q}_p} B_{crys}$$

which is equivalent to V being crystalline. □

17.11 p-adic Hodge Theory

Main references are [Berger, Galois representations and (φ, Γ)-modules], [Car19]. and [notes on p-adic Hodge, Conrad]. [notes on p-adic Hodge, Serin Hong].

Notation (17.11.0.1).

- Use notations from p-adic Local Galois Representations.

⌟

1 Fontaine's Period Rings

Fontaine's Ring A_{inf}

Def. (17.11.1.1) [Fontaine's Ring A_{inf}]. Let $C^\flat$ be a perfectoid field of characteristic p, for any untilt K of $C^\flat$, the Fontaine's ring $A_{\text{inf}} = A_{\text{inf}}(\mathcal{O}_K)$ is defined to be the ring of Witt vectors $W(\mathcal{O}_{C^\flat})$(5.5.1.15). Also denote $B_{\text{inf}} = A_{\text{inf}}[\frac{1}{p}]$.

the set of all the char0 untilts K of $C^\flat$ is denoted by Y. and $Y_{[a,b]}$ denotes those untilts that $a \le |p|_K \le b$. ⌟

Prop. (17.11.1.2). By(11.2.9.7), if $K \in \mathcal{P}\text{erfd}^0 \cap \texttt{Field}^0$, with tilt $C^\flat$, then there is a diagram

$$\begin{array}{ccc} A_{\text{inf}} & \xrightarrow{\theta} & \mathcal{O}_K \\ \downarrow & & \downarrow \\ \mathcal{O}_{C^\flat} & \xrightarrow{\bar{\sharp}} & \mathcal{O}_K/(p) \end{array}.$$

Then θ is surjective, and $\ker\theta$ is generated by some distinguished element $\xi = [t] - pu$ where $u \in A_{\text{inf}}$ is invertible. Moreover, any distinguished element in the kernel is a generator. ⌟

Proof: θ is surjective by(5.5.1.16). By(11.2.8.11), there exists $t \in A_{\text{inf}}$ s.t. $t^\sharp = pu'$ for some u' invertible in $\mathcal{O}_K$. Thus $u' = \theta(u)$ for some invertible $u \in A_{\text{inf}}$, then $\theta([t] - pu) = 0$. And ξ generates the kernel because it generates after modulo ϖ, and and use the fact $\mathcal{O}_K$ is p-complete.

For the last assertion, use(17.11.1.4), which shows that if ξ' is another distinguished element in $\ker\theta$, $A_{\text{inf}}/(\xi')$ is an integral domain of dimension 1. So $(\xi) = (\xi')$ as $\mathcal{O}_K$ is not a field. □

Lemma (17.11.1.3). If $R \in \mathcal{CR}\text{ing}$, $x, y \in R$, and $x \in R^\times$ and R is x-adically complete Hausdorff, and y is not a zero-divisor in R/x and R/x is y-adically complete Hausdorff, then the same is true with x, y interchanged. ⌟

Proof: ? □

Prop. (17.11.1.4) [Untilts and Distinguished Elements]. (17.11.1.2) shows that for any untilt K of $C^\flat$, the kernel is generated by a distinguished element. Conversely, for any distinguished element ξ, $A_{\text{inf}}/(\xi)$ can be identified with the valuation ring $\mathcal{O}_K$ of a perfectoid field K. and

$$\mathcal{O}_C^\flat = A_{\text{inf}}/p \to A_{\text{inf}}/(\xi, p) \cong \mathcal{O}_K/p$$

exhibits K as an untilt of $C^\flat$. ⌟

Proof: May assume $\xi = [t] - up$ and $t \neq 0$. Consider the mapping $\theta : A_{\text{inf}} \to A_{\text{inf}}/(\xi) = \mathcal{O}_K$, and denote $\theta([x])$ by $x^\sharp$.

Firstly, we can apply lemma(17.11.1.3) to ξ and p to conclude that A_{inf} is ξ-complete and ξ-torsion-free, and $\mathcal{O}_K$ is p-adically complete and p-torsion-free.

Now for any $y \in \mathcal{O}_K$ is p-adically complete, there is a $x \in \mathcal{O}_C^\flat$ that $(y) = (x^\sharp)$: multiplying p-power, we can assume y is not divisible by p, and there is a x that $y \equiv x^\sharp \mod p$, thus x is not divisible by t. Now $t = xx'$ for some $x' \in \mathfrak{m}_C^\flat$, thus $y = x^\sharp + t^\sharp w = x^\sharp(1 + x'w)$, and $1 + x'w$ is invertible in $\mathcal{O}_K$.

Next we prove $\mathcal{O}_K$ is an integral domain: It suffices to show any $y \neq 0 \in \mathcal{O}_K$ is not a zero-divisor. We can assume $y = x^\sharp$, by what just proved, and then x divides t^n for some n, so it suffices to consider $y = t^{n\sharp} = p^n$, and p^n is not a zero-divisor by what just proved.

Now we can endow $\mathcal{O}_K$ with the valuation $|y| = |x|_{C^\flat}$ for $y = x^\sharp u$, and extend it to the quotient field K. Then this is a Non-Archimedean valuation and the residue field has char p because $|p| < 1$, and K has char0, because $p \neq 0$ in K. And it is p-adically complete.

Finally, $\mathcal{O}_K/p\mathcal{O}_K \cong A_{\text{inf}}/(\xi, p) = \mathcal{O}_{C^\flat}/\pi$, so the Frobenius is surjective, thus $K = K(\mathcal{O}_K)$ is a perfectoid field. □

Cor. (17.11.1.5). The correspondence $\xi \mapsto \text{Frac}(A_{\text{inf}}/(\xi))$ induces a bijection

$$\{\text{Distinguished elements}\}/\text{units} \cong \{\text{Untilts of } C^\flat\}/\text{isomorphisms}.$$

⌟

Prop. (17.11.1.6)[A_{inf} as Holomorphic Function in p]. Any element in A_{inf} can be written uniquely as a unique Teichmuller representation $[c_0] + [c_1]p + [c_2]p^2 + \ldots +$. Now we can regard these elements as holomorphic functions on $B(0,1)$, and any untilts K of $\mathcal{O}_{C^\flat}$ can be regarded as points in $B(0,1)$, where A_{inf} take value $c_0^\sharp + c_1^\sharp p + \ldots \in \mathcal{O}_K$ at the point K.

This map can in fact be extended to $A_{\text{inf}}[\frac{1}{[t]}, \frac{1}{p}]$ s.t.

$$A_{\text{inf}} \hookrightarrow A_{\text{inf}}[\frac{1}{[t]}] \hookrightarrow A_{\text{inf}}[\frac{1}{[t]}, \frac{1}{p}] \to K.$$

called the **evaluation map**. ⌟

Fontain's Ring B

Def. (17.11.1.7) [Fontaine's Ring B]. If compared to the complex case, the elements of A_{inf} are just elements $\sum a_n z^n$ that $|a_n| \leq 1$, this are not all the holomorphic functions on $B(0,1)$, which is

$$\{\sum_{n\in\mathbb{Z}} a_n z^n | \limsup_{n>0} |a_n| \leq 1, \quad \lim_{n\to\infty} |a_{-n}|^{1/n} = 0\}.$$

This leads to a enlargement of A_{inf}:

For $0 < a \leq b < 1$ in the value group of $C^\flat$, $\pi_a, \pi_b \in C^\flat$ with $|\pi_a| = a, |\pi_b| = b$, define

$$B_{[a,b]} = A_{\text{inf}}[\frac{[\pi_a]}{p}, \frac{p}{[\pi_b]}]^\wedge[p^{-1}],$$

this is definable at any untilts K that $a \leq |p|_K \leq b$.

Then $B_{[a,b]}$ is an algebra over $A_{\text{inf}}[\frac{1}{[t]}, \frac{1}{p}]$, and define $B = \varprojlim B_{[a,b]}$. ⌟

Prop. (17.11.1.8) [Gauss Norm]. Any element f in $A_{\inf}[\frac{1}{[t]}, \frac{1}{p}]$ is of the form $\sum_{n>>-\infty}[c_n]p^n$, where $\{|c_n|\}$ is bounded. So we can define the valuation $|f|_\rho = \sup\{|c_n|\rho^n\}$, it is realizable by some term $|a_n|\rho^n$. Notice that for an until $y = (K, \iota)$, if $\rho = |p|_K$, then $|f(y)| \leq |f|_\rho$.

Then this is a non-Archimedean valuation on $A_{\inf}[\frac{1}{[t]}, \frac{1}{p}]$. ⌟

Proof: Firstly $|f+g|_\rho \leq \max\{|f|_\rho, |g|_\rho\}$ for every ρ that is generic for $f+g$ and in the value group of $C^\flat$: In this case,

$$|f+g|_\rho = |(f+g)(y)| \leq \max\{|f(y)|, |g(y)|\} \leq \max\{|f|_\rho, |g|_\rho\}$$

for some point y by(17.11.1.8), then by continuity and(17.11.1.9), this is true for any ρ.

The same method shows that $|f|_\rho|g|_\rho = |fg|_\rho$. □

Lemma (17.11.1.9) [Generic Norms]. ρ is called **generic** for f iff the valuation is realized exactly once. Notice if ρ is generic for f and in the value group of $C^\flat$, then $|f|_\rho = |f(y)|$ for some y(Choose $K = A_{\inf}/([c]-p)$ where $|c|_{C^\flat} = \rho$).

For any f, the numbers ρ that ρ is not generic for f is discrete in ρ. ⌟

Proof: Consider the Newton polygon of f, then only the slopes of the Newton polygon are not generic. □

Lemma (17.11.1.10). If $y = (K, \iota) \in Y$ and $|p|_K = \rho$, then $|f(y)| \leq |f|_\rho$, and equality holds if either ρ is generic or f is invertible. ⌟

Prop. (17.11.1.11) [Valuation Map]. For $0 < a \leq b < 1$ in the value group of $C^\flat$, $|\pi_a| = a, |\pi_b| = b$,

$$A_{\inf}[\frac{[\pi_a]}{p}, \frac{p}{[\pi_b]}] = \{f \in A_{\inf}[\frac{1}{[t]}, \frac{1}{p}] | |f|_a \leq 1, |f|_b \leq 1\} = V_0,$$

Thus the ring $B_{[a,b]}$ is identified with the completion of $A_{\inf}[\frac{1}{[t]}, \frac{1}{p}]$ w.r.t the valuation $|\cdot|_a + |\cdot|_b$(14.2.4.4). In particular, for any point y that $a \leq |p|_K \leq b$, the valuation map(17.11.1.6) can be extended to a map

$$B_{[a,b]} \to K.$$

⌟

Proof: Notice V_0 is a subring by(17.11.1.8), so clearly $A_{\inf}[\frac{[\pi_a]}{p}, \frac{p}{[\pi_b]}] \subset V_0$.

For the reverse containment, notice that $\{|c_n|\}$ is bounded, so there is an m that $\pi_b^m c_n \in C^\flat$ for any n. Now

$$f = \sum_{n<m}[c_n]p^n + (\sum_{n\geq 0}[c_{n+m}\pi_b^m]p^n)(\frac{p}{[\pi_b]})^m,$$

so it suffices to prove the case f has finite presentation. Now $c_n\pi_a^n, c_n\pi_b^n \in \mathcal{O}_C^\flat$, thus $[c_n]p^n = [c_n\pi_a^n](\frac{\pi_n}{p})^{-n} = [c_n\pi_b^n](\frac{p}{\pi_b})^n \in A_{\inf}[\frac{[\pi_a]}{p}, \frac{p}{[\pi_b]}]$, where $n \geq 0$ or $n \leq 0$. Thus the inverse containment is true. □

Prop. (17.11.1.12) [Topology of B]. For $0 < a \leq c \leq b < 1$, $|f|_c \leq \max\{|f|_a, |f|_b\}$(trivial), thus the Fontaine's ring B can be realized as the completion of $A_{\inf}$ w.r.t. all these norms, and endowed with the topology of p-adic Fréchet space. ⌟

Proof: Cf.[Conrad, P65].? □

Prop. (17.11.1.13) [Teichmuller Expansion]. An infinite sum $f = \sum [a_n]p^n$ converges in B iff it converges in any norm $|\cdot|_\rho$ for $0 < \rho < 1$, which is equivalent to

$$\limsup_{n>0} |c_n|_{C^\flat}^{1/n} \le 1, \quad \lim_{n\to\infty} |c_{-n}|_{C^\flat}^{1/n} = 0.$$

This is analogous to the complex case(11.4.3.4). However, for now, we don't know iff every element of B is of this form, and whether the representation is unique?. ⌟

Prop. (17.11.1.14) [Frobenius Action]. Notice the Frobenius action of $C^\flat$ extends to a Frobenius action on the Witt victor $A_{\inf}$, and it satisfies

$$|\varphi(f)|_{\rho^p} = (|f|_\rho)^p,$$

Thus induces an isomorphism $B_{[a,b]} \cong B_{[a^p,b^p]}$. Passing to the limit, we get an automorphism of B, denoted also by φ. ⌟

the Field B_{dR}

Prop. (17.11.1.15)[Untilts with Roots of Unity]. Let $\mathbb{Q}_p^{\mathrm{cycl}} = \mathbb{Q}_p(\mu_{p^\infty})^\wedge$, and $\varepsilon = (1, \mu_p, \mu_{p^2}, \ldots)$ be a compatible p^n-th roots of unity that is an element of $(\mathbb{Q}_p^{\mathrm{cycl}})^\flat$. Then $\varepsilon - 1$ is a pseudo-uniformizer of $(\mathbb{Q}_p^{cyc})^\flat$, For any untilts K of $\mathbb{C}^\flat$ and an embedding of $\mathbb{Q}_p^{\mathrm{cycl}}$ in K, the tilting maps $\varepsilon - 1$ to a pseudo-uniformizer of $\mathbb{C}^\flat$. This induces a bijection:

$$\{\text{Untilts } (K,\iota) \text{ of } C^\flat \text{ with an embedding } \mathbb{Q}_p^{\mathrm{cycl}} \hookrightarrow K\} \cong \{x \in \mathbb{C}^\flat | 0 < |x-1| < 1\}.$$

⌟

Proof: In fact, the left hand side is equivalent to K has a compatible p^n-th roots of unity, and we want to prove that for any x in the right hand side, there is a unique untilts K that $(x^{\frac{1}{p^k}})^\sharp$ is a compatible primitive roots of unity, and this is equivalent to $(x^{\frac{1}{p}})^\sharp$ satisfies $1 + x + \ldots + x^{p-1} = 0$, and further equivalent to $\theta : A_{\inf} \to \mathcal{O}_K$ annhilalates $1 + [x^{\frac{1}{p}}] + \ldots + [x^{\frac{p-1}{p}}]$.

It suffices to show $\xi = 1 + [x^{\frac{1}{p}}] + \ldots + [x^{\frac{p-1}{p}}]$ is distinguished(17.11.1.5). Let $\xi = \sum [c_n]p^n$, consider reducing to the residue field: $W(\mathcal{O}_{C^\flat}) \to W(\mathcal{O}_{C^\flat}/\mathfrak{m}_{C^\flat})$, then $\overline{x} = 1$, and $\overline{\xi} = p$, thus $|c_0| < 1, |c_1 - 1| < 1$, so it is distinguished(5.5.4.20). □

Cor. (17.11.1.16). Considering different p^n-th roots of unities, there is a correspondence:

$$\{\text{Char 0 Untilts } (K,\iota) \text{ of } C^\flat \text{ with a compatible } p^n\text{-th roots of unity}\} \cong \{x \in \mathbb{C}^\flat | 0 < |x-1| < 1\}/\mathbb{Z}_p^*.$$

where $\mathbb{Z}_p^*$ acts by exponentiation(11.2.8.8).

Furthermore, there is a correspondence:

$$\{\text{Char 0 Untilts } (K,\iota) \text{ of } C^\flat \text{ with a compatible } p^n\text{-th roots of unity}\}/\varphi_{C^\flat}^{\mathbb{Z}} \cong \{x \in \mathbb{C}^\flat | 0 < |x-1| < 1\}/\mathbb{Q}_p^*.$$

where the inverse is given by $x \mapsto$ the vanishing locus of $\log([x]) \in B$. ⌟

Proof: The only thing needed to be proven is the inverse is given by $N(\log([x]))$. Notice for any untilts K, $|(x^{p^n})\sharp - 1| < |p|_K^{1/(p-1)}$ for n large, then $\log((x^{p^n})\sharp) = 0$ iff $(x^{p^n})\sharp = 1$ by Newton polygon. Now $x^\sharp \ne 1$ because $x \ne 1$ and $\sharp$ is injective. Hence composing φ^n for some unique n, we can assume $x^\sharp = 1, x^{\frac{1}{p}} \ne 1$, thus it corresponds an untilt as in(17.11.1.15). □

Def. (17.11.1.17) [B_{dR}^+]**.** p is not a zero-divisor in $A_{\inf}/(\xi^n)$, as in the proof pf(17.11.1.4), so we can define
$$B_{\mathrm{dR}}^+ = \varprojlim_n A_{\inf}/(\xi^n)[\frac{1}{p}]$$
⌟

Prop. (17.11.1.18)[Fontaine's Ring B_{dR}]. B_{dR}^+ is a CDVR with ξ a uniformizer and the residue field K. Hence we can define $B_{\mathrm{dR}} = \mathrm{Frac}(B_{\mathrm{dR}}^+)$. ⌟

Proof: Firstly ξ is not a zero divisor in B_{dR}^+, because if $\xi x = 0, x = (x_n)$, then for any $n > 0$, and some k that $p^k x_n \in A_{\inf}/(\xi^n)$, so $p^k x_n$ is annihilated by ξ in $A_{\inf}/(\xi^n)$, thus $p^k x_n = \xi^{n-1} y_n$ for some y_n, because ξ is a non-zero-divisor in $A_{\inf}$(17.11.1.4). So $p^{n-1} x_{n-1} = 0 \in A_{\inf}/(\xi^n)$, thus $x_{n-1} = 0$, because p is non-zero-divisor in $A_{\inf}/(\xi^n)$(17.11.1.4).

Next there is a map $B_{\mathrm{dR}}^+/(\xi^m) \to A_{\inf}/(\xi^m)[p^{-1}]$. This is an isomorphism: it is clearly a surjection, and if $x = (x_n)$ is mapped to 0, then for each $n \geq m$, we choose $p^{k(n)} x_n = 0 \in A_{\inf}/(\xi^n)$, then $p^{k(n)} x_n = \xi^m y_n$ for a unique $y_n \in A_{\inf}/(\xi^{n-m})$. So $x = \xi^m \cdot (\frac{y_n}{p^{k(n)}}) \in \xi^m B_{\mathrm{dR}}$.(Notice the uniqueness of y_n shows $(\frac{y_n}{p^{k(n)}})$ is an element in B_{dR}^+).

Then it follows $B_{\mathrm{dR}}^+ \cong \varprojlim_m B_{\mathrm{dR}}^+/(\xi^m)$, which shows that B_{dR}^+ is ξ-adically complete, and $m = 1$ shows the residue field is equal to K. □

Remark (17.11.1.19). $A_{\inf}/(\xi^n)[\frac{1}{p}] = A_{\inf}/(\xi^n)[\frac{1}{[t]}]$, so if $\mathrm{char}\, k = p$, then B_{dR}^+ is just $W(C^\flat)$.

Thus B_{dR}^+ should be thought as the completed local ring at the point $y = (K, \iota)$. ⌟

Prop. (17.11.1.20)[Topology on B_{dR}]. The Gauss norms give $A_{\inf}$ a topology, giving B_{dR} a topology. Then B_{dR} is complete in this topology, and $B_{\mathrm{dR}} \to K$ is continuous.

With this topology, B_{dR} is abstractly isomorphic to $\mathbb{C}_p((T))$, but not topological isomorphic to it. ⌟

Proof: Cf.[Conrad, P65] or [p-adic Period Rings]P42.?

B_{dR} is abstractly isomorphic to $\mathbb{C}_p((T))$ by Cohn structure theorem?, but [Colmez, Une construction de BdR] proved that $\overline{K}$ is dense in B_{dR}, so it cannot by topological isomorphic to $\mathbb{C}_p((T))$. □

Prop. (17.11.1.21) [The Stalk Map]. Notice $A_{\inf} = \varprojlim_n A_{\inf}/(\xi^n)$ as ξ is distinguished, thus there is a natural injection $A_{\inf} \to B_{\mathrm{dR}}^+$, whose composition with $B_{\mathrm{dR}}^+ \to B_{\mathrm{dR}}^+/\xi \cong K$ maps $p, [t]$ to $p, t^\sharp$, which shows $p, [t]$ are invertible in B_{dR}^+, so there is a map
$$e : A_{\inf}[\frac{1}{p}, \frac{1}{[t]}] \to B_{\mathrm{dR}}^+.$$
In case $a \leq |p|_K \leq b$, this can be further extended to a map $e : B_{[a,b]} \to B_{\mathrm{dR}}^+$(The stalk map). ⌟

Proof: It suffices to prove for $a = |p|_K = b$ because the topology is stronger. In this case, choose $t = p^\flat \in C^\flat$, then $|t|_{C^\flat} = |p|_K$, thus $\overline{e}_n$ determined a map
$$A_{\inf}[\frac{[t]}{p}, \frac{p}{[t]}] \to B_{\mathrm{dR}}^+/(\xi^n) \cong (A_{\inf}/\xi^n)[p^{-1}],$$
It suffices to prove the image is contained in $p^{-k}(A_{\inf}/\xi^n)$ for some $k = k(n)$, because then $\overline{e}_n$ is p-adically continuous, and extends to map of $B_{[a]} = (A_{\inf}[\frac{[t]}{p}, \frac{p}{[t]}])\widehat{\ }_p \to (A_{\inf}/(\xi^n))[p^{-1}]$, which is compatible w.r.t n, thus gives a map $B_{[a]} \to B_{\mathrm{dR}}^+$.

For this, consider $f=\overline{e}_n(\frac{[t]}{p}), g=\overline{e}_n(\frac{p}{[t]})$, then their reduction under $B_{\mathrm{dR}}^+/(\xi^n)\to B_{\mathrm{dR}}^+/\xi\cong K$ is in $\mathcal{O}_K\cong A_{\mathrm{inf}}/(\xi)$, thus

$$f=f_1+\frac{\xi}{p^c}f_2,\quad g=g_1+\frac{\xi}{p^c}g_2$$

for $f_1,f_2,g_1,g_2\in A_{\mathrm{inf}}/(\xi^n)$ for some c. Then any

$$f^m=(f_1+\frac{\xi}{p^c}f_2)^m=\sum_{i=0}^{n-1}C_m^i f_1^{m-i}(\frac{\xi}{p^c}f_2)^i\in p^{-nc}(A_{\mathrm{inf}}/(\xi^n)).$$

Thus $\overline{e}_n(A_{\mathrm{inf}}[\frac{[t]}{p},\frac{p}{[t]}])\in p^{-nc}(A_{\mathrm{inf}}/(\xi^n))$. □

Cor. (17.11.1.22). The stalk map $e:B_{[a,b]}\to B_{\mathrm{dR}}^+$ composed with the map $B_{\mathrm{dR}}^+/(\xi)\cong K$ are in fact equivalent to the valuation map(17.11.1.11). ⌟

$\underline{B_{\mathrm{crys}}}$

Cf.[Notes on p-adic Hodge, Serin Hong].

Def. (17.11.1.23) [B_{crys}]. ⌟

$\underline{B_{\mathrm{st}}, B_e}$

2 C_{dR}-Theorem

Thm. (17.11.2.1) [C_{dR}, Faltings/Tsuji]. If $X\in\mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}/K$, then for any $r\in\mathbb{N}$, there exists a canonical isomorphism

$$\gamma_{\mathrm{dR}}(X):B_{\mathrm{dR}}\otimes_K H_{\mathrm{dR}}^r(X/K)\cong B_{\mathrm{dR}}\otimes_{\mathbb{Q}_p}\mathrm{H}_{\text{ét}}^r(X_{\overline{K}},\mathbb{Q}_p).$$

which identifies filtrations and Gal_K-actions on both sides. Moreover γ_{dR} is functorial in X. ⌟

Proof: Cf.[Faltings, p-adic Hodge Theory]. or [p-adic Hodge for Rigid Analytic Varieties, Scholze], [BMS18]P104. □

Cor. (17.11.2.2) [deRham Comparison for Étale Cohomologies]. $\mathrm{H}_{\text{ét}}^r(X_{\overline{K}},\mathbb{Q}_p)\in\mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{dR}}(\mathrm{Gal}_K)$, and

$$H_{\mathrm{dR}}^r(X)\cong D_{B_{\mathrm{dR}}}(\mathrm{H}_{\text{ét}}^r(X_{\overline{K}};\mathbb{Q}_p)),\quad H^{n-p}(X;\Omega_X^p)\cong\mathrm{gr}^p H_{\mathrm{dR}}^r(X).$$

Also by taking the gradation of(17.11.2.1), by(18.4.5.5), there is a Hodge-like decomposition

$$\mathbb{C}_K\otimes_{\mathbb{Q}_p}\mathrm{H}_{\text{ét}}^r(X_{\overline{K}},\mathbb{Q}_p)\cong\bigoplus_{a+b=r}\mathbb{C}_K(-a)\otimes_K H^b(X,\Omega_X^a).$$

This shows we can recover the de Rham cohomology of X from the étale cohomology, and the Hodge-Tate weights of $\mathrm{H}_{\text{ét}}^r(X_{\overline{K}},\mathbb{Q}_p)$ lies in in $[-r,0]$. ⌟

Remark (17.11.2.3). Is this true for non-proper varieties with logarithmic poles? ⌟

Example (17.11.2.4) [Elliptic Curve Case, Tensoring $\mathbb{C}_K$ Lost Informations]. For $E \in \mathcal{E}\mathrm{ll}/K$ with multiplicative reduction and $j(E) > 1$, by(15.11.5.13) and(15.11.5.10),

$$E(\overline{K}) \cong \overline{K}^{\times}/q^{\mathbb{Z}}$$

as Gal_K-representations for some $q \in K^{\times}$. Thus $T_p(E) \cong q^{\mathbb{Q}_p/\mathbb{Z}_p}$ and there exists an exact sequence

$$0 \to \mathbb{Z}_p(1) \to T_p(E) \to \mathbb{Z}_p \to 0.$$

Then this sequence doesn't split when tensoring $\overline{K}$, but split when tensoring $\mathbb{C}_K$, by(17.11.3.3). ⌟

Proof: Suppose it splits ofter tensoring $\overline{K}$, then it splits after tensoring some finite extension K'. Then by projection of K' onto $\mathbb{Q}$, we see

$$0 \to \mathbb{Q}_p(1) \to V_p(E) \to \mathbb{Q}_p \to 0$$

is splitting as a $\mathrm{Gal}_{K'}$-representations. But this is not true, as any system of roots of p □

C_{dR}-theorem(17.11.2.1) implies any representation of Gal_K of the form $\mathrm{H}^r_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is deRham, thus it is natural to consider the converse:

3 C_{crys}-Theorem

Thm. (17.11.3.1) [Hyodo-Kato Isomorphism]. If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{sm},proper}/K$ has good reduction $\mathcal{X}/\mathcal{O}_K$, let $\overline{\mathcal{X}} = \mathcal{X}_k$, then for any $r \in \mathbb{N}$, $H^r_{\mathrm{crys}}(\overline{\mathcal{X}}) \in \varphi\text{-}\mathcal{M}\mathrm{od}_{W(k)}$, and there is an isomorphism

$$K \otimes_{W(k)} H_{\mathrm{crys}}(\overline{\mathcal{X}}) \cong H^r_{\mathrm{dR}}(X).$$

Then this isomorphism descends $H^r_{\mathrm{dR}}(X)$ to K_0, and this K_0-structure is independent of the smooth model $\mathcal{X}/\mathcal{O}_K$. ⌟

Proof: □

Thm. (17.11.3.2) [C_{crys}, Faltings]. If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{sm},proper}/K$ has good reduction $\mathcal{X}/\mathcal{O}_K$, let $\overline{\mathcal{X}} = \mathcal{X}_k$, then for any $r \in \mathbb{N}$, there exists a canonical isomorphism

$$\gamma_{\mathrm{dR}}(X) : B_{\mathrm{dR}} \otimes_K H^r_{\mathrm{dR}}(X/K) \cong B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} \mathrm{H}^r_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p).$$

which respect Gal_K-actions and Frobenius-actions on both sides. Moreover γ_{crys} is functorial in X, and $B_{\mathrm{dR}} \otimes \gamma_{\mathrm{crys}} = \gamma_{\mathrm{dR}}$(17.11.2.1). ⌟

Proof: Cf.[Faltings, Crystalline Representations and *p*-adic Galois Representations].**?** □

Cor. (17.11.3.3) [Crystalline Comparison for Étale Cohomologies]. If $X \in \mathcal{S}\mathrm{ch}^{\mathrm{sm},proper}/K$ has good reduction $\mathcal{X}/\mathcal{O}_K$, let $\overline{\mathcal{X}} = \mathcal{X}_k$, then for any $r \in \mathbb{N}$, $\mathrm{H}^r_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \in \mathrm{Rep}^{\mathrm{dR}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$, and

$$H^r_{\mathrm{crys}}(\overline{\mathcal{X}}) \cong D_{\mathrm{crys}}(\mathrm{H}^r_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)).$$

? ⌟

4 Rigid Analytic Varieties

Main references are [Scholze, p-adic Hodge on Rigid Analytic Varieties] and [P. Scholze, *p*-adic Hodge theory for rigid-analytic varieties—corrigendum. Forum Math. Pi 4 (2016), e6, 4 pp.].

18 Representation Theory

18.1 Classical Representation Theory

In this section the representation theory over field $\mathbb{C}$ are studied(at least over a topological field of characteristic0). Modular representations are studied in Modular Representations.

For classical representations, the theory of semisimple algebras should be kept in mind.

1 Topological Representations

Def. (18.1.1.1) [Representations]. Let G be a topological group, R be a topological ring with a G-action, then an R-**representation** of G is a topological R-module V with an R-covariant action of G on M s.t. $G \times M \to M$ is continuous. The category of such representations is denoted by $\mathrm{Rep}_R(G)$.

An **irreducible representation** is a representation that has no non-trivial invariant closed subspaces. An **indecomposable representation** is a representation that is not a direct sum of two subrepresentations. ⌟

Def. (18.1.1.2) [Free Representations]. Situation as in(18.1.1.1), $V \in \mathrm{Rep}_R(G)$ is called a **free** R**-representation** if V is free over B. And it is trivial iff $V \cong B^n \in \mathrm{Rep}_B(G)$. ⌟

Def. (18.1.1.3) [Constructing Representations]. Dual representations, tensor product, and symmetric and exterior tensors. ⌟

Def. (18.1.1.4)[Projective Representations]. A **projective representation** of a topological group G on a TVS V is a continuous map $G \times P(V) \to P(V)$, where the topology on $P(V)$ is induced from $V \backslash \{0\} \subset V$. ⌟

Prop. (18.1.1.5)[F.D. Schur's Lemma]. Let $(\pi_1, V_1), (\pi_2, V_2)$ be an irreducible f.d. $\mathbb{C}$-representation of a topological group G, then $C(\pi_1, \pi_2) = \mathbb{C}$ if $\pi_1 \cong \pi_2$, and 0 otherwise. ⌟

Proof: This is because π_i are irreducible as representations with discrete topology of G: Any subspace of V_i is closed. So we reduce to(18.1.1.10). □

Def. (18.1.1.6) [Types of Representations]. Let V be an irreducible f.d. $\mathbb{C}$-representation of a topological group G, then there are three possibilities:

- $V \ncong V^*$, called a **representation of complex type**.
- There is an invariant symmetric form on V inducing an isomorphism $V \cong V^*$, called a **representation of real type**.
- There is an invariant alternating form on V inducing an isomorphism $V \cong V^*$, called a **representation of quaternion type**.

The category of representation of $\mathbb{K}$-type is denoted by $\mathrm{Rep}(G)_{\mathbb{K}}$. ⌟

Proof: By Schur's lemma(18.1.1.5), either $V \not\cong V^*$ or there is a unique isomorphism $V \cong V^*$ up to scalar, which is equivalent to an invariant form B on V. The two coordinate of this invariant form induces two isomorphisms $V \cong V^*$, which must be proportional, so $B(x,x) = cB(x,x)$, so $c = 0$ or $B(x,x) = 0$ for all x, which means B is symmetric or alternating. □

Def. (18.1.1.7)[Unitary Representations]. Usually we consider unitary representations on a Hilbert space. A **unitary representation** of a topological group G on a Hilbert space $\mathcal{H}$ is defined to be a homomorphism from G to the group $U(\mathcal{H})$ of unitary operators of $\mathcal{H}$ continuous in the strong operator topology(11.7.4.7). Notice by(11.7.4.8), this is equivalent to the unitary and continuous in the weak operator topology.

The category of unitary representations of G is denoted by $\mathrm{Rep}\,\mathrm{uni}(G)$. ⌟

Def. (18.1.1.8) [Projective Unitary Representation]. A **projective unitary representation** of a topological group G on a Hilbert space $\mathcal{H}$ is defined to be a continuous homomorphism from G to the group $PU(\mathcal{H})$ of unitary operatoes of $\mathcal{H}$, where the topology of $PU(\mathcal{H})$ is induced from the strong operator topology of $U(\mathcal{H})$(11.7.4.7). Notice by(11.7.4.8), this is equivalent to the unitary and continuous in the weak operator topology. ⌟

Def. (18.1.1.9) [Character]. Let $\rho : G \to GL(n, V)$ be a linear representation of f.d of a group G. Then the **character** of χ_ρ is defined to be $\chi_\rho(g) = \mathrm{tr}(\rho(g))$. ⌟

Prop. (18.1.1.10) [Schur's lemma]. If (π, V) is an at most countable dimensional irreducible $\mathbb{C}$-representation of a topological $\mathbb{C}$-algebra, then $\mathrm{End}_A(V) \cong \mathbb{C}$. In particular this holds for $\dim A$ countable. ⌟

Proof: First the dimension of $\dim_{\mathbb{C}} \mathrm{End}(V)$ is at most countable, because V is acyclic by irreducibly, so $\dim_{\mathbb{C}} \mathrm{End}(V) \leq \dim_{\mathbb{C}} V$. And $\mathrm{End}(V)$ is a skew field, by irreducibility. So the result follows from(3.2.1.10). □

Cor. (18.1.1.11). Any irreducible representation of a commutative group has dimension 1. ⌟

Cor. (18.1.1.12)[Index 2 Subgroup]. Let G be a topological group and H an open (normal)subgroup of index 2, $G = H \rtimes \{\sigma\}$. Let (π, V) be an irreducible representation of H of at most countable dimensional, then

- $\mathrm{res}_H^G \mathrm{ind}_H^G \pi \cong \pi \oplus \pi^\sigma$.
- $\pi \cong \pi^\sigma$ iff π is the restriction of an irreducible representation of G, called **type I**. And there are exactly two such extensions to G.
- $\pi \not\cong \pi^\sigma$ iff $\mathrm{ind}_H^G \pi$ is an irreducible representation of G, called **type II**.

All these are true for unitarizable representations. ⌟

Proof: 1: This is clear.

2: If π is a restriction of an irreducible smooth representation of G, then σ intertwines π and π^σ. Conversely, if $\pi \cong \pi^\sigma$, then there is an operator A on V that intertwines π and π^σ, and then $A^2 = \mathrm{id}$ by Schur's lemma(18.1.1.10). Let σ acts by A, then this representation extends to G.

3: If π extends to G, then clearly π appear in $\mathrm{ind}_H^G \pi$ but not surjective, so $\mathrm{ind}_H^G \pi$ is not irreducible. Conversely, if $\mathrm{ind}_H^G \pi$ is not irreducible, notice $\mathrm{res}_H^G \mathrm{ind}_H^G \pi \cong \pi \oplus \pi^\sigma$, thus $\pi \cong \pi^\sigma$, otherwise any G-invariant subspace can only be π or π^σ, so π or π^σ extends to representations of G, contradicting 2. □

Prop. (18.1.1.13). For any topological G a topological ring B with a G-action, $d \in \mathbb{N}$, there is a bijection between the set of equivalence classes of trivial B-representations V of G of rank d and the category of $H^1(G, \mathrm{GL}(d, B))$. Moreover, V is trivial iff it is mapped to the distinguished point of $H^1(G, \mathrm{GL}(d, B))$. ⌟

Proof: This follows by taking the matrix of $g \in G$ w.r.t. a B-basis of V. □

Cor. (18.1.1.14). Let L/K be a Galois extension of fields, then any f.d. L-representation of $\mathrm{Gal}(L/K)$ is trivial. ⌟

Proof: This follows from Hilbert's theorem90(8.7.3.16). □

Admissible Representations

Def. (18.1.1.15) [Admissible Representations]. Let $G \in \mathcal{G}\mathrm{rp}^{\mathrm{top}}$ and E a topological field that G acts trivially and B a topological E-algebra s.t. $B \in \mathrm{Rep}_E(G)$. Then $V \in \mathrm{Rep}_E^{\mathrm{fd}}(G)$ is called a **B-admissible** representation if $B \otimes_E V \in \mathrm{Rep}_B(G)$ is trivial.

The category $\mathrm{Rep}_E^{B\text{-adm}}(G)$ is the full subcategory of $\mathrm{Rep}_E(G)$ consisting of f.d. B-admissible E-representations of G. ⌟

Prop. (18.1.1.16) [Inclusions and Admissibility]. Let $G \in \mathcal{G}\mathrm{rp}^{\mathrm{top}}$ and E a topological field that G acts trivially and B_1, B_2, B a topological E-algebra s.t. $B_1, B_2, B \in \mathrm{Rep}_E(G)$, and $B_1 \subset B, B_2 \subset B$, $B_1 \cap B_2 = B_0$, and $B^G \subset B_0$, then

$$\mathrm{Rep}_E^{B_1\text{-adm}}(G) \cap \mathrm{Rep}_E^{B_2\text{-adm}}(G) = \mathrm{Rep}_E^{B_0\text{-adm}}(G).$$

⌟

Proof: The RHS is contained in LHS trivially. For the converse inclusion, if $V \in \mathrm{Rep}_E^{B_1\text{-adm}}(G) \cap \mathrm{Rep}_E^{B_2\text{-adm}}(G)$, there exists elements $\{u_i\} \subset (B_1 \otimes_E V)^G$ and $\{v_i\} \subset (B_2 \otimes_E V)^G$ s.t.

$$B \otimes_E V = Bu_1 \oplus \ldots Bu_n = Bv_1 \oplus \ldots Bv_n.$$

Then the transformation matrix from $\{u_i\}$ to $\{v_i\}$ is an element in $GL(n; B)$ that is invariant under G, so contained in $GL(n; B^G)$. Thus it is clear that

$$\{v_i\} \subset (B_2 \otimes_E V)^G \cap (B_1 \otimes_E V)^G = (B_0 \otimes_E V)^G,$$

and then $B_0 \otimes_E V = B_0 v_1 \oplus \ldots B_0 v_n$, and V is B_0-admissible. □

Gal_K-Regularity

Def. (18.1.1.17) [G-Regularity]. Situation as in(18.1.1.15), we want to establish a numerical criterion for recognizing B-admissible representations. B is called **G-regular** if it satisfies the following three conditions:

H1 : B is a domain.

H2 :$(\mathrm{Frac}(B))^G = B^G$, in particular, B^G is a field.

H3 : if $b \neq 0 \in B$ and Eb is stable under G-action, then $b \in B^*$.

Notice a field is clearly G-regular. ⌟

Cor. (18.1.1.18). Notice that (H3) implies $B^G \in \texttt{Field}$, because for $b \in B^{\mathrm{Gal}_K}$, Eb is clearly stable under G-action, thus b is invertible.

Also the morphism
$$\alpha_B(W) : B \otimes_{B^G} W^G \to W$$
is injective for all finite free $W \in \mathrm{Rep}_B(G)$. In particular, this is true for $W = B \otimes_E V, V \in \mathrm{Rep}_E^{\mathrm{fd}}(G)$, and we get a functor
$$D_B : \mathcal{V}\mathrm{ect}_E \to \mathcal{V}\mathrm{ect}_{B^G}$$
such that
$$\dim_{B^G} D_B(V) \leq \dim_E V.$$
⌟

Proof: To show α_W is injective, it suffices to show a linear basis $\{e_i\}$ of W^G over B^G is linearly independent over B: Suppose $\sum a_i e_i = 0$, where $a_i \in B$, with the number of nonzero coefficients minimal, and $a_1 \neq 0$, then dividing $a_1 \in \mathrm{Frac}(B)$, we assume $a_1 = 1$, and then acting by $g - \mathrm{id}$, we get
$$\sum (g(a_i) - a_i)e_i = 0$$
and this has smaller non-zero elements, unless a_i is fixed by g for any $g \in G$, so $a_i \in \mathrm{Frac}(B)^G = B^G$ by (H2), contradiction. □

Prop. (18.1.1.19)[B-Admissible Representations]. If B is G-regular(18.1.1.17), $V \in \mathrm{Rep}_E^{\mathrm{fd}}(G)$ and $W = B \otimes_E V$, then the following are equivalent:

- W is trivial, i.e. V is B-admissible.
- $\alpha_B(W)$(18.1.1.18) is an isomorphism.
- $\dim_{B^G} D_B(V) = \dim_E V$.

⌟

Proof: $1, 2$ are equivalent by(18.1.1.18), as B^{Gal_K} is a field. Also $2 \to 3$ is clear.

$3 \to 2$: $\alpha_W : B \otimes_{B^G} W^G \to B \otimes_E V$ is a B-linear morphism of two finite free B-modules, then it suffices to show the determinant map is an isomorphism. Let $v_1, \ldots, v_d$ be a E-basis of V and $w_1, \ldots, w_d$ a B^G-basis of W^G. Let b be the unique element of B that
$$\alpha_W(v_1) \wedge \ldots \wedge \alpha_W(v_d) = bw_1 \wedge \ldots \wedge w_d$$
then $gb = \eta b$ for $g \in G$ where η is determined by the identity $\alpha_W(gv_1) \wedge \ldots \wedge \alpha_W(gv_d) = \eta\alpha_W(v_1) \wedge \ldots \wedge \alpha_W(v_d)$. Now the E-space of $v_1, \ldots, v_d$ is V, which is stable under G action, thus $\eta \in E$, and then by (H3) $b \in B^*$, so we are done. □

Cor. (18.1.1.20)[$\mathrm{Rep}_E^{B-\mathrm{adm}}(G)$]. If B is Gal_K-regular, then

- $\mathrm{Rep}_E^{B-\mathrm{adm}}(G) \subset \mathrm{Rep}_E(G)$ is stable under subobjects and quotients.
- $D_B : \mathrm{Rep}_E^B(G) \to \mathcal{V}\mathrm{ect}_{B^G}$ is exact and faithful.
- $\mathrm{Rep}_E^{B-\mathrm{adm}}(G) \subset \mathrm{Rep}_E(G)$ is stable under taking dual and tensor products. And if $V, V_1, V_2 \in \mathrm{Rep}_E^{B-\mathrm{adm}}(G)$, then there is a natural isomorphism
$$D_B(V_1) \otimes D_B(V_2) \cong D_B(V_1 \otimes V_2)$$
and
$$D_B(V) \otimes D_B(V^\vee) \cong D_B(V \otimes V^\vee) \to D_B(E) = B^G$$
is a perfect pairing between $D_B(V)$ and $D_B(V^\vee)$.

⌟

Proof: 1: Given an exact sequence $0 \to V_1 \to V \to V_2 \to 0 \in \mathrm{Rep}_E(G)$, tensoring B and taking G-fixed points, we get an exact sequence

$$0 \to D_B(V_1) \to D_B(V) \to D_B(V_2)$$

from which we derive the inequality $\dim_{B^G} D_B(V) \le \dim_{B^G} D_B(V_1) + \dim_{B^G} D_B(V_2)$. Now we have $\dim_{B^G} D_B(V_i) \le \dim_E V_i$ by(18.1.1.18), so

$$\dim_{B^G} D_B(V) \le \dim_{B^G} D_B(V_1) + \dim_{B^G} D_B(V_2) \le \dim_E V_1 + \dim_E V_2 = \dim_E V.$$

But this is an equality because V is B-admissible, thus V_1, V_2 are all B-admissible, and the exact sequence is in fact an isomorphism by dimension reason.

2: D_B is faithful because $B \otimes_{B^G} D_B(V) \cong B \otimes_E V$.

3: There is a natural map

$$D_B(V_1) \otimes_{B^G} D_B(V_2) = (B \otimes_E V_1)^G \otimes (B \otimes_E V_2)^G \to (B \otimes_E (V_1 \otimes_E V_2))^G = D_B(V_1 \otimes_E V_2),$$

and $\dim_{B^G} D_B(V_1 \otimes_E V_2) \le \dim_E(V_1) \cdot \dim_E(V_2)$, so it suffices to show that this map is injective. For this, notice that $D_B(V_1 \otimes_E V_2) \subset B \otimes_E (V_1 \otimes_E V_2)$, and after tensoring B,

$$D_B(V_1) \otimes_{B^G} D_B(V_2) \subset B \otimes_{B^G} (D_B(V_1) \otimes_{B^G} D_B(V_2)) \cong (B \otimes_E V_1) \otimes_B (B \otimes_E V_2) \to B \otimes_E (V_1 \otimes_E V_2)$$

is an isomorphism.

To show for the dual preserves B-admissibility, notice that $\mathrm{Rep}_E^{B-\mathrm{adm}}(G)$ is also stable under exterior products, as exterior products are quotient of tensor products. Notice there is an isomorphism

$$\wedge(V^\vee) \otimes \wedge^{\dim V - 1} V \cong V^\vee,$$

so it suffices to show for $\dim V = 1$. Let v_0 be an E-basis of V, $g(v_0) = \eta(g) v_0$, then $D_B(V) = B^G(b \otimes v_0)$ for some $b \neq 0 \in B$. Thus $b/g(b) = \eta(g)$. And it is easy to show that $D_B(V^\vee) = B^G(b^{-1} \otimes v_0)$, and the natural pairing is perfect. In general, the pairing is also perfect because perfectness of a pairing can be checked after passing to the determinant space. □

Unitary Representations of Locally Compact Groups

For unitary representations of locally compact groups, see11.10.

2 Smooth Representations

Prop. (18.1.2.1)[Smooth Representations]. A **smooth representation** of a locally compact group G on a complex vector space is a continuous representation w.r.t the discrete topology.

The category $\mathrm{Rep}^{\mathrm{alg}}(G)$ of smooth representations is a full Abelian subcategory of the category of continuous representations, and there is a right adjoint to the forgetful functor:

$$\mathrm{Rep}(G) \to \mathrm{Rep}^{\mathrm{alg}}(G) : V \mapsto V^\infty = \bigcup_{K \subset G \text{ compact open}} V^K$$

So it preserves injectives and $\mathcal{M}(G)$ has enough injectives. ⌟

Def. (18.1.2.2) [Equivariant Sheaves]. Let G be a locally compact group acting on a space X, let $p : G \otimes X \to X$ be the projection and $a : G \times X \to X$ be the action, then a **equivariant sheaf** on X is a pair $(\mathcal{F}, \rho)$, where $\mathcal{F}$ is a locally constant complex sheaf on X and ρ is an isomorphism of sheaves $p^*(\mathcal{F}) \cong a^*(\mathcal{F})$ that:

- ρ is identity on $e \otimes X$.
- $p_{23}^* \rho \circ (\mathrm{id}_G \times a)^* \rho = (m \times \mathrm{id}_X)^* \rho$ on $G \times G \times X$.

⌟

Prop. (18.1.2.3). If X is a pt with the trivial G-action, then a equivariant sheaf on X is equivalent to a representation of G. ⌟

Proof: For any equivariant sheaf on X, the pullback are just locally constant functions of G with value in V. Then ρ on each stalk g defines an action of g on V. Compatibility with the G-action shows that this is a group action. And consider the stalk at e, because ρ is id at e, for each v, there is an open nbhd U that $\rho(u)v = v$ on for $u \in U$, thus it is smooth. The converse is obvious. □

Def. (18.1.2.4) [Coinvariants]. The **Jacquet functor** $J_G : \mathrm{Rep}(G) \to \mathcal{V}\mathrm{ect}_{\mathbb{C}}$ is the functor mapping a representation V of G to $V/V(G)$, where $V(G)$ is spanned by $\pi(g)v - v$. It is equivalent to the functor $V \mapsto V \otimes_G \mathbb{C}$.

Let ψ be a character of G, then we can more generally define $J_{G,\psi} : \mathrm{Rep}(G) \to \mathcal{V}\mathrm{ect}_{\mathbb{C}}$ is the functor mapping a representation V of G to $V/V_{G,\psi}$, where $V_{G,\psi}$ is spanned by $\pi(g)v - \psi v$. It is equivalent to the functor $V \mapsto V \otimes_G \mathbb{C}_\psi$, or equivalently $J_{G,\psi} = J_G \circ (\psi^{-1} \otimes)$. ⌟

Prop. (18.1.2.5). If G is compact, then $e_G V = V^G = V/V(G)$.

And if G is a union of increasing family of compact groups, then J_G is exact, so is $J_{G,\psi}$. ⌟

Proof: J_G is clearly right exact. And if G is compact, $e_G V = V^G = V/V(G)$: if $\pi(G)v = v$, then $v = e_G v$, and if $e_G v = 0$, then because v is smooth, $\sum_{h_i \in G/K} h_i v = 0$, thus $v = \frac{1}{[G:K]}(v - h_i v)$ is in $V(G)$.

If G is a union of compact groups K_i, then $V/V(G) = \mathrm{colim}\, V/V(K_i)$ is exact. □

Prop. (18.1.2.6). If G is a union of increasing family of compact open subgroups $\{K_\alpha\}$, then $v \in V(G,\psi)$(ψ can be trivial) iff for some K_α, $\int_{K_\alpha} \psi^{-1}(h)\pi(h)v dh = 0$. ⌟

Proof: We can assume ψ is trivial. If $v = \pi(h)w - w$ and $h \in K_\alpha$, then $\int_{K_\alpha} \psi^{-1}(h)\pi(h)v dh = 0$. Conversely, by the proof of(18.1.2.5), $V(G) = \cup V(K_\alpha) = \cup \ker(e_{K_\alpha})$, which is equivalent to $\int_{K_\alpha} \pi(h)v dh = 0$. □

Def. (18.1.2.7) [Contragradient Representation]. For a smooth representation V of G, the **contragradient smooth representation** $V^\wedge = (V^*)^\infty$ is the smooth part of V^*. ⌟

Prop. (18.1.2.8). Let E be a smooth or f.d. representation of a topological group G, then

- E has an irreducible subquotient.
- If E is f.g., then it has an irreducible quotient.

⌟

Proof: 2: Use Zorn's lemma for the set of proper G-subspaces of U, the union of a chain of proper G-subspaces is proper, because it is f.g.. So it has a maximal proper G-space, thus the quotient is irreducible.

1 follows from 2 by choosing a f.g. submodule. □

Prop. (18.1.2.9) [Induced Representation]. The induced and compactly induced representations have the following equivalent forms:

$$\mathrm{Ind}_H^G(V) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], V), \quad \mathrm{ind}_H^G(V) = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} V.$$

I.e., if H acts on V by ρ, then $\mathrm{ind}_H^G(\rho)$ is the space $\oplus_{\gamma\in G/H} V_\gamma$ where $V_\gamma \cong V \in \mathcal{M}\mathrm{od}_H$, and that for $v_\gamma \in V_\gamma$, $(\mathrm{Ind}(\rho)g)v_\gamma = \rho(h)v_{\gamma'} \in V_{\gamma'}$ where $g\gamma = \gamma' h$ that $\gamma' \in G/H, h \in H$. ⌟

Proof: Choose a set of left coset representatives Γ of G/H, then Γ^{-1} is a set of right coset representatives for $H\backslash G$. Now $\mathbb{Z}[G] = \oplus_{\gamma\in\Gamma}\mathbb{Z}[H]\gamma^{-1}$, and we define the space $V_\gamma \cong V$ of maps from $\mathbb{Z}[G]$ to V determined by: $v_\gamma(g) = \rho(g\gamma)v \in V$ if $g \in H\gamma^{-1}$ and 0 otherwise.

Then $\mathrm{Ind}(\rho)(V) = \oplus_{\gamma\in\Gamma} V_\gamma$ that for $v_\gamma \in V_\gamma$, $(\mathrm{Ind}(\rho)g)v_\gamma$ is the map $\mathbb{Z}[G]$ to V determined by: $((\mathrm{Ind}(\rho)g)v_\gamma)(g') = \rho(g'\gamma' h)v \in V$ if $g' \in H(\gamma')^{-1}$, and 0 otherwise, where $g\gamma = \gamma' h$. Then $(\mathrm{Ind}(\rho)g)v_\gamma = \rho(h)v_{\gamma'}$, which is the same as the formula for $\mathrm{Ind}(\rho)$ as in(18.1.2.9). So the map $v_\gamma \to v_\gamma : \mathrm{Ind}(\rho) \to \mathrm{Ind}(\rho)$ is an isomorphism in $\mathbb{Z}[G] - \mathcal{M}\mathrm{od}$. □

Prop. (18.1.2.10) [Clifford's Theorem]. If $\rho : G \to GL(V)$ is a semisimple smooth or f.d. representation and H is a normal subgroup of G, then $\rho|_H$ is also semisimple.

In particular, a normal Abelian subgroup acts by scalars on any irreducible $\mathbb{C}$-representation of G, by(18.1.1.11). ⌟

Proof: Use definition(3.6.1.4), we reduce to the case ρ is simple. Now an H-subrepresentation is simple iff it has no proper H-subrepresentations, so clearly G maps a simple H-subrepresentation to another simple H-subrepresentation. So if W is the sum of all simple H-subrepresentations, then G preserves W, which shows $W = V$, and V is H-semisimple by(3.6.1.4). □

Prop. (18.1.2.11) [Restriction]. If G is a group and H is an open normal subgroup of G of finite index n. Let (π, V) be a smooth representation of G of f.d. over a field of characteristic $p \nmid n$, then

- If $\pi|_H$ is completely reducible, then π is also completely reducible.
- If (π, V) is irreducible, then $\pi|_H = \pi_1 \oplus \ldots \oplus \pi_k$ where π are irreducible representations of H and $k \leq [G : H]$.
- If (π, V) is irreducible, the isotopy parts of H are all of the same dimension, and if there are more than 1 isotropy classes, then G is an induced representation.

Moreover, item2, 3 are also true for H open normal in G s.t. $HZ(G)$ is of finite index n. ⌟

Proof: Let $g_1, \ldots, g_n$ be a coset representation of G/H.

1: If V_1 is a G-submodule of V, then V_1 has a complementary H-submodule $V_1^\perp$. Let P_0 be the projection of V onto V_1 along $V_1^\perp$, then $P = \frac{1}{p}\sum \pi(g_i)P_0\pi(g_i)^{-1}$ is a projection of V onto V_1 that commutes with G-action. Therefore the kernel of P is a G-submodule of V that is complementary to V_1.

2: Let $v \in V$, then $\{\pi(g_i)v\}$ generates V as a H-representation, thus by(18.1.2.8) there is an H-submodule $V' \subset V$ that V/V' is irreducible. Let $V_i = \pi(g_i)V'$, then V/V_i are also irreducible representations of H. Consider the H-invariant map $V \mapsto \oplus V/V_i$, its kernel is G-invariant, thus trivial, thus V is a submodule of $\oplus V/V_i$, and the assertion follows.

3: The G-action permutes with isotopy classes. And if there are more than 1 classes, choose the stabilizer G_ρ of one V^ρ, then $V = \mathrm{Ind}_{G_\rho}^G V^\rho$ by(18.1.2.9). □

Prop. (18.1.2.12) [Kolchin]. Let G be a discrete group acting on a f.d. vector space V s.t. each $g \in G$ acts via a unipotent endomorphism, then there is a basis s.t. G is mapped into $U(n, T)$. ⌟

Proof: Cf.[Mil17]P279. □

3 Linear Representation of Finite Groups

Basic references are [Ser77], [A-B95]. [群表示论 notes 薛航].

Remark (18.1.3.1). The representations in this subsection is assumed to be of f.d. over a field of char0, in particular, over a subfield of $\mathbb{C}$. In particular, there is no need to consider topologies.

Because a finite group is compact, all results of compact groups apply to a finite group, see4.

Because a finite group is locally profinite, all results of locally profinite groups apply to finite groups2. ⌟

Prop. (18.1.3.2) [Orthogonality of Characters]. The characters χ_i of irreducible representations of G form a basis of $ZL^2(G)$ by(11.10.4.30). Also, for $s \in G$, let $c(s)$ be the number of elements in the conjugacy class of s, then:

- $\int_i |\chi_i(s)|^2 = g/c(s)$.
- If t is not conjugate to s, then $\sum_i \chi_i(s)^* \chi_i(t) = 0$.

⌟

Proof: The last assertion follows from the first one, if you consider a matrix with conjugacy classes as column and characters as rows, and place $\sqrt{c(s)/g}\chi_i(s)$ in the entries, then it is an orthogonal matrix. □

Cor. (18.1.3.3) [Representations Determined by Characters]. A representation of G over $\mathbb{C}$ is determined by its character, by(3.6.1.13). ⌟

Cor. (18.1.3.4) [Number of Representations]. If G is a finite group, then the cardinality of $\widehat{G}$ is equal to the number of conjugates of G, and $\sum_{\pi \in \widehat{G}} d_\pi^2 = |G|$. ⌟

Proof: Both $\{\chi_\pi\}$ and the characteristic functions of the conjugate classes of G are basis for $L^2(G)$. And the second assertion follows from the Peter-Weyl theorem(11.10.4.15) as $\sum_{\pi \in \widehat{G}} d_\pi^2$ is the dimension of $L^2(G)$. □

Cor. (18.1.3.5). G is Abelian iff every irreducible representation of G is of dimension 1. ⌟

Proof: This follows immediately from the equation $\sum_{\pi \in \widehat{G}} d_\pi^2 = |G|$(18.1.3.4), as G is Abelian iff it has $|G|$ conjugacy classes iff $|\widehat{G}| = |G|$ iff $d_\pi = 1$ for any π. □

Prop. (18.1.3.6). If G is a finite p-group and A is a nonzero p-torsion G-module, then $A^G \neq 0$. ⌟

Proof: We may consider A generated by a single element. Because A is p-torsion, $|A| = p^n$ for some n. Now consider the orbit, then if the orbit is not a single element, then its order is divisible by p, so $|A^G|$ is divisible by p. But 0 is fixed, so $A^G \neq 0$. □

Group Algebra $\mathbb{C}[G]$

Prop. (18.1.3.7) [Maschke's Theorem]. If F is a field of char p and G is a finite group of order prime to p, then for any representation U of $F[G]$ and a submodule V, there exists a complement of V in U. ⌟

Proof: Choose an arbitrary projection π of U to V, and let $\rho(v) = 1/|G| \sum g^{-1}\pi(g(v))$, then it can be checked ρ commutes with G-actions, thus its kernel is also a G-modules, and it is identity on V, so $U = V \oplus k \ker \rho$. □

Cor. (18.1.3.8) [Totally Decomposable]. Any such representation of G is a direct sum of irreducible representations. ⌟

Prop. (18.1.3.9) [Brauer-Nesbitt]. For a finite group G, if two finite dimensional semisimple representations over a field has the same char poly for every element g of G, then they are isomorphic. ⌟

Proof: Just use the irreducible representations are orthogonal and that they have the same and for char p, we can use divide by p and the char poly becomes p-th power and we can do this forever, contradiction. □

Prop. (18.1.3.10). Integral properties of characters. ⌟

Prop. (18.1.3.11) [Dimensions Divisor Order]. The dimension of the irreducible representations of G divides the order of G. ⌟

Proof: □

Cor. (18.1.3.12). The dimension of the irreducible representations of a p-group G is a p-power. ⌟

Prop. (18.1.3.13) [Burnside's Theorem]. Any group of order n that n has only two prime divisors are solvable. ⌟

Proof: □

Induced Representations and Mackey Theory

Remark (18.1.3.14). When G is a finite group, the induced representation Ind_H^G(18.1.2.9) is the same as the (compact)induction in(18.1.5.34). In particular, all the results there holds in the finite group case. ⌟

Prop. (18.1.3.15) [Character of Induced Representations]. Character of induced representations, Cf.[Serre, P30]. ⌟

Rationality Problems

Def. (18.1.3.16) [Ring $R_K(G)$]. We want to consider the representations over a subfield K of $\mathbb{C}$.

Let $R_K(G)$ be the $\mathbb{Z}$-module generated by the characters of the representations of G over K, then it is a subring of $R(G) = R_{\mathbb{C}}(G)$. And define the $\mathbb{Z}$-module $\overline{R}_K(G)$ to be the elements of $R(G)$ with values in K. Clearly $R_K(G) \subset \overline{R}_K(G)$. ⌟

Prop. (18.1.3.17) [Induction and Restriction Morphism]. Let H be a subgroup of G, then the induction induces a Abelian group homomorphism $R(H) \to R(G)$, and restriction induces a ring homomorphism $R(G) \to R(H)$. The formula $\mathrm{Ind}(\varphi \cdot \mathrm{res}(\psi)) = \mathrm{Ind}(\varphi) \cdot \psi$ shows the image of Ind is an ideal of $R(G)$. Also by Frobenius reciprocity(18.1.5.37), Ind and Res are dual to each other:

$$(\varphi, \mathrm{res}\,\psi)_H = (\mathrm{Ind}\,\varphi, \psi)_G.$$

⌟

Prop. (18.1.3.18). Let ρ_i be the isomorphism classes of all irreducible linear representations of G over K and χ_i there characters. Then

- χ_i form a basis of $R_K(G)$.
- χ_i are mutually orthogonal.

┘

Proof: □

Cor. (18.1.3.19). A representation of G over $\mathbb{C}$ is realizable over K iff its character belongs to $R_K(G)$. ┘

Proof: One direction is trivial, for the other, if $\chi \in R_K(G)$, then $\chi = \sum n_i\chi_i$, and $(\chi, \chi_i) = n_i(\chi_i, \chi_i)$. As $(\chi, \chi_i) \geq 0$ as they are representations of G, we have $n_i \geq 0$, thus $\rho = \sum n_i\rho_i$ is realizable over K, by(18.1.3.3). □

Def. (18.1.3.20) [Schur Indices]. $K[G]$ is called **quasisplit** if the D_i are all commutative, or equivalently, all $m_i = 1$. ┘

Prop. (18.1.3.21). If L/K is finite and $L[G]$ is quasisplit, then $[L : K]$ is divisible by each of the Schur indices m_i. ┘

Proof: □

Prop. (18.1.3.22). The characters $\psi = \chi_i/m_i$ form a basis of $\overline{R}_K(G)$. ┘

Proof:

□

Cor. (18.1.3.23). $R_K(G) = \overline{R}_K(G)$ iff $K[G]$ is quasisplit. ┘

Cor. (18.1.3.24) [Brauer]. If m is the least common multiples of the orders of the elements of G and K contains the m-th roots of unity, then $R_K(G) = R(G)$. ┘

Proof:

□

Cor. (18.1.3.25). If m is the least common multiples of the orders of the elements of G, then all the Schur indices of G over any field K divides the Euler function $\varphi(m)$. ┘

Proof: This follows from(18.1.3.24) and(18.1.3.21) by considering the field $K[\mu_m]$ over K. □

Def. (18.1.3.26) [Galois-Action on G]. Let $L = K(\mu_m)$, where m divides the order of any element in G, then L/K is Galois and $G(L/K) = \Gamma_K$ is a subgroup of $(\mathbb{Z}/m\mathbb{Z})^*$. Then this group can act on G by $\sigma_t(x) = x^n$ as a set, and we call two elements $s, s' \in G$ Γ_K**-conjugate** iff they are in the same Γ_K orbits of G. ┘

Prop. (18.1.3.27). A class function f on G with values in L belongs to $K \otimes_{\mathbb{Z}} R(G)$ iff

$$\sigma_t(f(s)) = f(s^t)$$

for $\sigma_t \in \Gamma_K$ and $s \in G$. ┘

Proof: Cf.[Serre, P95]. □

Cor. (18.1.3.28). A class function f on G with values in K belongs to $K \otimes_{\mathbb{Z}} R_K(G)$ iff it is constant on the Γ_K-orbits of G. ┘

Proof: Because the □

Prop. (18.1.3.29). For a finite group G, all representations of G has characters in $\mathbb{Q}$ iff it all representations have characters in G, iff every two element generating the same subgroup of G is conjugate. ⌟

Proof: Cf.[Serre P103]. □

Cor. (18.1.3.30). representations of S_n all has characteristic in $\mathbb{Z}$. ⌟

Artin's Theorem & Brauer's Theorem

Prop. (18.1.3.31) [Generalized Artin Theorem]. Let X be a family of subgroups of a finite group G. Let $\mathrm{Ind} : \oplus_{H\in X} R_K(H) \to R_K(G)$ be the ring homomorphism induced by induction, then the following properties are equivalent:

- G is the union of conjugates of the subgroups in X.
- the cokernel of Ind is finite.

⌟

Proof: $2 \to 1$: By the character of induced representations(18.1.3.15), any function in the image of Ind vanishes outside the union of conjugates of the subgroups in X, so if this is not G, then the cokernel cannot by finite.

$1 \to 2$: Notice the duality of Ind and Res(18.1.3.17), it suffices to show that Res is injective, but this is clear. □

Cor. (18.1.3.32) [Artin Theorem]. Choose X as the family of cyclic subgroups of G, then every character of G is a rational combination of characters induced from cyclic subgroups of G. ⌟

Proof:

□

Prop. (18.1.3.33) [Brauer's Theorem]. Let $G \in \mathcal{A}\mathrm{b}^{\mathrm{fin}}$, then $K_0(\mathrm{Rep}(G))$ is generated by $\mathrm{Ind}_{H_i}^G(\chi_i)$, where $H_i \leq G, \chi_i \in \widehat{H}_i$. ⌟

Proof: □

Prop. (18.1.3.34) [Generalized Brauer's Theorem]. ⌟

Proof: □

Important representations

Prop. (18.1.3.35) [Q_8]. There is a 2-dimensional representation of the quadratic group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$:

$$i \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad j \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad k \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

⌟

Prop. (18.1.3.36). There is a representation of S_n on the $n-1$-dimensional hypersurface $\sum x_i = 0$. ⌟

4 Symmetric Groups

Main references are [The Symmetric Group, Sagan].

5 Locally Profinite Groups

Notation (18.1.5.1).

- Use notations as in Structure Sheaves and Distributions.
- For structure theory of locally profinite groups, Cf. Locally Profinite Groups.

⌟

Structure Sheaf and Distributions

Cf.[Representations of the Group GL(n,F) over Local Fields Bernstein/Zelevinsky] and [Bernstein, Representation of p-adic Groups, Bernstein].

Prop. (18.1.5.2). For $G \in \mathrm{loc}\mathcal{P}\mathrm{rof}$, any $\varphi \in C_c^\infty(G)$ is K-bi-invariant under some compact open subgroup K. ⌟

Proof: φ must be of the form $\sum a_i\chi_{U_i}$, where each U_i is open compact. Then for each element $x \in U_i$, there is an open compact group U_x that $U_x x \cup xU_x \subset U_i$, by(11.10.1.50). Now because $\mathrm{Supp}\, f$ is compact, f.m. of the $U_x x \cap xU_x$ covers $\mathrm{Supp}\,\varphi$, thus we consider their intersection $\cap U_{x_i}$, which is a compact open subgroup K_0 that φ is K_0-bi-invariant. □

Lemma (18.1.5.3). Let G be a locally profinite group and H a closed subgroup, then G/H is locally profinite space by(11.10.1.51). Then the projection $P : C_c(G) \to C_c(G/H)$ defined in(11.10.1.36) restricts to a projection $P^\infty : C_c^\infty(G) \to C_c^\infty(G/H)$, and it is surjective. ⌟

Proof: Firstly P maps $C_c^\infty(G)$ into $C_c^\infty(G/H)$ because if φ is left invariant under K, then $P\varphi$ is also left invariant under K. For the surjectivity, let $\varphi \in C_c^\infty(G/H)$, then $V = \mathrm{Supp}\,\varphi$ is open compact, then by(11.10.1.52) there is an open compact subspace V that $p(V) = U$, Then we can define

$$\psi(x) = \chi_V(x)\varphi(p(x))/P(\chi_V)(p(x)),$$

then it is supported on V, and $P(\psi) = \varphi$. Also, it is locally constant, as is easily verified. □

Prop. (18.1.5.4) [Left Invariant Distribution]. Let G be a locally profinite group and T is a left invariant distribution on G, then it is the restriction of a unique Haar measure. ⌟

Proof: Any element $f \in C_c^\infty(G)$ is of the form $\sum a_i\lambda(h_i)e_K$ for some K, by(18.1.5.2), where $e_K = \mu(K)^{-1}\chi_K$. Because T is left-invariant, $T(f) = \sum a_i T(e_K)$, and $\int f d\mu = \sum a_i$. Thus to show T is a multiple of $d\mu$, it suffices to show $T(e_K)$ is independent of K.

If $K_1 \le K_2$, then $K_2 = \coprod_{i=1}^n a_i K_1$, where $n = [K_2 : K_1]$, so $e_{K_2} = \mu(K_1)/\mu(K_2)\sum_{i=1}^n \lambda(a_i)e_{K_1}$. Also $\mu(K_2) = n\mu(K_1)$ by left invariance. Now it is clear $T(e_{K_1}) = T(e_{K_2})$ by left invariance of T. Then for any two K, K', we can find an open compact group K'' in their intersection, thus $T(e_K) = T(e_{K'})$. □

Cor. (18.1.5.5). If T is a distribution on G that satisfies $\lambda(g)T = \xi(g)^{-1}T$ for $g \in G$, then there is a unique Haar measure $d\mu$ that $T(f) = \int_G \xi(g)f(g)d\mu(g)$. ⌟

Proof: Consider the distribution $T'(f) = T(\xi^{-1}f)$, then it is left invariant. □

Cor. (18.1.5.6) [Invariant Quotient Distribution]. Let G be a locally profinite group and H a closed subgroup. then left H-invariant measures on G are identified with measures on G/H.

And if there exists a left G-invariant distribution D on G/H, then G/H admits a G-invariant measure(11.10.1.38), whose restriction to $C_c^\infty(G/H)$ is D. ⌟

Proof: Consider the distribution $D \circ P^\infty$, which is a left invariant linear functional on $C_c^\infty(G)$, (18.1.5.4) shows that it's the restriction of a Haar measure on G.

Then we can use the same method as in(11.10.1.38) to show $\Delta_G|_H = \Delta_H$, and the surjectivity of P^∞(18.1.5.3) shows D is a quotient measure on G/H. □

Prop. (18.1.5.7) [Gelfand Pairs]. Let G be a locally profinite group and H a closed subgroup s.t. $\Delta(G)|_H = \Delta_H$. Suppose ι is an involution on G that leaves H invariant and acts trivially on those distributions on G with are H-bi-invariant, then for any smooth irreducible representation V of G, $\dim(V^*)^H \cdot \dim((V^\vee)^*)^H \leq 1$. ⌟

Proof: Given two H-invariant maps $l : C \to \mathbb{C}, m : V^\vee \to \mathbb{C}$, by Frobenius reciprocity, we get two maps $l' : C_c^\infty(H\backslash G) \to V, m' : C_c^\infty(H\backslash G) \to V^\vee$ that are surjective, and give rise to $B : C_c^\infty(\mathcal{H} \times \mathcal{H}\backslash G \times G) \to V \times V^\vee \to \mathbb{C}$.

Then B satisfies $B(f, g) = B(i(g), i(f))$, where $i(f)(x) = f(\overline{x}^{-1})$: There is a commutative diagram

$$\begin{array}{ccc} G \times G & \xrightarrow{(x,y)\mapsto xy^{-1}} & G \\ \downarrow{\scriptstyle (x,y)\mapsto(\iota(y)^{-1},\iota(x)^{-1})} & & \downarrow{\scriptstyle \iota} \\ G \times G & \xrightarrow{(x,y)\mapsto xy^{-1}} & G \end{array}$$

and the horizontal arrows identify left H-invariant right G-invariant distributions on G with left $H \times H$-invariant distributions on $G \times G$.

By the surjectivity of l', m', $\ker(l'), \ker(m')$ are left and right radicals of B resp., and the above formula shows they determine each other, and l', m' are determined by their kernels, thus we are done. □

Prop. (18.1.5.8) [Bernstein-Zelevinsky?]. If $p : X \to Y$ is a continuous map of locally profinite groups, $\mathcal{F}$ be a cosmooth C^∞-sheaf on X**??**. Let G be a group acting on X and the sheaf $\mathcal{F}$ that $p(gx) = p(x)$, and χ a character of G. Then

- Let $\Gamma_c(X, \mathcal{F})(\chi)$ be the $C_c^\infty(X)$-submodule of $\Gamma_c(X, \mathcal{F})$ generated by $gf - \chi(g)^{-1}f, g \in G, f \in \Gamma_c(X, \mathcal{F})$. Then $\Gamma_c(X, \mathcal{F})/\Gamma_c(X, \mathcal{F})(\chi)$ is a non-degenerate $C_c^\infty(Y)$-module by composing p, so we can define $\mathcal{G}$ the sheaf on Y corresponding to this submodule by(4.4.4.14). Then if $y \in Y$ and $Z = p^{-1}(y)$, the stalk
$$\mathcal{G}_y \cong \Gamma_c(Z, \mathcal{F})/\Gamma_c(Z, \mathcal{F})(\chi).$$
- Assume there are no non-zero distributions $D \in \mathcal{D}(p^{-1}(y), \mathcal{F}|_{p^{-1}(y)})$ that satisfies $gD = \chi(g)D$ for any $y \in Y$, then no such D exists in $\mathcal{D}(X, \mathcal{F})$.

⌟

Proof: 1: Firstly $\Gamma_c(X, \mathcal{F})/\Gamma_c(X, \mathcal{F})(\chi)$ is a $C_c^\infty(Y)$-module because $\varphi \circ p$ fixes $\Gamma_c(X, \mathcal{F})(\chi)$:

$$(\varphi \circ p)(gf - \chi(g)^{-1}f) = g((\varphi \circ p)f) - \chi(g)^{-1}((\varphi \circ p)f),$$

which uses the condition $p(gx) = p(x)$. The non-degeneracy is also clear, by(4.4.4.14).

Secondly $\Gamma_c(Z,\mathcal{F})\cong\Gamma_c(X,\mathcal{F})/\Gamma_c(U,\mathcal{F})$ by(4.4.4.11), so $\Gamma_c(Z,\mathcal{F})/\Gamma_c(Z,\mathcal{F})(\chi)$ is isomorphic the quotient of $\Gamma_c(X,\mathcal{F})$ by $\Gamma_c(U,\mathcal{F})$ and $\Gamma_c(X,\mathcal{F})(\chi)$, because $\Gamma_c(U,\mathcal{F})$ is stable under action of $f\mapsto gf-\chi(g)^{-1}f$(this uses the condition $p(gx)=p(x)$).

We claim the space $\Gamma_c(U,\mathcal{F})$ is the space L generated by elements of the form $(\varphi\circ p)f$, where $\varphi\in C_c^\infty(Y),\varphi(y)=0,f\in\Gamma_c(X,\mathcal{F})$: L is clearly contained in $\Gamma_c(U,\mathcal{F})$, and if $f\in\Gamma_c(U,\mathcal{F})$, then $\operatorname{Supp} f$ is compact and disjoint from Z, so there is an open compact subset $U\subset Y$ containing $p(\operatorname{Supp} f)$ but not y. Let $\varphi=\chi_U$, then $f=(\chi_U\circ p)f\in L$.

Then by(4.4.4.14), the stalk $\mathcal{G}_y$ is isomorphic to $M/M(y)$, where $M=\Gamma_c(X,\mathcal{F})/\Gamma_c(X,\mathcal{F})(\chi)$. So $M(y)$ is just the image of the space L in M by(4.4.4.15), hence $\mathcal{G}_y$ is exactly $\Gamma_c(Z,\mathcal{F})/\Gamma_c(Z,\mathcal{F})(\chi)$.

2: this follows from 1, as $gD=\chi(g)D$ is just saying $D(g^{-1}f-\chi(g)f)=0$, or that D annihilates $\Gamma_c(Z,\mathcal{F})/\Gamma_c(Z,\mathcal{F})(\chi)=\mathcal{G}_y$ by item1. So this is equivalent to $\mathcal{G}_y$=0 for any y, which is equivalent to $\mathcal{G}=0$, as $\mathcal{G}$ is a sheaf. □

Cor. (18.1.5.9) [Invariant Distribution On Orbits]. Let γ be an action of a locally profinite group G on a locally profinite space X and a $C^\infty(X)$-sheaf. Assume the action is constructible(4.12.1.21) and there are no G-invariant distribution on any G-orbit in X, then there are no non-zero G-invariant distribution on X. ⌟

Proof: Firstly, by(4.12.1.22) and(4.4.4.6) any orbit is locally profinite. If there is a G-invariant distribution on X, we may change X to $\operatorname{Supp} T$, which is G-invariant, thus by(4.12.1.22) there is an open subset $U\subset X$ that G acts regularly, thus we reduce to the regular action case.

Then we can consider $X\to X/G$, X/G is locally profinite by(4.12.1.10), so Bernstein-Zelevinsky(18.1.5.8) can be used. □

Prop. (18.1.5.10) [Gelfand-Kazhdan]. If G is a locally profinite group, and γ is an action of G on a locally profinite space X, σ is a homeomorphism $X\cong X$, $\mathcal{F}$ is a C^∞-sheaf on X, and we assume:

- γ is constructible,
- for each $g\in G$, there is a $g^\sigma\in G$ that $\gamma(g)\sigma=\sigma\gamma(g^\sigma)$.
- For some $n\geq 0$ and $g_0\in G$, $\gamma^n=\gamma(g_0)$.
- If there is a non-zero G-invariant $\mathcal{F}$-distribution T on a G-orbit S, then $\sigma(S)=S$ and $\sigma(T)=T$.

Then any G-invariant distribution on X is invariant under σ. ⌟

Proof: Let T be a G-invariant $\mathcal{F}$-distribution that $\sigma T\neq T$, then $n>1$, and for any n-th root of unity ξ, consider $T_\xi=\sum\xi^{-i}\sigma^i(T)$. Then

$$\sigma T_\xi=\xi T_\xi,\quad \sum_\xi T_\xi=nT,\quad \sum\xi T_\xi=n\sigma(T).$$

so $\sum_\xi(\xi-1)T_\xi=n(\sigma(T)-T)\neq 0$, which shows there is a root $\xi\neq 1$ that $T_\xi\neq 0$. Notice T_ξ is G-invariant by condition2. Consider the action $\sigma_x i=\xi\cdot\sigma$, then T_ξ is invariant under σ_ξ.

Let G' be the semi-direct product of G with σ_ξ, under the action of $\sigma_\xi^{-1}g\sigma_\xi=g^\sigma$, then G' is locally profinite and acts on $X,\mathcal{F}$. Clearly this action is also constructible.

Now for any G'-orbit S', we prove there are no G'-invariant distribution on S', because it is in priori G-invariant, so some distribution exists on some G-orbit $S\subset S'$, but then condition4 shows σ fixes S, then $S=S'$ and $\sigma(T)=T$. But $\sigma_\xi(T)=T$, contradiction. Finally,(18.1.5.9) shows there are no G'-invariant distribution on X, contradicting T_ξ. □

Cor. (18.1.5.11) [Gelfand-Kazhdan]. If G is a locally profinite group that is σ-compact, and γ is an action of G on a locally profinite space X, $\sigma:X\cong X$ is a homeomorphism, and we assume:

- γ is constructible,
- for each $g \in G$, there is a $g^\sigma \in G$ that $\gamma(g)\sigma = \sigma\gamma(g^\sigma)$.
- For some $n \geq 0$ and $g_0 \in G$, $\sigma^n = \gamma(g_0)$.
- For any x, x and $\sigma(x)$ are in the same G-orbit.

Then any G-invariant distribution on X is invariant under σ. ⌟

Proof: We use(18.1.5.11) and take $\mathcal{F}$ to be just $C^\infty(X)$. Then we need to check condition4: for any G-orbit S of X let $s \in S$ and $\mathrm{Stab}(s) = H$, $S \cong G/H$ by(4.12.1.22) and(11.10.1.53). Then(18.1.5.6) shows T is just the G-invariant measure on $G/H : T\varphi = \int_{G/H} \varphi(\gamma(g)s)$. Now condition4 and2 shows σT is also G-invariant, thus $\sigma T = cT$. Clearly $c \geq 0$, and condition3 shows $c^n = 1$, thus $c = 1$. □

Hecke Algebra

This is a continuation of Hecke Algebras.

Def. (18.1.5.12) [Hecke Algebras of Locally Profinite Groups]. The algebra $\mathcal{H}(G)$ of test functions(4.4.4.10) on a locally profinite group G under convolution is an algebra, called the **Hecke algebra** of G. And for a compact open subgroup K of G, $\mathcal{H}_K$ is the subspace of K-bi-invariant functions in $\mathcal{H}(G)$.

Notice $\mathcal{H} = \cup_K \mathcal{H}_K$ by(18.1.5.2). Also $\mathcal{H}_K$ has a unit $e_K = \mu(K)^{-1}\chi_K$. This is easily verified.

Then $\mathcal{H}_G$ is an idempotented algebra(3.6.4.2). ⌟

Proof: Define the set $\mathcal{E}$ of idempotents in $\mathcal{H}(G)$ as e_K, where K is compact open in G. The fact that $\mathcal{H}$ is an idempotented algebra follows from(18.1.5.13) and(18.1.5.15). □

Prop. (18.1.5.13) [Point Measure]. Consider the point measure δ_g for $g \in G$, it is not an element in $\mathcal{H}(G)$, but it can convolute on $\mathcal{H}(G)$: $(\delta_g * \varphi)(x) = \varphi(g^{-1}x), (\varphi * \delta_g)(x) = \varphi(xg)$. Then

- If $g \in K$, then $\delta_g * e_K = e_K * \delta_g = e_K$.
- $\delta_g * e_K * \delta_{g^{-1}} = e_{gKg^{-1}}$.
- If $K = K_1K_2$ is an open subgroup, then $e_{K_1} * e_{K_2} = e_K$. In particular, $e_K * e_K = e_K$.

⌟

Remark (18.1.5.14). In fact we should define the Hecke algebra as locally constant distributions on G, then there equations are more natural. This algebra is equivalent to Hecke algebra by $f \mapsto f\mu_G$. ⌟

Prop. (18.1.5.15). $\mathcal{H}_K = e_K * \mathcal{H} * e_K = \mathcal{H}[e_K]$. ⌟

Proof: Notice by(18.1.5.13), functions in $e_K * \mathcal{H} * e_K$ is clearly K-bi-invariant. For the other direction, notice if φ is left and right K-invariant, then $\varphi = e_K * \varphi = \varphi * e_K = e_K * \varphi * e_K$. □

Prop. (18.1.5.16) [Smooth Representations and $\mathcal{H}$-Modules]. For a smooth representation (π, V) of G, for any v, $g \mapsto \pi(g)v$ can be regarded as a locally constant function with value in V, thus for any $\varphi \in \mathcal{H}_G$, $g \mapsto \varphi(g)\pi(g)v$ is locally constant with compact support, thus we can define a representation of the Hecke algebra $\mathcal{H}_G$ by

$$\pi(\varphi)v = \int_G \varphi(g)\pi(g)v dg$$

which just has nothing to do with integration, and this is compatible with convolution by formal reason. Then this is a smooth $\mathcal{H}_G$-module, and this gives an equivalence between the category of smooth(admissible) representations of $\mathcal{H}(G)$(3.6.4.4) and the category of smooth(admissible) representations of G. ⌟

Proof: For any $v \in V$, there is an open compact subgroup K that $v \in V[e_K]$, thus $e_K v = v$, so V is smooth. For the equivalence of categories, for any $\mathcal{H}(G)$-module V, we can define a G-action by linearly extending the action $\pi(g)e_K v = (\delta_g * e_K)v$. Notice by associativity of representation and smoothness, this is well-defined on all of V, and is a representation of G. Also it is continuous because $v = e_K v$ for some K thus $\pi(g)v = (\delta_g * e_K)v = e_K v = v$ for any $g \in K$. Finally these two functors are inverse to each other is also easily checked. □

Cor. (18.1.5.17). $(-)^K, (-)^\infty$(18.1.2.1) are both exact, by(3.6.4.3). ⌟

Cor. (18.1.5.18). Let (π, V) be a non-zero smooth representation of a locally profinite group G, then the following are equivalent by(3.6.4.6) and(18.1.5.16):

- π is irreducible.
- V is simple as $\mathcal{H}$-module.
- V^{K_0} is either zero or simple as a $\mathcal{H}_{K_0}$-module for all open compact subgroups K_0 of G.

⌟

Prop. (18.1.5.19) [Fourier Transform]. If G is a locally profinite Abelian group, then the Fourier transform induces an isomorphism

$$\mathcal{H}(\widehat{G}) \cong C_c^\infty(G) : \varphi \mapsto \widehat{\varphi}(\xi) = \int_G \varphi(y)\overline{\langle \xi, y\rangle} dy.$$

⌟

Proof: By(11.10.3.8) this is an algebra homomorphism. It remains to show that the image are all locally compact, and this is clear from the fact $\widehat{G}$ is given the compact-open topology(11.10.3.6). □

Admissible Smooth Representations

Prop. (18.1.5.20).

- For any compact open subset K of G, $V^K = ((V^\wedge)^K)^*$.
- $\mathrm{Hom}_G(V, W^\wedge) = \mathrm{Hom}(W, V^\wedge)$.
- $V \hookrightarrow (V^\wedge)^\wedge$ is an injection.

⌟

Proof: 1: Using(18.1.5.16), because $(\widetilde{V})^K = V^{*K}$. There is a homomorphism $V^{*K} \to V^{K*}$, it is injective, because if $f(v) = 0$ for each $v \in V^K$, then $f(w) = f(e_K v) = 0$. It is also injective, because for each $f \in V^{K*}$, the inverse image is $g(w) = g(e_K w)$.

2: $\mathrm{Hom}(V, \widetilde{W}) = \mathrm{Hom}(V, W^*) = \mathrm{Hom}(V \otimes W, \mathbb{C})$.

3: by the proof of item1,

$$\widetilde{\widetilde{V}} = \cup_K((\cup_K V^{*K})^{*K}) = \cup_K((\cup_K V^{*K})^{K*}) = \cup_K(V^{*K*}) = \cup_K(V^{K**}).$$

So the filtered colimits of the injections $V^K \to (V^K)^{**}$ gives an injection $\cup_K(V^{K**})$. □

Cor. (18.1.5.21) [Contragradient Functor is Exact]. The contragradient functor $V \mapsto \widehat{V}$ is exact. Because $(-)^*$, $(-)^\infty$ are all exact(18.1.5.17). ⌟

Cor. (18.1.5.22). If P is projective in $\mathcal{M}(G)$, then $\widetilde{P}$ is injective in $M(G)$. ⌟

Proof: $\mathrm{Hom}(X,\widetilde{P})=\mathrm{Hom}(P,\widetilde{X})$, and notice that the contragradient functor is exact(18.1.5.21). □

Def. (18.1.5.23) [Admissible Representations]. An **admissible smooth representation** of a locally profinite group G is a smooth representation that for any compact open subgroup K of G, V^K is of f.d.. The category of admissible smooth representation of G is denoted by $\mathrm{Rep}^{\mathrm{adm}}(G)$.

Then a smooth representation is admissible iff $V\cong (V^\wedge)^\wedge$. In particular, the contragradient of an admissible representation is admissible. ⌟

Proof: If V^K is of f.d. for each K, then by the proof of item3 of(18.1.5.20), $V\cong\widetilde{\widetilde{V}}$. Conversely, if $V\cong\widetilde{\widetilde{V}}$, then $V^K\cong V^{K**}$, thus V must be finite, by(3.5.3.9). □

Cor. (18.1.5.24). For an irreducible admissible representation, the contragradient is also irreducible admissible.

Extensions of admissible representations are admissible, by(18.1.5.17). ⌟

Prop. (18.1.5.25) [Decomposition of Admissible Representations]. Let K be a compact open subgroup of G, then any smooth representation of G decomposes as

$$V=\bigoplus_{\rho\in\mathrm{Rep}(K)}V^\rho,$$

and V is admissible iff each V^ρ are all of f.d. In particular, this shows the two notations of admissible(locally compact group and locally profinite groups) are compatible for smooth representations. ⌟

Remark (18.1.5.26). WARNING: The decomposition theorem of compact groups cannot be directly used, as representation may not be of f.d. so may not be unitarizable. ⌟

Proof: Firstly $V\subset\sum_{\rho\in\widehat{K}}V(\rho)$, because any $v\in V$ is fixed by some compact open subgroup K_0 of K, and we can choose K_0 to be normal in K by(4.12.1.6), so for $\Gamma=K/K_0$,

$$v\in V^{K_0}=\oplus_{\rho\in\widehat{\Gamma}}V(\rho)\subset\sum_{\rho\in\widehat{K}}V(\rho).$$

Also this sum is direct, because otherwise $\sum_{\rho\in S}c_\rho v_\rho=0$, but let K_0 be the intersection of kernels of ρ, then this is an equation of elements in representations of $\Gamma=K/K_0$ finite, so contradicting(18.1.3.8).

If π is admissible, then $V(\rho)\subset V^{\ker\rho}$ is of f.d.. Conversely, if V is not admissible, then V^{K_0} is of infinite dimensional for some K_0 compact compact normal, so V^{K_0} decomposes as direct sums of $V(\rho)$ for $\rho\in\widehat{K/K_0}$, thus one of these space must be of infinite dimensional. □

Def. (18.1.5.27) [Character of Admissible Representations]. Let (π,V) be an admissible representation of G, then for any $\varphi\in\mathcal{H}$, $\varphi\in\mathcal{H}_K$ for some compact open subset of G, by(18.1.5.12), so $\mathrm{Im}(\pi(\varphi))\subset V^K$, which is of f.d., so we can define the trace of φ as $\mathrm{tr}(\pi(\varphi)|V^K)$. Notice this is independent of K chosen by linear algebra reasons. And this defines a distribution on $\mathcal{H}:\varphi\mapsto\mathrm{tr}(\varphi)$, called the **character** of V. ⌟

Cor. (18.1.5.28). $\mathcal{M}(G)$ has enough injectives. ⌟

Proof: As $\mathcal{M}(G)$ has enough projectives(3.6.4.9)(18.1.5.16), there is a surjection $P\to\widetilde{X}$, thus an injection $\widetilde{\widetilde{X}}\hookrightarrow\widetilde{P}$(18.1.5.21). Now $X\hookrightarrow\widetilde{\widetilde{X}}$ by(18.1.5.20). □

Irreducible Admissible Representations

Prop. (18.1.5.29) [Separation Lemma]. If G is a σ-compact locally profinite group, then for any $0 \neq h \in \mathcal{H}(G)$, there is an irreducible representation ρ that $\rho(h) \neq 0$. ⌟

Proof: Cf.[Bernstein, P20], [Bernstein-Zelevinsky, P19].? □

Prop. (18.1.5.30) [Shur's Lemma].

- If G is a σ-compact locally profinite group, then any irreducible smooth representation V is of at most countable dimension, thus $\mathrm{End}_G(V) = \mathbb{C}$ by(3.2.1.10).
- If G is a locally profinite group, then any irreducible admissible representation V of G satisfies $\mathrm{End}_G(V) = \mathbb{C}$.

⌟

Proof: 1: If it is of at most finite dimension because if ξ generate V, then notice its stablizer is compact open, and G is σ-compact, so V is at mots countable.

2: Let K_0 be a small open compact subgroup that $V^{K_0} \neq 0$, then V^{K_0} is of f.d. and preserved under $T \in \mathrm{End}_G(V)$, thus T has an eigenvalue c, thus $T = cI$ on V. □

Prop. (18.1.5.31). Let $(\pi_1, V_1), (\pi_2, V_2)$ are two irreducible representations of a locally profinite group G. If $V_1^K \cong V_2^K \neq 0$ as $\mathcal{H}_K$-module for some compact open subgroup K of G, then $\pi_1 \cong \pi_2$. This follows immediately from(3.6.4.7). ⌟

Prop. (18.1.5.32) [Characters Determine Irreducible Admissible Representations]. Let $\pi_1, \ldots, \pi_n$ be inequivalent irreducible admissible representations of a locally profinite group G, then their characters $\mathrm{tr}(\pi_i)$ are linearly independent. In particular, an irreducible admissible representation is determined by its character. ⌟

Proof: Choose K that $V_i^K \neq 0$ for any i, the hypothesis together with(18.1.5.31) shows $V_i^K \not\cong V_j^K$. Then we finish by(11.10.4.22). □

Prop. (18.1.5.33) [Representations of Product Group]. If G_1, G_2 are all locally profinite groups and (π_i, M_i) are irreducible admissible representations of G_i, then $M_1 \otimes M_2$ is an irreducible admissible representation of $G_1 \times G_2$, and any irreducible admissible representations of $G_1 \times G_2$ comes like this. ⌟

Proof: By(18.1.5.16) and(3.6.4.15), this follows if we have $\mathcal{H}_{G_1 \otimes G_2} \cong \mathcal{H}_{G_1} \otimes \mathcal{H}_{G_2}$. And this fact is easily deduced from(4.4.4.12). □

Induced Representations and Mackey Theory

Def. (18.1.5.34) [Smooth Induced Representations]. Let G be a locally profinite group and H is a closed subgroup, (π, V) be a smooth representation of H, we can define the **smooth induced representation** $\mathrm{Ind}_H^G \pi$ as the space of locally constant f on G with values in V

$$f(hg) = \sqrt{\frac{\Delta_G(h)}{\Delta_H(h)}} \pi(h) f(g).$$

with the natural right G-representation. Notice this is similar to that of unitary representations of locally compact groups, in(11.10.5.3).

the induced representation $\mathrm{Ind}_H^G \pi$ has a subrepresentation ind_H^G consisting of functions that is compactly supported in $H \backslash G$, called the **compactly induced representation**. ⌟

Remark (18.1.5.35). The normalized factor here is used to make the induction of a unitarizable representation unitarizable(18.1.5.45). ⌟

Prop. (18.1.5.36) [Description of the Induced Representations]. Situation as in(18.1.5.34). Let $K\subset G$ be an open compact subgroup, and $\Omega\subset G$ be a system of coset representations of $H\backslash G/K$. For each $g\in G$, denote $N_g=H\cap gKg^{-1}$ the compact open subgroup of H, then the restriction of functions from G to Ω induces an isomorphism of $(\mathrm{Ind}_H^G(V))^K$ with the $\prod_{g\in\Omega}V^{N_g}$. And in this way, $(\mathrm{ind}_H^G(V))^K$ is mapped to $\bigoplus_{g\in\Omega}V^{N_g}$. ⌟

Prop. (18.1.5.37). Let G be a locally profinite group, H a closed subgroup of G, and B a closed subgroup of H, then

- Ind_H^G and ind_H^G are both exact functors $\mathrm{Rep}^{\mathrm{alg}}(H)\to\mathrm{Rep}^{\mathrm{alg}}(G)$.
- $\mathrm{Ind}_H^G\circ\mathrm{Ind}_B^H=\mathrm{Ind}_B^G$ and $\mathrm{ind}_H^G\circ\mathrm{ind}_B^H=\mathrm{ind}_B^G$.
- $\mathrm{Ind}_H^G(\sigma)^\vee=\mathrm{ind}_H^G(\sigma^\vee)$.
- (Smooth Frobenius Reciprocity)If $(\pi,W)\in\mathrm{Rep}^{\mathrm{alg}}(G)$, $(\rho,V)\in\mathrm{Rep}^{\mathrm{alg}}(H)$, then there are functorial isomorphisms

$$\mathrm{Hom}_G(\pi,\mathrm{Ind}_H^G(\rho))=\mathrm{Hom}_H(\pi|_H,\rho\otimes\sqrt{\frac{\Delta_G}{\Delta_H}}),\quad \mathrm{Hom}_G(\mathrm{ind}_H^G(\sigma),\pi)=\mathrm{Hom}_H(\rho\otimes\sqrt{\frac{\Delta_H}{\Delta_G}},(\pi^\vee|_H)^\vee)$$

⌟

Proof: 1: This follows from the description in(3.6.4.3) and(3.6.4.3) by taking colimits.

2: For simplicity we prove for G,H,B unimodular. An element in $\mathrm{Ind}_H^G\circ\mathrm{Ind}_B^H(V)$ is an element $\varphi:G\mapsto\mathrm{Hom}(H,V)$ that satisfies $\varphi(hg)(h')=(\pi(h)\varphi(g))(h')=\varphi(g)(hh')$, thus $\varphi(g)(h)=\varphi(hg)(1)$. Let $\Phi(g)=\varphi(g)(1)$, then Φ satisfies $\Phi(bg)=\pi(b)\Phi(g)$. So $\varphi\mapsto\Phi$ is an isomorphism. ind case follows from item3.

3: For $f:G\to V\in\mathrm{Ind}_H^G(\sigma),f'\in G\to V^\vee\in\mathrm{ind}_H^G(\sigma^\vee)$, $\langle f,f'\rangle$ is compactly supported in $H\backslash G$, and $\langle\pi(h)f,\pi(h)f'\rangle=\frac{\Delta_G(h)}{\Delta_H(h)}\langle f,f'\rangle$, thus we can define a G-invariant pairing

$$\langle f,f'\rangle=\int_{H\backslash G}\langle f(g),f'(g)\rangle d\mu_{H\backslash G}(g)(11.10.1.44).$$

This map is a perfect pairing on the K-fixed part for any compact open K using description in(18.1.5.36), thus we are done.

4: Given a $\Phi:W\to\mathrm{Ind}_H^G V$, we have a map $\varphi:W\to V:\varphi(w)=\Phi(w)(1)$, then it is verified that $\varphi\in C(\pi|_H,\rho\otimes\sqrt{\frac{\Delta_G}{\Delta_H}})$. Conversely, if $(\varphi:W\to V)\in C(\pi|_H,\rho\otimes\sqrt{\frac{\Delta_G}{\Delta_H}})$ is given, we can define $\Phi;W\to\mathrm{Ind}_H^G V:\Phi(w)(g)=\varphi(\pi(g)w)$, then $\Phi(w)\in\mathrm{Ind}_H^G V$ and this is linear in w(remember to check smoothness). Finally, it is easily verified these maps are inverse to each other. The second assertion follows from item3 and(18.1.5.20). □

Cor. (18.1.5.38). If $H\backslash G$ is compact, then $\mathrm{Ind}_H^G=\mathrm{ind}_H^G$, and they map admissible representations to admissible representations, by the description in(3.6.4.3), as $H\backslash G/K$ is both compact and discrete thus finite. ⌟

Prop. (18.1.5.39). If H is normal in G and for any $\rho\in\mathrm{Rep}(H)$, let ρ^g be ρ twisted by conjugation of $g\in G$, then $\mathrm{Ind}_H^G(\rho)\cong\mathrm{Ind}_H^G(\rho^g)$, and $\mathrm{ind}_H^G(\rho)\cong\mathrm{ind}_H^G(\rho^g)$ ⌟

Proof: □

Prop. (18.1.5.40). Let $H \leq G, K \trianglelefteq G, \rho \in \mathrm{Rep}(H)$, then

$$(\mathrm{Ind}_H^G(\rho))^K \cong \mathrm{Ind}_{H/H\cap K}^{G/K}(\rho^{H\cap K}) \in \mathrm{Rep}^{\mathrm{alg}}(G/K)$$

⌟

Proof: □

Prop. (18.1.5.41). Let G be a locally profinite group and H is a closed subgroup, (π, V) be a smooth representation of H, then there is a G-invariant map $P_\pi : C_c^\infty(G) \otimes V \to \mathrm{ind}_H^G(\pi)$:

$$P_\pi(\varphi, v)(g) = \int_H \varphi(b^{-1}g)\sqrt{\frac{\Delta_G(b)}{\Delta_H(b)}}\pi(b)vdb.$$

And if $\dim \pi < \infty$ and there is an open compact subgroup K of G that $G = HK$, then this map is surjective.

Moreover,

$$P(\lambda(b)^{-1}\varphi, v) = \sqrt{\Delta_G(b)\Delta_H(b)}P(\varphi, \pi(b)v), \quad b \in H$$

⌟

Proof: It can be verified that $P_\pi(\varphi, v)(bg) = \sqrt{\frac{\Delta_G(b)}{\Delta_H(b)}}\pi(b)P_\pi(\varphi, v)$.

If $H\backslash G$ is compact, by(11.10.1.52), there is a compact open subset K of G that $G = HK$, then for any $f \in \mathrm{Ind}_H^G(\pi) = \sum v_i \otimes f_i$, consider $\varphi_i = \chi_{K^{-1}} f_i$, then $\sum P(\varphi_i, v_i) = \sum V(H\cap K) f_i v_i = V(H \cap K)f$. □

Prop. (18.1.5.42) [Mackey's Decomposition]. Let H, K be closed subgroups of a locally profinite group G, ρ is a smooth representation of H. If $s \in G$, then we can define a new representation of $H_s = K \cap sHs^{-1}$ as $\rho^s(g) \mapsto \rho(s^{-1}gs)$. Then if we use unnormalized induction,

- If either H or K is open in G, then
$$\mathrm{res}_K^G \mathrm{ind}_H^G \rho \cong \bigoplus_{s\in H\backslash G/K} \mathrm{ind}_{H_s}^K \rho^s$$
- If K is open in G, then
$$\mathrm{res}_K^G \mathrm{Ind}_H^G \tau \cong (\prod_{s\in H\backslash G/K} \mathrm{Ind}_{H_s}^K \tau^s)^\infty$$

⌟

Proof: Cf.[Yam22]. □

Cor. (18.1.5.43) [Mackey's Intertwining Theorem]. Let H be a closed subgroup of a locally profinite group G, K an open subgroup of G, σ(resp. τ) be a smooth representation of K(resp. H), define τ^s as in(18.1.5.42), then if we use unnormalized induction,

- $$\mathrm{Hom}_G(\mathrm{ind}_K^G \sigma, \mathrm{Ind}_H^G \tau) \cong \prod_{s\in H\backslash G/K} \mathrm{Hom}_{H_s}(\sigma, \tau^s).$$
- If moreover $H\backslash HgK \cong H_s\backslash K$ is compact for any $g \in G$(e.g. K is compact) and σ is f.g. over K, then
$$\mathrm{Hom}_G(\mathrm{ind}_K^G \sigma, \mathrm{ind}_H^G \tau) \cong \bigoplus_{s\in H\backslash G/K} \mathrm{Hom}_{H_s}(\sigma, \tau^s).$$

⌟

Proof: 1: This is a direct consequence of Mackey's decomposition(18.1.5.42) and Frobenius reciprocity(18.1.5.37):

$$\begin{aligned}\mathrm{Hom}_G(\mathrm{ind}_K^G\sigma,\mathrm{Ind}_H^G\tau)&\cong\mathrm{Hom}_K(\sigma,\mathrm{res}_K^G\mathrm{Ind}_H^G\tau)\cong\mathrm{Hom}_K(\sigma,(\prod_{s\in H\backslash G/K}\mathrm{Ind}_{H_s}^K\tau^s)^\infty)\\&\cong\mathrm{Hom}_K(\sigma,\prod_{s\in H\backslash G/K}\mathrm{Ind}_{H_s}^K\tau^s)\cong\prod_{s\in H\backslash G/K}\mathrm{Hom}_K(\sigma,\mathrm{Ind}_{H_s}^K\tau^s)\\&\cong\prod_{s\in H\backslash G/K}\mathrm{Hom}_{H_s}(\sigma,\tau^s).\end{aligned}$$

2 is similar. □

Cor. (18.1.5.44) [Compact Induction Admissible]. If H is a subgroup of G that $H\backslash G$ is compact, then Ind_H^G takes admissible representations to admissible representations. ⌟

Proof: For any compact open subgroup $K\subset G$, $H\backslash G/K$ is finite, as $H\backslash G$ is compact and K is open, then by Mackey's decomposition(18.1.5.42), $(\mathrm{Ind}_H^G\rho)^K=\oplus_{s\in H\backslash G/K}\rho^{s^{-1}Ks\cap H}$ is of f.d. if ρ is admissible. □

Unitarizable Admissible Representations

Prop. (18.1.5.45). The induction of a unitarizable representation is unitarizable, by(11.10.5.3). ⌟

Prop. (18.1.5.46)[Converse of Schur's Lemma]. If (π,V) is a unitarizable admissible representation of a locally profinite group G that $\mathrm{Hom}_G(V,V)=\mathbb{C}$, then π is irreducible. ⌟

Proof: Cf.[Bump, P523].? □

Compact Representations

Def. (18.1.5.47) [Compact Representations]. For a locally profinite group G, a **compact representation** is a smooth representation of G s.t. for every $\xi\in V$ and every compact open subgroup $K\subset G$, the function $D_{\xi,K}:G\to V:g\mapsto\pi(e_K)\pi(g^{-1})\xi$ has compact support. ⌟

Prop. (18.1.5.48). $V\in\mathrm{Rep}^{\mathrm{alg}}(G)$ is compact iff every matrix coefficient of V is compactly supported. And every f.g. compact representation is admissible. ⌟

Proof: If V is compact, for any $\xi\in V,\xi^\wedge\in V^\wedge$, $\xi^\wedge\in(V^\wedge)^K$, then $\mathrm{Supp}\,\varphi_{\xi,\xi^\wedge}\in\mathrm{Supp}\,D_{\xi,K}$ is compact.

For the converse, Cf.[Bernstein Zelevinsky, P26]. □

18.2 Modular Representations

Main references are [Ser77] and [Bon11].

1 Block Theory

See [Bon11].

2 Mixed Characteristic

3 Equal Characteristic

Prop. (18.2.3.1). The only irreducible representation of a p-group over a a field of char p is the trivial representation. ⌟

Proof: For any $v \in V$, consider the additive subgroup generated by $g(s)v$, then it is a finite group of prime power order. Then(3.1.6.4) shows it has a element other than 0 fixed by all G, thus it is not irreducible unless trivial representation. □

18.3 Galois Representations(Basics)

Main references are [Theories of p-adic Galois Representations, Fontaine/Yi Ouyan], [Local Langlands for GL(n), Zijian Yao]. [Con06], [R. Taylor, Galois representations, long version of the talk given at the iCM 2002].

Notation (18.3.0.1).

- Use notations defined in Classical Representation Theory.
- Use notations defined in Cohomology of Arithmetic Fields.

⌟

Remark (18.3.0.2). For $K \in \texttt{Field}$, $E \in \texttt{Field}^{\text{top}}$, the theory of Galois representations study the category $\text{Rep}_E(\text{Gal}_K)$. ⌟

1 Basics

Def. (18.3.1.1) [Galois Representations]. For any $K \in \texttt{Field}, p \in \mathbf{P}$,

- an **Artin representation** of K is a f.d. smooth $\mathbb{C}$-representation of Gal_K.
- a **p-adic Galois representation** of K is a f.d. continuous $\mathbb{Q}_p$-representation of Gal_K. If $K \in p\text{-}\texttt{LField}$, this is called a **$p$-adic local Galois representation**(of K).
- a **p-adic integral Galois representation** of K is a f.d. continuous $\mathbb{Q}_p$-representation of Gal_K. If $K \in p\text{-}\texttt{LField}$, this is called a **$p$-adic local integral Galois representation**(of K).
- if $K \in p\text{-}\texttt{LField}, \ell \in \mathbf{P}\backslash\{p\}$, then an **$\ell$-adic Galois representation** of K is a f.d. continuous $\mathbb{Q}_\ell$-representation of Gal_K.

⌟

Cor. (18.3.1.2) [Artin Representations as ℓ-adic(or p-adic) Representations]. A choice of isomorphism(14.2.1.27) $\overline{\mathbb{Q}}_p \cong \overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ induces a bijection between Artin representations and ℓ-adic(or p-adic) representations with open kernels. ⌟

Prop. (18.3.1.3) [Compact Groups Stabilize a Lattice]. Let Γ be a compact group and let $\rho : \Gamma \to GL(n, \overline{\mathbb{Q}}_p)$ be a continuous homomorphism, then there exists a finite extension $L/\mathbb{Q}_p$ that $\rho(\Gamma) \subset GL(n, L)$, and up to conjugation, $\rho(\Gamma) \subset GL(n, \mathcal{O}_L)$, or equivalently, Γ fixes a $\mathcal{O}_L$-lattice. ⌟

Proof: Notice $\rho(\Gamma)$ is compact and Hausdorff, so by Baire category theorem, now that $GL(n, L)$ is closed in $GL(n, \overline{\mathbb{Q}}_p)$ for all $L/\mathbb{Q}_p$ finite, and all this extensions are countable by primitive element theorem, so there is an L that $\rho(\Gamma) \cap GL(n, L)$ contains an open subset of $\rho(\Gamma)$, so it is an open subgroup, thus of finite index, hence by adding all the coset representations into L, we get an L' finite.

For the second assertion, notice $\rho(\Gamma)$ is compact in $GL(n, L)$, thus by(15.4.1.5), it is conjugate to $GL(n, \mathcal{O}_L)$. □

Prop. (18.3.1.4) [Brauer-Nesbitt]. If two n-dimensional representations have the same char polynomial and char $k = 0$, or char $k > n$ and they have the same character, then their semisimplification are the same. ⌟

Proof: The proof is not hard, use the Artin-Wedderburn theorem, and the fact the representation may not by semisimple. □

Def. (18.3.1.5)[Restricted Galois Representations]. By(14.4.1.18), if $F \in \texttt{GField}$, for any $v \in \Sigma_F$, a Galois representation ρ of F can be restricted to a Galois representations ρ_v of Gal_{F_v}, called the **restricted Galois representation**. ⌟

Def. (18.3.1.6) [Cyclotomic Characters and Tate Twists]. For $K \in \texttt{Field}, p \in \mathbf{P}$, the p-adic **cyclotomic character** χ_p of Gal_K is the character corresponding to the 1-dimensional p-adic Tate module of $\mathbb{G}_{a,K}$.

For any $(\rho, V) \in \mathrm{Rep}_{\mathbb{Z}_p}(\mathrm{Gal}_K)$ or $(\rho, V) \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$ and $n \in \mathbb{Z}$, we can define the **Tate twist** $\rho(n)$ as the representation twisted by n-th power of the cyclotomic character χ_p^n. ⌟

Def. (18.3.1.7)[Tate Duals]. For a p-adic representation V of the Galois group of a field K, the **Tate dual** V^D of V is defined to be $V^D = V^\vee(1)$. Similarly for p-adic integral representations. ⌟

Def. (18.3.1.8)[Properties of Galois Representations]. Let ρ be a representation of $\mathrm{Gal}_\mathbb{Q}$ on some topological ring A, then

- ρ is called an **odd representation** if $\rho(\mathtt{c}) = -1$, and an **even representation** otherwise.
- For $p \in \mathbf{P}$, ρ is said to be **unramified at** p if $I_p \subset \ker(\rho|_{\mathrm{Gal}_{\mathbb{Q}_p}})$.
- For $p \in \mathbf{P}$, ρ is said to be **flat at** p if for any Artinian quotient A/I of A, the quotient representation $\overline{\rho}|_{\mathrm{Gal}_{\mathbb{Q}_p}}$ is isomorphic to the representation of $\mathrm{Gal}_{\mathbb{Q}_p}$ on the geometric points of a finite flat group scheme over $\mathbb{Z}_p$.

⌟

2 ℓ-adic (Local)Galois Representations

Def. (18.3.2.1) [Notations].

- Let $p \in \mathbf{P}, q \in p^{\mathbb{Z}_+}$, $K \in p\text{-}\texttt{NField}$ with residue field $\mathbb{F}_q$.
- Let $\ell \in \mathbf{P} \setminus \{p\}$.
- $t_\ell : I_K/R_K \to \mathbb{Z}_\ell$ be the ℓ-adic tame character(14.2.3.20).
- Let σ be a fixed lift of $\mathrm{Frob} \in \mathrm{Gal}_{\mathbb{F}_q}$.
- Let $\chi = \chi_\ell$ be the unramified cyclotomic character(18.3.1.6) $\widehat{\mathbb{Z}} \cong \mathrm{Gal}_K / I_K \to \mathbb{Z}_\ell : \sigma \mapsto q$.

⌟

Prop. (18.3.2.2). If $\rho : \Gamma \to GL(n,k) = GL(V)$ is a representation, then it has a filtration $0 = V_0 \subset V_1 \subset \ldots \subset V_n = V$ where V_{i+1}/V_i is irreducible, then there is a semisimplification of ρ, which is $\rho^{ss} = \oplus V_{i+1}/V_i$. ⌟

Def. (18.3.2.3) [Residential Representation]. If $L/\mathbb{Q}_p$ finite, we may take a Γ-stable $\mathcal{O}_L$-lattice Γ, then the **residual representation** $\overline{\rho}_L$ is defined by $\Gamma \to GL(\Lambda/\pi\Lambda)$. Then the semisimplification of $\overline{\rho}_L$ is independent of Λ chosen.**?** ⌟

Prop. (18.3.2.4) [Induced Galois Representations]. Let F be a local field with residue characteristic p. Let $(n, q) = 1$, then any irreducible representation (ρ, V) of Gal_F of dimension n is induced from a character χ of K^* for a field extension K/F of degree n. ⌟

Proof: Suppose χ factors through a normal subgroup $G(L/F)$. It suffices to show ρ is an induced representation from a subgroup, then use induction. Suppose it is not, then consider the filtration of Galois groups $R_v \subset I_v \subset G_F$. R_v is a pro-p-group, thus all irreducible f.d. representations are p-powers, by(18.1.3.12), thus it is 1-dimensional. Now R_v is a normal subgroup, by(18.1.2.10), R_v acts by scalars on V. Now the exact sequence $1 \to R_v \to I_v \to I_v/R_v \to 0$ is a split exact sequence(14.2.2.17), and I_v/R_v is cyclic, thus $\rho|_{I_v}$ also contains a character, and the same argument as above shows I_v acts by characters. Then a twist of ρ factors through G/I_v, which is a cyclic group, contradiction. □

Thm. (18.3.2.5). Let K be a p-adic field with residue field k and $k = \overline{k}$, then any $\rho \in \mathrm{Rep}_{\mathbb{Q}_\ell}^{\mathrm{pot.\,st}}(\mathrm{Gal}_K)$ comes from geometry. ⌟

Proof: Cf.[Fontaine, Galois Rep]P12.**?** □

Weil Representations

References are [Yao17].

Prop. (18.3.2.6)[Primitive Weil Representation]. $\pi \in \mathrm{Rep}^{\mathrm{alg}}(W_K)$ is called primitive if it is not induced from a representation of a proper subgroup. Then for any primitive representation of W_F, it factors through $C_{E/F}$ for some finite extension E/F by continuity, and by Clifford's theorem(18.1.2.10), the normal subgroup C_E acts by scalars, so the image of $W_{E/F}$ in $GL(V)$ is a finite group. ⌟

Def. (18.3.2.7) [Twisting Character of W_K]. For $s \in \mathbb{C}$, define the quasi-character $\omega_s : W_F \to \mathbb{C}^\times : x \mapsto ||x||^s$. ⌟

Prop. (18.3.2.8) [Twisting of Weil Representation]. For any $\rho \in \mathrm{Irr}^{\mathrm{alg}}(W_F)$, there exists some $s \in \mathbb{C}$ that $\omega_s \otimes \rho$ factors through $W_F \to G_F$. And for this s, $(\omega_s \otimes \rho)(W_F)$ is a finite subgroup of $GL(V)$. ⌟

Proof: $\ker(\rho|_{I_F})$ is an open subgroup of I_F. Conjugation by σ induces a permutation on the finite subgroup $\rho(I_F)$, so there is some n that $\rho^n = \mathrm{id}$ on $\rho(I_F)$, which means $\rho(\sigma^n)$ commutes with each elements of W_F, thus it is a scalar by Schur's lemma. Thus we can chose s that $(\omega_s \otimes \rho)(\sigma^n) = 0$, then $\omega_s \otimes \rho$ is trivial on $U = \langle \sigma^n, \ker(\rho|_{I_F}) \rangle$, which is a subgroup of W_F of finite index. Thus the image is finite.

Also the closed subgroup $\overline{U} = \overline{\langle \sigma^n, \ker(\rho|_{I_F}) \rangle} \subset \mathrm{Gal}_K$ if of finite index, and $\overline{U} \cap W_F = U$, thus $W_F/U \cong \mathrm{Gal}_F/\overline{U}$, and this representation extends to Gal_K. □

Cor. (18.3.2.9) [Galois-Type Representations]. As W_K is dense in Gal_K, $\mathrm{Rep}^{\mathrm{alg}}(\mathrm{Gal}_K) \subset \mathrm{Rep}^{\mathrm{alg}}(W_K)$ is a subcategory. The representations in this subcategory are called **representations of Galois-type**.

(18.3.2.8) shows $\mathrm{Rep}^{\mathrm{alg}}(\mathrm{Gal}_K)$ are almost the same as $\mathrm{Rep}^{\mathrm{alg}}(W_K)$. $\rho \in \mathrm{Rep}^{\mathrm{alg}}(W_K)$ is of Galois-type iff it has a finite image. ⌟

Prop. (18.3.2.10). Let ρ be a representation of W_K that $\rho(I_K)$ is finite, the following are equivalent:

- $\rho(\sigma)$ is semisimple for any $\sigma \in W_K$.
- $\rho(\varphi)$ is semisimple.
- ρ is a semisimple representation.

⌟

Proof: Cf.[Yao17]P4. □

Def. (18.3.2.11) [ℓ-Integral Representations]. For $\rho \in \mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(W_K)$, by(18.3.2.8), the eigenvalues of r are ℓ-adic units iff the eigenvalues of $\rho(\sigma) \in \mathcal{O}^*_{\overline{\mathbb{Q}}_\ell}$, iff the characteristic polynomial of $\rho(\sigma)$ are in $\mathcal{O}_{\overline{\mathbb{Q}}_\ell}[T]$ and $|\det(\rho(\sigma))| = 1$. Such a representation is called an **ℓ-integral representation**. ⌟

Def. (18.3.2.12) [Types of 2-Dimensional Representations]. By(18.3.2.6), any 2-dimensional representation of W_F has finite image in $\mathrm{PGL}(2,\mathbb{C}) \cong \mathrm{SO}(3,\mathbb{R})$(12.12.0.14). Thus by conjugacy into $\mathrm{SO}(3,\mathbb{R})$, the image is isomorphic to a cyclic, dihedral, tetrahedral, octahedral or icosahedral group by(12.12.3.1), called the **type of this Weil representation**. ⌟

Def. (18.3.2.13) [Dihedral Representation]. A **dihedral Weil representation** is a representation $W_F \to GL(2,\mathbb{C})$ that is induced from a quasi-character of W_E for some quadratic extension E/F. (What's the relation with(18.3.2.12)**?**) ⌟

Prop. (18.3.2.14) [Induced Weil Representations]. If $(p,n) = 1$ and $K \in p$-`NField`, then any irreducible representation $W_K \to GL(n,\mathbb{C})$ is induced from a quasi-character of W_E(equivalently $E^\times$) where E is a n-dimensional field extension E/F. ⌟

Proof: By(11.10.5.4), the class of such induced extensions are stable under twisting by ω_s, thus using(18.3.2.8), we can assume that the representation factors through $G(\overline{F}/F)$, thus through $G(K/F)$ for some finite extension K/F, thus the assertion follows from(18.3.2.4). □

Def. (18.3.2.15) [Artin Conductor]. For $(\rho, V) \in \mathrm{Rep}^{\mathrm{alg}}(W_K)$, define the **Artin conductor**

$$f(\rho) = f(\chi_\rho) = \sum_{i>0} \frac{1}{[G_0 : G_i]} \dim(V/V^{G_i})$$

where G_i are the higher ramification groups of G. ⌟

Def. (18.3.2.16) [Artin Conductors]. Let L/F be a Galois extension of global fields and $(\rho, V) \in \mathrm{Rep}(\mathrm{Gal}(L/F))$, for $v \in \Sigma_F^{\mathrm{fin}}$, let $G_v = G_{v,0} \supset G_{v,1} \supset \ldots \supset G_{v,m} = 0$ be higher ramification groups at v, then the **Artin conductor** of ρ is defined to be the ideal in $\mathcal{O}_F$:

$$\mathfrak{f}(\rho) = \prod_{v \in \Sigma_F^{\mathrm{fin}}} \mathfrak{p}_v^{a_v}, \quad a_v = \sum_{i \geq 0} \dim(V/V^{G_{v,i}}) \frac{\# G_{v,i}}{\# G_{v,0}}.$$

And we also define the **Swan conductor**

$$\mathfrak{b}(\rho) = \prod_{v \in \Sigma_F^{\mathrm{fin}}} \mathfrak{p}_v^{b_v}, \quad b_v = \sum_{i \geq 1} \dim(V/V^{G_{v,i}}) \frac{\# G_{v,i}}{\# G_{v,0}}.$$

⌟

Prop. (18.3.2.17) [Conductor-Discriminant-Formula]. For any Galois extension of global fields L/F,

$$\mathfrak{d}_{L/F} = \prod_{\rho \in \mathrm{Irr}(\mathrm{Gal}(L/F))} \mathfrak{f}(F, \rho)^{\chi_\rho(1)}$$

⌟

Proof: Cf.[Neu99]P534. □

Weil-Deligne Representations

Def. (18.3.2.18)[Weil-Deligne Groups]. The **Weil-Deligne group** WD_K is the group scheme $W_K \ltimes \mathbb{G}_a \in \mathcal{G}\mathrm{rp}/\mathbb{Q}$ given by the action

$$wxw^{-1} = |w|x.$$

⌟

Def. (18.3.2.19) [Deligne-Weil Representations]. For $L \in \mathtt{Field}^0$, the category $\mathfrak{wd}_L(W_K)$ of **Deligne-Weil representations** of W_K over L consists of triples (ρ, V, N), where $(\rho, V) \in \mathrm{Rep}_L^{\mathrm{alg}}(W_K)$ and $N \in \mathrm{End}(V)$ s.t.

$$\rho(x)N\rho(x)^{-1} = |x|\cdot N, \quad x \in W_K.$$

Equivalently, a Deligne-Weil representation is a smooth representation (ρ, V) of W_K together with a W_K-map $V \mapsto V(1)$(18.3.1.6).

Equivalenly, a Deligne-Weil representation is a representation of the group scheme WD_K(18.3.2.18) over L, by**??**.

N is necessarily nilpotent, and for an irreducible Weil-Deligne representation, $N = 0$.

$\mathfrak{wd}_{\mathbb{C}}(W_K)$ is also denoted by $\mathfrak{wd}(W_K)$. ⌟

Proof: Because $\sigma N\sigma^{-1} = q^{-1}\cdot N$, N has no non-zero eigenvalues, so N is nilpotent. □

Remark (18.3.2.20). Deligne-Weil representations are exactly the continuous representations of W_K, as will be illustrated in(18.3.2.26). ⌟

Def. (18.3.2.21). Define tensor product and inner Homs: $(\rho_1, V_1, N_1)\otimes(\rho_2, V_2, N_2) = (\rho_3, V_3, N_3)$ where

$$V_3 = V_1 \otimes V_2, \quad \rho_3(x)(v_1 \otimes v_2) = \rho_1(x)v_1 \otimes \rho_2(x)v_2, \quad N_3(v_1 \otimes v_2) = N_1(v_1) \otimes v_2 + v_1 \otimes N_2(v_2).$$

and also $\mathrm{Hom}((\rho_1, V_1, N_1), (\rho_2, V_2, N_2)) = (\rho_3, V_3, N_3)$ where

$$V_3 = \mathrm{Hom}(V_1, V_2), \quad (\rho_3(x)\varphi)(v_1) = \rho_2(x)(\varphi(\rho_1(x)^{-1}(v_1))), \quad (N_3\varphi)(v_1) = N_2(\varphi(v_1)) - \varphi(N_1(v_1)).$$

And also the dual $\rho^\vee = \mathrm{Hom}(\rho, \mathbb{1})$. ⌟

Def. (18.3.2.22) [F-Semisimple Representations]. $\rho = (\rho_0, V, N) \in \mathfrak{wd}_L(W_K)$ is called **F-semisimple** if (ρ_0, V) is semisimple. ⌟

Prop. (18.3.2.23)[$\mathrm{Sp}_m(\rho)$]. If $(\rho, V) \in \mathrm{Rep}^{\mathrm{alg}}(W_K)$ and $m \geq 0$, we can define $\mathrm{Sp}_m(\rho) \in \mathfrak{wd}(W_K)$ given by $\mathrm{Sp}_m(\rho) = V \oplus V(1) \ldots \oplus V(m-1)$ and N maps $V(i)$ isomorphically to $V(i+1)$ for $i < m-1$, and trivial on $V(m-1)$.

Then any representation that ⌟

Thm. (18.3.2.24) [Grothendieck's ℓ-adic Monodromy Theorem]. For $\ell \in \mathbf{P} \setminus \{p\}$ and $\rho \in \mathrm{Rep}_{\mathbb{Q}_\ell}(W_K)$,

- There exists an open subgroup $I_K' \subset I_K$ and a uniquely determined nilpotent operator $N \subset \mathrm{End}(V)$ s.t. for all $\sigma \in I_K'$, $\rho(\sigma) = \exp(t_\ell(\sigma)N)$.
- For any element $x \in W_K$,

$$\rho(x)N\rho(x^{-1}) = |\cdot|N.$$

⌟

Proof: Cf.[Fontaine, P12].**?** □

Cor. (18.3.2.25) [Potentially Unramified]. If ρ is a semisimple ℓ-adic continuous representation of W_K, then $\#\rho(I_K) < \infty$. ⌟

Proof: Choose a finite extension K'/K s.t. $I_{K'} \subset I'_K$, then $\rho|_{I_{K'}}$ is both unipotent and semisimple(18.1.2.10). □

Thm. (18.3.2.26) [ℓ-adic Deligne-Weil Representations, Deligne]. There is an equivalence of categories

$$\mathrm{WD} = \mathrm{WD}_p : \mathrm{Rep}^{\mathrm{fd}}(W_K) \cong \mathfrak{wd}(W_K)$$

$$(\rho, V) \mapsto (\rho_\sigma, V, N), \quad \rho_\sigma(\sigma^n x) = \rho(\sigma^n x)\exp(-t_\ell(x)N),$$

where N is given in(18.3.2.24).

Moreover, by(18.3.2.9) and (18.3.2.11), this map identifies

$$\mathrm{WD} : \mathrm{Rep}^{\mathrm{fd}}(\mathrm{Gal}_K) \cong \mathfrak{wd}^{\ell\text{-int}}(W_K),$$

and ρ is unramified iff $\mathrm{WD}(\rho)$ is unramified. ⌟

Proof: **?** This is a Weil-Deligne representation by(18.3.2.24). WD is a functor and is an equivalence by the uniqueness of N(18.3.2.24). □

Cor. (18.3.2.27). In the above situation, for $\rho \in \mathrm{Rep}_L(\mathrm{Gal}_K)$, the following are equivalent:

- ρ is semisimple.
- ρ is F-semisimple and $\rho(I_K)$ is finite.
- ρ' is F-semisimple and $N = 0$.

⌟

3 Mod ℓ Local Galois Representations

Notation (18.3.3.1). Use notation as in(18.3.2.1). ⌟

Def. (18.3.3.2) [Decomposed Generically]. Let $K \in p$-`LField` with residue field $\mathbb{F}_q$ and $\ell \in \mathbf{P}\backslash p$, an unramified representation

$$\overline{\rho} : \mathrm{Gal}_K \to \mathrm{GL}(n, \overline{\mathbb{F}_\ell})$$

is called **decomposed generically** if the eigenvalues $\{\lambda_1, \ldots, \lambda_n\}$ of $\overline{\rho}(\varphi)$ satisfies $\lambda_i/\lambda_j \notin \{1, q\}$ for any $1 \leq i \neq j \leq n$. ⌟

4 Representations from Geometry

Prop. (18.3.4.1). Let $k \in$ `Field` and $E \in \mathcal{E}\mathrm{ll}/k$, then for any $N \in \mathbb{Z} \cap k^\times$, there is an action of Gal_k on $E[N] \cong (\mathbb{Z}/(N))^2$, giving a representation

$$\rho_{E,N} : \mathrm{Gal}_k \mapsto \mathrm{GL}(2, \mathbb{Z}/(N)).$$

Let $\overline{\rho}_{E,N}$ denote the representation $\mathrm{Gal}_k \mapsto GL(2, \mathbb{Z}/(N))/\{\pm 1\}$. Then $\rho_{E,N}$ is surjective iff $\overline{\rho}_{E,N}$ is surjective. ⌟

Proof: Notice if $\overline{\rho}_{E,N}$ is surjective, then either $\begin{bmatrix} & -1 \\ 1 & \end{bmatrix}$ or $\begin{bmatrix} & 1 \\ -1 & \end{bmatrix}$ is in the image, thus -1 is in the image. □

Def. (18.3.4.2) [Tate modules representations]. For $\ell \in \mathbf{P}$, the action of Gal_k on the Tate module $T_\ell(E)$(15.7.6.15) is denoted by ρ_{E,ℓ^∞}. Equivalently,

$$\rho_{E,\ell^\infty} = \varprojlim_{n\in\mathbb{Z}_+} \rho_{E,\ell^n}.$$

If $\mathrm{char}\, k = 0$, we can assemble all the $T_\ell(E), \ell \in \mathbf{P}$ together to get a representation

$$\rho_E : \mathrm{Gal}_k \to \mathrm{End}(E(k^s)_{\mathrm{tor}}) \cong \mathrm{GL}(2, \widehat{\mathbb{Z}}).$$

⌟

Prop. (18.3.4.3) [Determinant of Tate Modules]. If (K, k) be a CDVR and $E \in \mathcal{E}\mathrm{ll}/K, \ell \in \mathbf{P} \setminus \{\mathrm{char}\, k\}$, then $\det(\rho_{E,\ell^\infty}) \cong \chi_\ell$(18.3.1.6), by Weil pairing(15.7.7.10). ⌟

Prop. (18.3.4.4) [Serre]. If $p \in \mathbf{P}$ and $\mathbb{Q}_p \subset_{\mathrm{fin}} K$ is a local field with ramification index e. Let $E \in \mathcal{E}\mathrm{ll}/K$ with semistable reduction, then if $2e < p - 1$, then the image of I_K under the projective representation associated to $\rho_{E,p}$ contains an element of order$\geq (p-1)/e$. ⌟

Proof: ? □

Thm. (18.3.4.5) [Serre]. Assume $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ is non-CM, then $\mathrm{Im}(\rho_E) \subset \mathrm{GL}(2, \widehat{\mathbb{Z}})$ has finite index. In particular, there exists $N \in \mathbb{Z}_+$ s.t. $\rho_{E,p}$ is surjective for any $p \geq N$. ⌟

Proof: Cf.[Abelian l-adic representations and elliptic curves, Serre].? □

Conj. (18.3.4.6) [Serre's Uniformity Problem]. There exists a number $N \in \mathbb{Z}_+$ s.t. for any $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ non-CM, $\rho_{E,p}$ is surjective for any $p \in \mathbf{P}_{\geq N}$. ⌟

Proof: □

5 Deformation of Galois Representations(Mazur)

Prop. (18.3.5.1). Let (A, k) be a Noetherian complete local ring and Π a profinite group. Then for any continuous representation $\rho : \Pi \to \mathrm{GL}(n; A)$,

$$\overline{\rho} : \Pi \to \mathrm{GL}(n; k)$$

is absolutely irreducible iff

$$r : A[[\Pi]] \to \mathrm{Mat}(n; A)$$

is surjecitve. ⌟

Proof: □

18.4 p-adic Local Galois Representations

Main references are [Berger, Galois representations and (φ,Γ)-modules], [Car19]. and [notes on p-adic Hodge, Conrad], [notes on p-adic Hodge, Serin Hong].

Notation (18.4.0.1).

- This is a continuation of the section Galois Representations(Basics).
- Use notations defined in Classical Representation Theory.
- Use notations defined in Untilts and Fargues-Fontaine Curves.
- Let K be a p-adic field with (perfect) residue field k,
- $K_0 = W(k)[\frac{1}{p}]$ its maximal unramified subextension.
- The Frobenius action on K_0 is denoted by σ.
- $K_\infty = K(\mu_{p^\infty})$, $\Gamma = \mathrm{Gal}(K_\infty/K)$.

⌟

1 $\mathbb{C}_K$-Admissibility

$\mathbb{C}_K$-Admissibility

Prop. (18.4.1.1) [Variant of Hilbert's Theorem90]. Any $V \in \mathrm{Rep}^{\mathrm{fd}}_{\widehat{K^{\mathrm{ur}}}}(\mathrm{Gal}(K^{\mathrm{ur}}/K))$ is trivial. In particular, any unramified f.d. representation of Gal_K is $\widehat{K^{\mathrm{ur}}}$-admissible thus $\mathbb{C}_p$-admissible, which is a special case of(18.4.1.2). ⌟

Proof: Denote by $\mathcal{O}$ the ring of integers of $\widehat{K^{\mathrm{ur}}}$ and $\mathfrak{m}$ the maximal ideal, Let W be a f.d. $\widehat{K^{\mathrm{ur}}}$-semi-linear representation, $(v_{1,0},\ldots,v_{d,0})$ a basis of W over $\widehat{K^{\mathrm{ur}}}$ and $\mathcal{O}_W$ the $\mathcal{O}$-span of $(v_{1,0},\ldots,v_{d,0})$, then we are going to construct a sequence of tuples $(v_{1,n},\ldots,v_{d,n})$ that $v_{i,n+1} \equiv v_{i,n} \mod \mathfrak{m}^n$ and $\mathrm{Frob}_q(v_{i,n}) \equiv v_{i,n} \mod \mathfrak{m}^n$ for all i and n.

Use induction on n: the case $n = 1$ follows from the fact $\mathcal{O}_W/\mathfrak{m}\mathcal{O}_W$ is trivial as a $\overline{k}$-semi-linear representation of Gal_k. To prove this, notice there is a finite extension l of k and an l-semi-linear representation W_L of $G_{l/k}$ that $\overline{k} \otimes_l W_l \cong \mathcal{O}_W/\mathfrak{m}\mathcal{O}_W$, then the assertion follows from Hilbert's theorem90(8.7.3.16).

For general n, we are looking for vectors $w_1,\ldots,w_d \in \mathcal{O}_W$ that $\mathrm{Frob}_q(v_{i,n} + \pi^n w_i) \equiv v_{i,n} + \pi^n w_i \mod \mathfrak{m}^{n+1}$, which is equivalent to $\mathrm{Frob}_q\overline{w_i} - \overline{w_i} = \frac{\mathrm{Frob}_q v_{i,n} - v_{i,n}}{\pi^n}$ in $\mathcal{O}_W/\mathfrak{m}\mathcal{O}_W$. To prove this, notice $\mathrm{Frob}_q - \mathrm{id}$ is surjective on $\mathcal{O}_W/\mathfrak{m}\mathcal{O}_W$, which follows from the fact $\mathcal{O}_W/\mathfrak{m}\mathcal{O}_W$ is trivial as proved above and $\mathrm{Frob}_q - \mathrm{id}$ is surjective on $\overline{k}$.

Now $v_{i,n}$ are Cauchy sequences and they converges to a tuple v_i that $G_{K^{ur}/K}$ acts trivially and it is an $\mathcal{O}$-basis of $\mathcal{O}_W$, as its reduction modulo $\mathfrak{m}$ is a basis of $\mathcal{O}_W/\mathfrak{m}\mathcal{O}_W$, so it is a $\widehat{K^{\mathrm{ur}}}$-basis of W. □

Prop. (18.4.1.2) [$\mathbb{C}_p$-Admissibility]. For $(\rho, V) \in \mathrm{Rep}^{\mathrm{fd}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$, the following are equivalent:

- V is $\mathbb{C}_p$-admissible.
- $\#\rho(I_K) < \infty$.
- V is $L\widehat{K^{\mathrm{ur}}}$-admissible for some finite extension L/K.

⌟

Proof: Cf.[p-adic Period Rings Intro, P18].?
2 → 3: This follows from(18.4.1.1). □

Cor. (18.4.1.3) [$H^0_{\mathrm{cont}}(\mathrm{Gal}_K, \mathbb{C}_p(\psi))$, Sen-Tate]. $H^0_{\mathrm{cont}}(\mathrm{Gal}_K, \mathbb{C}_p(\psi)) = \begin{cases} K & ,\#\psi(I_K) < \infty \\ 0 & ,\#\psi(I_K) = \infty \end{cases}$. In particular,

$$H^0_{\mathrm{cont}}(\mathrm{Gal}_K, \mathbb{C}_p(m)) = \begin{cases} K & ,m = 0 \\ 0 & ,m \neq 0 \end{cases}.$$

⌟

Proof: This follows from(18.1.1.19) and(18.4.1.2). For the last assertion, the cyclotomic extension of K thus also the cyclotomic character of G_K is infinitely unramified, thus χ^s_{cycl} factors through a finite quotient iff $s = 0$. And $H^0(\mathrm{Gal}_K, \mathbb{C}_p) = K$ by Ax-Sen-Tate(14.2.5.8). □

Cor. (18.4.1.4) [Potentially Unramified]. If $\eta : \mathrm{Gal}_K \to \mathbb{Z}_p^*$ is a character and there is $y \in \mathbb{C}_K^\times$ that $\eta(g) = g(y)/y$, then there exists a finite Abelian extension L of K that $\eta|_{G_L}$ is unramified, i.e. η is **potentially unramified**. ⌟

Cor. (18.4.1.5). For any $n, m \in \mathbb{Z}$,

$$\mathrm{Hom}_{\mathrm{Rep}_{\mathbb{C}_K}(\mathrm{Gal}_K)}(\mathbb{C}_K(n), \mathbb{C}_K(m))$$

is of one-dimensional over K if $n = m$, and vanishes otherwise. ⌟

Proof: Let $W = \mathrm{Hom}_{\mathbb{C}_p}(\mathbb{C}_K(n), \mathbb{C}_K(m)) = \mathbb{C}_K(m - n)$, then the desired space is W^{Gal_K}, and the assertion follows from(18.4.1.3). □

<u>H^1_{cont} **of** Gal_K**-Actions on** $\mathbb{C}_p(\psi)$</u>

Def. (18.4.1.6) [Notations]. Let $K \in p$-`NField`, K_∞ is an Abelian extension of K that the Galois group Γ has a subgroup Γ_0 of finite index that $\Gamma_0 \cong \mathbb{Z}_p$, and $H_K = \mathrm{Gal}_{K_\infty}$. The natural examples is $K_\infty = K(p^{\frac{1}{p^\infty}})$.

Let $\Gamma_m = \Gamma_0^m$ and K_m the fixed field of Γ_m.

Decompose $\Gamma = \Sigma \times \Gamma_0$ and let γ be a topological generator of Γ_0, then every element of Γ_0 can be written as γ^t for some $t \in \mathbb{Z}_p$. Denote $\gamma_s = \gamma^{p^s}$.

$\psi : G_K \to \Gamma \to \mathbb{Z}_p^*$ be a character factoring through Γ, then we can form a representation $\mathbb{C}_p(\psi)$ of G_K on $\mathbb{C}_p$ that $\rho(\sigma)(x) = \psi(\sigma)\sigma(x)$. This is an action because G_K acts trivial on $\mathbb{Z}_p^*$. ⌟

Lemma (18.4.1.7). Giving an $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$, if $x, y \in \mathfrak{m}_{\mathbb{C}_p}$ that $x \equiv y \mod \pi_K^n$, then $[\pi_K]^\sigma(x) \equiv [\pi_K]^\sigma(y) \mod \pi_K^{n+1}$, where f^σ is given by action of σ on the coefficients. ⌟

Proof: This is because the coefficients of $[\pi_K]^\sigma$ are divisible by π_K except for degree q, where it is $x^q - y^q = (x - y)(x^{q-1} + x^{q-2}y + \ldots + y^{q-1})$ which is divisible by π_K^{n+1} because the residue field of K is of order q. □

Prop. (18.4.1.8). If we let the action of $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$ on the residue field giving by $\overline{\sigma} : k_K \to \overline{\mathbb{F}}_p : x \mapsto x^{q_\sigma}$, where $q_\sigma = p^{n_\sigma}$ is a p-power, given an element $\eta = (\eta_0, \eta_1, \ldots) \in TG$, we have $\eta^{q_\sigma} \equiv [\pi_K]^\sigma(\eta^{q_\sigma}_{n+1}) \mod \pi_K$, hence the above lemma(18.4.1.7) shows that $[\pi_K^n]^\sigma \eta_n^{q_\sigma} \equiv$

$[\pi_K^{n+1}]^\sigma(\eta_{n+1}^{q_\sigma}) \mod \pi_K^{n+1}$, so $[\pi_K^n]^\sigma(\eta_n^{q_\sigma})$ is a Cauchy sequence, converging to an element μ_σ(don't care about η).

If $g \in G_K$, then $g(\eta_n) = [\chi_K(g)](\eta_n)$, hence take q_σ-th power, $g(\eta_n^\sigma) \equiv [\chi_K(g)]^\sigma(\eta_n^{q_\sigma}) \mod \pi_K$, then

$$[\chi_K(g)]^\sigma[\pi_K^n]^\sigma(\eta_n^{q_\sigma}) \equiv [\pi_K^n]^\sigma g(\eta_n^{q_\sigma}) = g([\pi_K^n]^\sigma \eta_n^{q_\sigma}) \mod \pi_K.$$

hence by limiting, $g(\mu_\sigma) = [\chi_K(g)]^\sigma(\mu_\sigma)$. ⌟

Lemma (18.4.1.9).

$$v_p(\mu_\sigma) = \begin{cases} \frac{q_\sigma}{e_K(q-1)} + \frac{1}{e_K} & n(\sigma) \neq 0 \\ \frac{1}{e_K(q-1)} + v_p(\sigma(\pi_K) - \pi_K) & n(\sigma) = 0 \end{cases}$$

⌟

Proof: By(9.5.3.28), we know the Newton polygon of $[\pi_K^n]^\sigma$. When $n(\sigma) \neq 0$, $v(\eta_1^{q_\sigma}) = \frac{q_\sigma}{e_K(q-1)} > \frac{1}{e_K(q-1)}$, so the valuation of $[\pi_K]^\sigma(\eta_1^{q_\sigma})$ equals the valuation of its degree 1 term, which is $v(\pi_K \eta_1^{q_\sigma}) = \frac{q_\sigma}{e_K(q-1)} + \frac{1}{e_K}$. Now we have by(18.4.1.8), we have $[\pi_K]^\sigma \eta^{q_\sigma} \equiv [\pi_K^2]^\sigma(\eta_2^{q_\sigma}) \mod \pi_K^2$, and $\frac{q_\sigma}{e_K(q-1)} + \frac{1}{e_K} < 2/e_K$, so valuation already stable at degree 1, and $v(\mu_\sigma) = v([\pi_K]^\sigma(\eta_1^{q_\sigma}))$.

If $q_\sigma = 1$, it's more delicate, because degree 1 and degree q term has the same minimal valuation, so they may jump to higher valuations. Notice $[\pi_K^n](\eta_n) = 0$, so $[\pi_K^n]^\sigma(\eta_n) = ([\pi_K^n]^\sigma - [\pi_K^n])(\eta_n)$. And we have by(14.2.2.21), for $x \in \mathcal{O}_K$, $v(\sigma(x) - x) \geq v(x) + v(\frac{\sigma(\pi_K)}{\pi_K} - 1) + \delta_{v(x),0} v(\pi_K)$, with equality when $v_p(x) = q/e_K$. So by the Newton polygon, the minimum valuation of the coefficient of $[\pi_K^n]^\sigma - [\pi_K^n]$ appear at degree p^{n-1} and possibly p^n. The valuation of η_n is too small($\frac{1}{e_K p^{n-1}(p-1)}$) that we don't need to consider other degrees but can assure that degree p^{n-1} is of minimum valuation, which is $v(\eta_n^{p^{n-1}}) + v(\sigma(\pi_L) - \pi_L) = \frac{1}{e_K(q-1)} + v_p(\sigma(\pi_K) - \pi_K)$. □

Prop. (18.4.1.10). For any $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)\backslash\{\mathrm{id}\}$, there is an element $\alpha_\sigma \in \mathbb{C}_p^*$ that $\sigma \circ \chi_K(g) = g(\alpha_\sigma)/\alpha_\sigma$ for all $g \in \mathrm{Gal}_K$, where χ_K is the Lubin-Tate character. ⌟

Proof: We let $\alpha_\sigma = \log_{\mathcal{F}_\pi}^\sigma(\mu_\sigma)$, by(18.4.1.9), $1/e_K < \mu_\sigma < \infty$, so by the Newton polygon analysis of $\log_{F_\pi}$(9.5.3.29), α_σ has the same valuation of μ_σ, in particular, $\alpha_\sigma \neq 0$. Then

$$g(\alpha_\sigma) = \log_{\mathcal{F}_\pi}^\sigma(g(\mu_\sigma)) = (\log_{\mathcal{F}} \circ [\chi_K(g)])^\sigma(\mu_\sigma) = (\chi_K(g) \cdot \log_{\mathcal{F}_\pi})^\sigma(\mu_\sigma) = \sigma(\chi_K(g)) \cdot \alpha_\sigma.$$

□

Cor. (18.4.1.11). $\log_p(\sigma(\chi_K(g))) = g(\log(\alpha_\sigma)) - \log_p(\alpha_\sigma)$. ⌟

Prop. (18.4.1.12) [$H^1_{\mathrm{cont}}(\mathrm{Gal}_K, \mathbb{C}_p(\psi))$, Sen-Tate]. There is an inf-res exact sequence

$$0 \to H^1_{\mathrm{cont}}(\Gamma_K, \widehat{K}_\infty(\psi)) \to H^1_{\mathrm{cont}}(\mathrm{Gal}_K, \mathbb{C}_p(\psi)) \to H^1_{\mathrm{cont}}(H_K, \mathbb{C}_p(\psi)),$$

and

$$H^1_{\mathrm{cont}}(H_K, \mathbb{C}_p(\psi)) = 0, \quad H^1_{\mathrm{cont}}(\mathrm{Gal}_K, \mathbb{C}_p(\psi)) = \begin{cases} 0 & , \#\psi(I_K) = \infty \\ \text{a } K\text{-vector space of dimension } 1 & , \#\psi(I_K) < \infty \end{cases}.$$

⌟

Proof: For the first assertion, ψ is trivial on H_K, so $\mathbb{C}_p(\psi)\cong\mathbb{C}_p$ as H_K-representation, so it suffice to show for $\psi=\mathrm{id}$. Let f be a cocycle, as H_K is compact, $f(H_K)\in p^{-k}\mathcal{O}_{\mathbb{C}_p}$ for some integer k. So the lemma below(18.4.1.13) shows that we can move f cohomologouly to higher valuation, i.e. $f(g)=\sum x_i-g(\sum x_i)$, so f is a coboundary.

For the second assertion, we assume $\Gamma_K\neq\mathbb{Z}_p^*$, for this case, see remark(18.4.1.14) below.

let γ be a topological generator of $\Gamma_K=1+p^k\mathbb{Z}_2^*$, $k\geq 0$, because $\mathbb{Z}_p^*$ are all topological cyclic groups except for $\mathbb{Z}_2^*\cong\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}_2$, and γ_n be a topological generator of Γ_{F_n} which is also a power of γ. By(8.7.4.4) we know $H^1(\Gamma_K,\widehat{K_\infty}(\psi))=\widehat{K_\infty}(\psi)/1-\gamma$.

For n large, we have a decomposition $\widehat{K_\infty}(\psi)=K_n(\psi)\oplus X_n(\psi)$ by(14.2.3.33), and $1-\gamma_n$ is invertible on $X_n(\psi)$. Now $1-\gamma_n=(1-\gamma)(1+\gamma+\ldots+\gamma^{k-1})$, so $1-\gamma$ is also invertible in $X_n(\psi)$. And on $K_n(\psi)$, if ψ is of infinite order, then $1-\gamma$ is injective, otherwise $x=\psi(\gamma)^N\gamma^N(x)=\psi(\gamma)^Nx$. So it is also surjective because it is a K-linear mapping of K_n. So $\widehat{K_\infty}(\psi)/1-\gamma=0$. If ψ is of finite order then $K_n(\psi)\cong K_n$ as Γ_K-module when n is large enough that γ factors through Γ_{K_n}, by(8.7.3.1). So $K_n/1-\gamma=K_n/\ker(\mathrm{tr}_{K_n/K})=K$. □

Lemma (18.4.1.13). If $f:H_K\to p^n\mathcal{O}_{\mathbb{C}_p}$ is a continuous cocycle, then there exists a $x\in p^{n-1}\mathcal{O}_{\mathbb{C}_p}$ that the cohomologous cocycle $g\mapsto f(g)-(x-g(x))$ has values in $p^{n+1}\mathcal{O}_{\mathbb{C}_p}$. ⌟

Proof: $p^{n+2}\mathcal{O}_{\mathbb{C}_p}$ is open in $p^n\mathcal{O}_{\mathbb{C}_p}$, so there is a finite extension L/K that $f(H_L)\in p^{n+2}\mathcal{O}_{\mathbb{C}_p}$. By(14.2.3.27), there is a z that $\mathrm{tr}_{L_\infty/K_\infty}(z)=p$, so there is a $y\in p^{-1}\mathcal{O}_{L_\infty}$ that $\mathrm{tr}_{L_\infty/K_\infty}(y)=1$.

Now for a set of representatives Q of H_K/H_L, denote $x_Q=\sum_{h\in Q}h(y)f(h)$, then for $g\in H_K$, $g(Q)$ is also a set of representative, and $g(x_Q)=\sum_{h\in Q}gh(y)gf(h)=\sum_{h\in Q}gh(y)(f(gh)-f(g))=x_{g(Q)}-f(g)$, as $\mathrm{tr}(y)=1$. So $f(g)-(x_Q-g(x_Q))=x_{g(Q)}-x_Q$. The RHS is in $p^{n+1}\mathcal{O}_{\mathbb{C}_p}$, because: if we let $gh_i=h_{g(i)}a_i$, where $a_i\in H_L$, then $x_{g(Q)}-x_Q=\sum h_{g(i)}(y)f(h_{g(i)}a_i)-\sum h_{g(i)}(y)f(h_{g(i)})=\sum h_{g(i)}(y)h_{g(i)}(f(a_i))$, which is in p^{n+1} because $h_{g(i)}(y)\in p^{-1}\mathcal{O}_{\mathbb{C}_p}$ and $f(a_i)\in p^{n+2}\mathcal{O}_{\mathbb{C}_p}$ by the choice of L. □

Remark (18.4.1.14). In case $\Gamma_K=\mathbb{Z}_2^*$,

$$0\to H^1_{\mathrm{cont}}(\{\pm1\},K(\psi))\to H^1_{\mathrm{cont}}(\mathbb{Z}_2^*,\widehat{K_\infty}(\psi))\to H^1_{\mathrm{cont}}(1+2\mathbb{Z}_2^*,\mathbb{C}_p(\psi))$$

$H^1(\{\pm1\},K(\psi))=0$ whether $\psi(-1)=1$ or -1. And by the same proof as above, possibly replace X_n with X_{n+1}, to remedy the singularity of $p=2$, $H^1(1+2\mathbb{Z}_2^*,\mathbb{C}_p(\psi))=K$, with generator $[g\mapsto\frac{\chi(g)-1}{\gamma-1}(a)]$ for some a. This cocycle extends to a cocycle of $\mathbb{Z}_2^*$, so the map is surjective. ⌟

Prop. (18.4.1.15). The 1-dimensional K-vector space $H^1_{\mathrm{cont}}(\mathrm{Gal}_K,\mathbb{C}_p)$ is generated by the cocycle $[g\mapsto\log_p\chi(g)]$. ⌟

Proof: By the proof of(18.4.1.12), we know that $H^1(\Gamma_K,K_n)\xrightarrow{f}H^1(G_K,\mathbb{C}_p)$ is an isomorphism. for $\alpha\in K$, if $\chi(g)=\gamma^k$, then $f(\alpha)(g)=(1+\gamma+\ldots+\gamma^{k-1})(\alpha)=k\alpha=\alpha\cdot\log_p(\chi(g))/\log_p(\gamma)$. So by continuity, f is a multiple of $[g\mapsto\log_p(\chi(g))]$. □

Lemma (18.4.1.16). And $f\in\mathrm{Hom}(I_K^{\mathrm{ab}},\mathbb{Q}_p)$ is of the form $f(g)=\mathrm{tr}_{K/\mathbb{Q}_p}(\beta_f\log_p\chi_K(g))$ for some $\beta_f\in K$. ⌟

Proof: By(14.6.2.25), χ_K is a canonical isomorphism $I_K^{ab}\cong\mathcal{O}_K^*$. Any $f\in\mathrm{Hom}(\mathcal{O}_K^*,\mathbb{Q}_p)$ is of the form $f(y)=\mathrm{tr}_{K/\mathbb{Q}_p}(\beta_f\log_p(y))$ for some $\beta_f\in K$, because: by(14.2.3.9), when n is large, $\log_p$ is a bijection between U_K^n and $\pi_K^n\mathcal{O}_K$.

$\pi_K^n\mathcal{O}_K\to\mathbb{Q}_p$ can be extended to a map $K\to\mathbb{Q}_p$ as $\mathbb{Q}_p$ is divisible. Now trace is a invertible bilinear form on K, so the assertion is true on U_K^n for some n, and because U_K^n is of finite index in $\mathcal{O}_K^*$ and $\mathbb{Q}_p$ is of char 0, this is true for all $\mathcal{O}_K^*$. □

Prop. (18.4.1.17). The map $H^1(\mathrm{Gal}_K, \mathbb{Q}_p) \to H^1(\mathrm{Gal}_K, \mathbb{C}_p)$ is given as follows: as $f \in H^1(\mathrm{Gal}_K, \mathbb{Q}_p)$ must factor through $\mathrm{Gal}_K^{\mathrm{ab}}$, if the restriction of f to I_K^{ab} corresponds to β_f, then f maps to $\beta_f[g \mapsto \log_p \chi(g)]$. ⌟

Proof: $f(g) = \mathrm{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p \chi_K(g))$ on I_K, but this map extends to map on G_K. So $f(g) = \mathrm{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p \chi_K(g)) + c(g)$ for a unramified map c on G_K.

Now by(8.7.4.3), $H^1(G, \widehat{\mathbb{Q}}_p^{ur}/\mathbb{Q}_p)$ vanish because $H^1(G, \overline{\mathbb{F}}_p)$ vanish(8.7.3.1), so there is a $z \in \widehat{\mathbb{Q}}_p^{ur}$ that $c(g) = g(z) - z$. And

$$\mathrm{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p \chi_K(g)) = \sum_\sigma \sigma(\beta_f \log_p \chi_K(g)) = \beta_f \,\mathrm{tr}_{K/\mathbb{Q}_p}(\log_p \chi_K(g)) + \sum_\sigma (\sigma(\beta_f) - \beta_f)\sigma(\log_p \chi_K(g)).$$

Notice(18.4.1.10) gives a β_σ that $\sigma(\log_p \chi_K(g)) = g(\beta_\sigma) - \beta_\sigma$, and $\mathrm{tr}_{K/\mathbb{Q}_p}(\log_p \chi_K(g)) = \log_p \chi(g)$ because $(N_{K/\mathbb{Q}_p}\chi_K(g))^{-1} = (\chi(g))^{-1}$, as they both correspond via local CFT to the element in G_K^{ab} which acts by g on L_π and id on K^{ur}. Thus the result. □

2 Hodge-Tate Representations

References are [Sen80] and [Car19].

Hodge-Tate Representations

Def. (18.4.2.1) **[$B_{\text{H-T}}$].** Let $B_{\text{H-T}} = \mathbb{C}_K[t, t^{-1}], B'_{\text{H-T}} = \mathbb{C}_K((t))$, and let G_K acts on it by $g(at^i) = g(a)\chi_{\mathrm{cycl}}(g)^i t^i$. In addition, there is a filtration on $B'_{\text{H-T}}$ given by $\mathrm{Fil}^m B'_{\text{H-T}} = t^m \mathbb{C}_p[[t]]$, then the graded ring of $B'_{\text{H-T}}$ is isomorphic to $B_{\text{H-T}}$. (18.4.1.3) shows that $B_{\text{H-T}}^{\mathrm{Gal}_K} = (B'_{\text{H-T}})^{\mathrm{Gal}_K} = K$.

$B_{\text{H-T}}$ and $B'_{\text{H-T}}$ are Gal_K-regular(18.1.1.17). ⌟

Proof: $B'_{\text{H-T}}$ is Gal_K-regular because it is a field. For $B_{\text{H-T}}$, $B_{\text{H-T}} \subset \mathrm{Frac}(B_{\text{H-T}}) \subset B'_{\text{H-T}}$, taking Gal_K-fixed points shows (H2). For (H3), if $\mathbb{Q}_p x$ is stable under Gal_K and x is not of the form at^i, then we can get a non-trivial Gal_K-fixed point of $\mathbb{C}_K(j-i)$, which is impossible by(18.4.1.3). □

Cor. (18.4.2.2) **[Hodge-Tate Representations].** Let $W \in \mathrm{Rep}_{\mathbb{C}_K}(\mathrm{Gal}_K)$. For $k \in \mathbb{Z}$, let

$$W\{k\} = \{x \in W | g(x) = \chi_{\mathrm{cycl}}^k(g)x\} \subset W(-k)$$

then

$$\bigoplus_{k\in\mathbb{Z}} (\mathbb{C}_K(k) \otimes_K W\{k\}) \to W$$

is injective. W is called a **Hodge-Tate representation** if this is an isomorphism. ⌟

Proof: Notice $B_{\text{H-T}} \cong \bigoplus_{m\in\mathbb{Z}} \mathbb{C}_K(m) \in \mathrm{Rep}_{\mathbb{C}_K}(\mathrm{Gal}_K)$, so

$$B_{\text{H-T}} \otimes_K (B_{\text{H-T}} \otimes_{\mathbb{C}_K} W)^{\mathrm{Gal}_K} \cong B_{\text{H-T}} \otimes_K \bigoplus_{m\in\mathbb{Z}} (\mathbb{C}_K(m) \otimes_K W\{m\}) \hookrightarrow B_{\text{H-T}} \otimes_{\mathbb{C}_K} W.$$

is injective by(18.1.1.18). □

Cor. (18.4.2.3) **[Hodge-Tate Representations].** Let K be a p-adic field, then $V \in \mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{fd}}(\mathrm{Gal}_K)$ is called a **Hodge-Tate representation** if it is $B_{\text{H-T}}$-admissible. The category of Hodge-Tate representations are denoted by $\mathrm{Rep}_{\mathbb{Q}_p}^{\text{H-T}}(\mathrm{Gal}_K)$.

Then $V\in\mathrm{Rep}^{\mathrm{fd}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$ is Hodge-Tate iff it is $B'_{\text{H-T}}$-admissible iff $\mathbb{C}_K\otimes_{\mathbb{Q}_p}V$ is Hodge-Tate thus decomposes as

$$\mathbb{C}_K\otimes_{\mathbb{Q}_p}V\cong\mathbb{C}_K(n_1)\oplus\ldots\oplus\mathbb{C}_K(n_d)\in\mathrm{Rep}_{\mathbb{C}_K}(\mathrm{Gal}_K).$$

⌟

Proof: If $\mathbb{C}_K\otimes_{\mathbb{Q}_p}V$ is Hodge-Tate, then clearly $\dim_K(B_{\text{H-T}}\otimes_{\mathbb{Q}_p}V)^{\mathrm{Gal}_K}=\dim_{\mathbb{Q}_p}V$, thus V is $B_{\text{H-T}}$-admissible(18.1.1.19). Conversely, $\dim_K(B_{\text{H-T}}\otimes_{\mathbb{Q}_p}V)^{\mathrm{Gal}_K}=\dim_{\mathbb{Q}_p}V=d$ implies V is Hodge-Tate by(18.4.2.2). The equivalence with $B'_{\text{H-T}}$-admissibility is similar. □

Def. (18.4.2.4)[Hodge-Tate Weights]. For $V\in\mathrm{Rep}^{\text{H-T}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$, V is said to have Hodge-Tate weights i with multiplicity d_i if $\dim_K W\{i\}=d_i$.

In particular, $\mathbb{Q}_p(n)$ has a single Hodge-Tate weight n. ⌟

Prop. (18.4.2.5). If $K'\in\mathtt{Field}$, $K'\subset\overline{K}$, then for $W\in\mathrm{Rep}^{\mathrm{fd}}_{\mathbb{C}_K}(\mathrm{Gal}_K)$, the natural maps

$$K'\otimes_K D_K(W)\to D_{K'}(W),\quad \widehat{K^{\mathrm{ur}}}\otimes_K D_K(W)\to D_{\widehat{K^{\mathrm{ur}}}}(W)$$

are isomorphisms. In particular,

$$\mathrm{Rep}^{\mathrm{fd}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)\cap\mathrm{Rep}^{\text{H-T}}_{\mathbb{Q}_p}(\mathrm{Gal}_{K'})=\mathrm{Rep}^{\mathrm{fd}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)\cap\mathrm{Rep}^{\text{H-T}}_{\mathbb{Q}_p}(I_K)=\mathrm{Rep}^{\text{H-T}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$$

⌟

Proof: For $K'\subset\overline{K}$, $D_K(W)=D_{K'}(W)^{\mathrm{Gal}(K'/K)}$, thus the isomorphism follows from Galois descent(18.1.1.14). For $\widehat{K^{\mathrm{ur}}}$, Cf.[Conrad, P20]**?** □

3 Sen-Tate Theory

Colmez-Sen-Tate Conditions

Sen's Theory

Remark (18.4.3.1). Sen's theory goes further than $\mathrm{Rep}^{\text{H-T}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$ and to study $\mathrm{Rep}^{\mathrm{fd}}_{\mathbb{C}_K}(\mathrm{Gal}_K)$. ⌟

Prop. (18.4.3.2)[Hilbert's Theorem90 for Gal_{K_∞}]. Any $W\in\mathrm{Rep}^{\mathrm{fd}}_{\mathbb{C}_p}(\mathrm{Gal}_K)$ is trivial as a $\mathbb{C}_p$-semi-linear representation of Gal_{K_∞}. In particular, there is an isomorphism

$$\mathbb{C}_K\otimes_{\widehat{K_\infty}}W^{\mathrm{Gal}_{K_\infty}}\cong W\in\mathrm{Rep}_{\mathbb{C}_K}(\mathrm{Gal}_{K_\infty}).$$

⌟

Proof: The proof is similar to that of(18.4.1.1).

Let $\mathcal{O}_W$ be any $\mathcal{O}_{\mathbb{C}_p}$-lattice in W. Firstly we construct a $\mathbb{C}_p$-basis $w_1,\ldots,w_d$ of W that $w_i\in\mathcal{O}_W$ and $gw_i\equiv w_i \mod p^2\mathcal{O}_W$ for all $g\in\mathrm{Gal}_{K_\infty}$ and $p\mathcal{O}_W\subset\mathcal{O}_{\mathbb{C}_p}w_1\oplus\ldots\oplus\mathcal{O}_{\mathbb{C}_p}w_d$.

By continuity there is a finite Galois extension L/K that **?** Cf.[p-adic Hodge Intro, P23]. □

Prop. (18.4.3.3). By(18.4.3.2), the next step of Sen's theory is to study $W\in\mathrm{Rep}_{\widehat{K_\infty}}(\Gamma_K)$. To this attempt, Sen considers the subspace of Γ_K-finite vectors in W, they form a vector space $W_0\subset W$ over K_∞. Then there exists an integer r and a basis $(v_1,\ldots,v_d)$ of W that the K_r-span of v_i are stable under Γ_K-actions.

Obviously, these v_i are G_K-finite, thus in particular

$$\widehat{K_\infty}\otimes_{K_\infty}W_0\cong W.$$

⌟

Proof: Cf.[p-adic Hodge Intro, P25].**?** □

Cor. (18.4.3.4) [Sen's Operator]. Combining the previous two propositions, let $W \in \mathrm{Rep}^{\mathrm{fd}}_{\mathbb{C}_p}(\mathrm{Gal}_K)$, denote $\widehat{W}_\infty = W^{G_{\overline{K}/K_\infty}}$ and W_∞ the set of Γ_K-finite vectors of $\widehat{W}_\infty$, then

$$\mathbb{C}_p \otimes_{K_\infty} W_\infty \cong W.$$

Let $v_1, \ldots, v_d$ be given by(18.4.3.3), $W_r = \oplus K_r v_i$. For $g \in G_K$, let $\rho_W(g)$ be the endomorphism of W_r given by action of g, then $\rho_W(\gamma_s)$ is linear when $s \geq r$, and because γ_s converges to id, $\log \rho_W(\gamma_s)$ is defined for s large. Then **Sen's operator** Φ_W is defined to be $\Phi_W = \frac{\log \rho(\gamma_s)}{p^s}$, or equivalently $\Phi_W(v) = \lim_{t\to 0} \frac{\gamma^t(v)-v}{t}$.

Sen's operator is defined over K, as it commutes with Γ_K seen from the limit form, and its kernel is the $\mathbb{C}_p$-subspace of W generated by elements invariant under Γ_K. ⌟

Proof: It is evident that fixed points of Γ_K are killed by Φ_W. Conversely, the kernel of Φ_W on W_∞ is stable under action of G_K, thus is a sub-representation of Γ_K in W_∞, and because W_∞ consists of finite vectors, the G_K-action is continuous w.r.t the discrete topology, and Hilbert's theorem90(8.7.3.16) shows this subspace is generated by elements invariant under G_K. □

Prop. (18.4.3.5) [Sen's Category]. Let $\mathrm{Sen}(K, K_\infty)$ be the category of f.d. K_∞-vector spaces equipped with an endomorphism defined over K, then the construction sending W to (W_∞, Φ_W) induces a functor

$$\mathrm{Sen} : \mathrm{Rep}^{\mathrm{fd}}_{\mathbb{C}_p}(\mathrm{Gal}_K) \to \mathrm{Sen}(K, K_\infty).$$

This functor commutes with direct sums, and also under tensor products, with the Sen's operator given by

$$\Phi_{W\otimes W'} = \Phi_W \otimes \mathrm{id}_{W'} + \mathrm{id}_W \otimes \Phi_{W'}.$$

This functor is faithful, but in general not full. However, it reflects isomorphisms. ⌟

Proof: This functor is faithful because W_∞ generates W as a $\mathbb{C}_p$-vector space. To show it reflects isomorphism, Let $f : W_\infty \to W'_\infty$ be an isomorphism commuting with Sen's operator, then it extends by linearity to an isomorphism of $\mathbb{C}_p$-vector spaces $W \to W'$, and f is Γ_s-equivariant for some s by the definition of Sen's operator. Then considering the space of Γ_s-equivariant $\mathbb{C}_p$-linear morphisms from W to W', Hilbert's theorem90 shows there is a basis f_i consisting of G_K-equivariant morphisms. Then it remains to show there exists a linear K-combination of f_i that is invertible. This is possible because it is true for K_s, as f is invertible, and K is an infinite field. □

Cor. (18.4.3.6). $W \in \mathrm{Rep}^{f}_{\mathbb{C}_p}(\mathrm{Gal}_K)$ is trivial iff $\Phi_W = 0$. ⌟

Proof: As $\mathcal{S}$ reflects isomorphisms, compare with the trivial representation $\mathbb{C}_p^d$. □

Prop. (18.4.3.7) [Hodge-Tate Representations and Sen's Operators]. A representation $V \in \mathrm{Rep}^{\mathrm{fd}}_{\mathbb{Q}_p}(G_K)$ is Hodge-Tate iff the Sen's operator $\Phi_{\mathbb{C}_p\otimes_{\mathbb{Q}_p}V}$ is semisimple with eigenvalues in $\mathbb{Z}$. For a general V, the eigenvalues of $\Phi_{\mathbb{C}_p\otimes_{\mathbb{Q}_p}V}$ is called the **generalized Hodge-Tate weights** of V. ⌟

Proof: If V is a Hodge-Tate representation, then clearly $\Phi_W(v) = \lim_{t\to 0} \frac{\gamma^t(v)-v}{t}$ acts by k on $\mathbb{C}_p(k)$, thus it is semisimple with eigenvalues in $\mathbb{Z}$. Conversely, on the i-eigenspace of Φ, tensoring χ_{cycl}^{-i}, Φ acts trivially, then because the kernel of Φ are the fixed points of Γ_K(18.4.3.4), thus this eigenspace is isomorphic to $\mathbb{C}_p(i)^d$, so V is Hodge-Tate. □

4 Fontaine's Rings

Notation (18.4.4.1). In this subsection, we denote $B_{\mathrm{dR}}, B_{\mathrm{crys}}$ etc. to denote Fontaine's ring w.r.t. the perfectoid field $\mathbb{C}_K$ defined in Fontaine's Period Rings. ⌟

Lemma (18.4.4.2). Let $\varepsilon = (\ldots, \varepsilon_1, \varepsilon_0) \in \mathcal{O}^\flat_{\mathbb{C}_K}$ s.t. $\varepsilon_0 = 1$ and $\varepsilon_1 \neq 1$, then $|\varepsilon - 1| = \frac{p}{p-1}$. ⌟

Proof:

$$|\varepsilon - 1| = |(\varepsilon-1)^\sharp|_{\mathbb{C}_K} = |\lim_{n\to\infty}(\varepsilon_n - 1)^{p^n}|_{\mathbb{C}_K} = \lim_{n\to\infty} p^n|\varepsilon_n - 1| = \lim_{n\to\infty}\frac{p^n}{p^{n-1}(p-1)} = \frac{p}{p-1}$$

□

Prop. (18.4.4.3) [$\mathbb{Q}_p$-Line in B_{dR}]. $\theta([\varepsilon]-1) = \varepsilon_0 - 1 = 0$, so $[\varepsilon]-1 \in \ker\theta$, and we can define

$$t_\varepsilon = \log([\varepsilon]) = \sum_{n\geq 1}(-1)^{n-1}\frac{([\varepsilon]-1)^n}{n} \in B^+_{\mathrm{dR}}.$$

Then this is a uniformizer in the CDVR B^+_{dR}. Moreover, any other choice of ε is of the form $\varepsilon' = \varepsilon^a$ for $a \in \mathbb{Z}_p$, then $t_{\varepsilon'} = at_\varepsilon$, and $\gamma(t_\varepsilon) = \chi_{\mathrm{cycl}}(\gamma)t$ for any $\gamma \in \mathrm{Gal}_K$. ⌟

Proof: t_ε is a uniformizer because $[\varepsilon]-1$ is: $[\varepsilon^{1/p}]-1$ is a unit in B_{dR}, and

$$\eta = \frac{[\varepsilon]-1}{[\varepsilon^{1/p}]-1} = 1 + [\varepsilon^{1/p}] + \ldots + [\varepsilon^{(p-1)/p}]$$

is distinguished, because if $\eta = \sum [c_n]p^n$, consider reducing to the residue field: $W(\mathcal{O}_{\mathbb{C}^\flat_K}) \to W(\mathcal{O}_{\mathbb{C}^\flat_K}/t)$, then $\overline{\varepsilon} = 1$ by(18.4.4.2), and $\overline{\eta} = p$, thus $|c_0| < 1, |c_1 - 1| < 1$, so it is distinguished(5.5.4.20), thus a uniformizer by(17.11.1.2).

For the last assertion, by the formal property of log, it suffices to show that if $a_i \to a \in \mathbb{Z}_p$, then $[\varepsilon^{a_i}] \to [\varepsilon^a] \in B_{\mathrm{dR}}$. Then it suffices to show that for $a \in \mathbb{Z}_p, |a|$ small,

$$|[\varepsilon^a] - 1| \to 0.$$

And this can be done with the topology given in(17.11.1.20)**?** □

Cor. (18.4.4.4). $\mathrm{gr}(B_{\mathrm{dR}}) \cong B_{\text{H-T}}$. ⌟

Cor. (18.4.4.5). B_{dR} is Gal_K-regular, but B^+_{dR} is not Gal_K-regular. ⌟

Proof: B_{dR} is Gal_K-regular because it is a field. B^+_{dR} is not Gal_K-regular because $\mathbb{Q}_p t_\varepsilon$ is stable under Gal_K-action but t_ε is not invertible in B^+_{dR}. □

Prop. (18.4.4.6) [Galois Actions]. Gal_K acts on $\mathcal{O}_{\mathbb{C}_K}/(p)$ thus acts on $\mathcal{O}_{\mathbb{C}^\flat_K}$ and on A_{inf}. Then Fontaine's functor $\theta : A_{\mathrm{inf}} \to \mathcal{O}_{\mathbb{C}_K}$ is Gal_K-equivariant, thus $\ker\theta$ is Gal_K-stable, so Gal_K-acts on B^+_{dR} and B_{dR}, and $B_{\mathrm{dR}} \to \mathbb{C}_K$ is Gal_K-equivariant. ⌟

Prop. (18.4.4.7). There is a canonical lifting of $\overline{K} \to \mathbb{C}_K$ along $B^+_{\mathrm{dR}} \to \mathbb{C}_K$, and it is Gal_K-equivariant.

However, this embedding is not continuous, thus there is no embedding $\mathbb{C}_K \subset B^+_{\mathrm{dR}}$. ⌟

Proof: $K_0 = W(k)[\frac{1}{p}] \subset W(\mathcal{O}^\flat_{\mathbb{C}_K})[\frac{1}{p}] = B_{\mathrm{inf}} \subset B_{\mathrm{dR}}$, and it follows from Hensel's lemma that any element in $\overline{K}$ lifts uniquely to an element of B^+_{dR}, so $\overline{K} \subset B^+_{\mathrm{dR}}$, and is Gal_K-invariant, by uniqueness and the fact $B_{\mathrm{dR}} \to \mathbb{C}_K$ is Gal_K-equivariant(18.4.4.6).

For the last assertion, if the embedding is continuous, the $B^+_{\mathrm{dR}} \to \mathbb{C}_K$ has a section, and the filtration splits so $B_{\mathrm{dR}} \cong B_{\text{H-T}}$. □

Prop. (18.4.4.8).

- $K = (B^+_{\mathrm{dR}})^{\mathrm{Gal}_K} = B^{\mathrm{Gal}_K}_{\mathrm{dR}}$
- $K_0 = B^{\mathrm{Gal}_K}_{\mathrm{crys}}$, and the canonical morphism $K \otimes_{K_0} B_{\mathrm{crys}} \to B_{\mathrm{dR}}$ is injective.
- $\mathbb{Q}_p = B^{\mathrm{Gal}_K}_e$.
- $\mathbb{Q}_p = (\mathrm{Fil}^0 B_\mu)^{\mathrm{Gal}_K}$ for $\mu = \mathrm{crys}$ or $\mu \geq 1$.

⌟

Proof: 1: Firstly $K \subset B_{\mathrm{dR}}$ and is invariant under Gal_K by(18.4.4.7). On the other hand, the exact sequence

$$0 \to \mathrm{Fil}^{m+1} B_{\mathrm{dR}} \to \mathrm{Fil}^m B_{\mathrm{dR}} \to \mathbb{C}_p(m) \to 0(18.4.4.13).$$

induces an injection

$$B^{\mathrm{Gal}_K}_{\mathrm{dR}} \cap \mathrm{Fil}^m B_{\mathrm{dR}} / B^{\mathrm{Gal}_K}_{\mathrm{dR}} \cap \mathrm{Fil}^{m+1} B_{\mathrm{dR}} \hookrightarrow \mathbb{C}_p(m)^{\mathrm{Gal}_K}.$$

Thus $B^{\mathrm{Gal}_K}_{\mathrm{dR}} = B^{\mathrm{Gal}_K}_{\mathrm{dR}} = K$.

2: The injectivity of $K \otimes_{K_0} B_{\mathrm{crys}} \to B_{\mathrm{dR}}$ Cf.[Laurent Fargues and Jean-Marc Fontaine Prop10.2.8].

3: From 2 and notice $B_e = B^{\varphi=\mathrm{id}}_{\mathrm{crys}}$.

4: Cf.[Period Rings, P45].**?** □

Lemma (18.4.4.9). Let $W \in \mathcal{V}\mathrm{ect}^{\mathrm{fd}}_K$, then the map:

$$\{\text{Filtrations on } W\} \to \{\mathrm{Gal}_K\text{-stable } B^+_{\mathrm{dR}}\text{-lattice in } W \otimes_K B_{\mathrm{dR}}\} : \mathrm{Fil} \mapsto \mathrm{Fil}^0(W \otimes_K B_{\mathrm{dR}})$$

is bijective and the inverse is given by $\Gamma \mapsto \{(t^n\Gamma)^{\mathrm{Gal}_K} \subset (B_{\mathrm{dR}} \otimes_{B^+_{\mathrm{dR}}} \Gamma)^{\mathrm{Gal}_K} = W\}_{n\in\mathbb{Z}}$. ⌟

Proof: Cf.[Laurent Fargues and Jean-Marc Fontaine Prop10.4.3].**?** □

deRham and Crystalline Representations

Def. (18.4.4.10) [deRham, Crystalline and Semistable Representations]. Situation as in(18.4.4.8), for $V \in \mathrm{Rep}^{\mathrm{fd}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$,

- V is called a **deRham representation** iff V is B_{dR}-admissible**??**, or equivalently

  $$\dim_K (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{\mathrm{Gal}_K} = \dim_{\mathbb{Q}_p} V.$$

  The category of deRham representations of Gal_K are denoted by $\mathrm{Rep}^{\mathrm{dR}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$.

- V is called a **crystalline representations** iff V is B_{crys}-admissible, or equivalently

  $$\dim_{K_0} (B_{\mathrm{crys}} \otimes_{\mathbb{Q}_p} V)^{\mathrm{Gal}_K} = \dim_{\mathbb{Q}_p} V.$$

  The category of crystalline representations of Gal_K are denoted by $\mathrm{Rep}^{\mathrm{crys}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$.

⌟

Def. (18.4.4.11)[$\mathrm{Rep}'_{B_e}(\mathrm{Gal}_K)$]. Denote by $\mathrm{Rep}'_{B_e}(\mathrm{Gal}_K)$ the category of finite locally free B_e-modules M with a semi-linear Gal_K-action that there exists a Gal_K-invariant B^+_{dR}-lattice $\Gamma \in M \otimes_{B_e} B_{\mathrm{dR}}$ that G_K acts continuously. ⌟

Summary

Prop. (18.4.4.12) [Diagram of Inclusions].

$$\begin{array}{ccccccccccc} B^+_{\mathrm{inf}} & \longrightarrow & B^+_{\mu} & \hookrightarrow & B^+_{\mathrm{crys}} & \hookrightarrow & B^+_{\mu} & \hookrightarrow & B^+_{\max} & \hookrightarrow & B^+_{\mathrm{dR}} \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ & & \underset{(\mu>p-1)}{B_{\mu}} & \hookrightarrow & B_{\mathrm{crys}} & \hookrightarrow & \underset{(1\leq\mu\leq p-1)}{B_{\mu}} & \hookrightarrow & \underset{=B_1^+}{B_{\max}} & \hookrightarrow & B_{\mathrm{dR}} \end{array}$$

⌟

Prop. (18.4.4.13) [Properties of B_{dR}].

- B_{dR} is a discretely valued field with residue field $\mathbb{C}_K$ and valuation ring B^+_{dR}.
- B_{dR} is an algebra over $\overline{\widehat{K^{\mathrm{ur}}}} = \overline{K}\widehat{K^{\mathrm{ur}}}$ but not over $\mathbb{C}_K$.
- B_{dR} has a special uniformizer t_ε s.t. $\mathbb{Q}_p t_\varepsilon \cong \mathbb{Q}_p(1) \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$.
- B_{dR} has a filtration $\{\mathrm{Fil}^m B_{\mathrm{dR}} = t_\varepsilon^m B^+_{\mathrm{dR}}\}$, and $B^{\mathrm{gr}}_{\mathrm{dR}} \cong B_{\text{H-T}}$ as graded rings.
- $B_{\mathrm{dR}}^{\mathrm{Gal}_K} = K$.

⌟

Proof: 1 follows from(17.11.1.18), 2 follows from(18.4.4.7). 3 follows from(18.4.4.3). 4 follows from(18.4.4.4). 5 follows from(18.4.4.8). □

Prop. (18.4.4.14) [Properties of B_{crys}].

- B_{crys} is an algebra over $\widehat{K^{\mathrm{ur}}}$.
- B_{crys} has a Frobenius endomorphism φ.
- There is a canonical embedding $B_{\mathrm{crys}} \otimes_{K_0} K \hookrightarrow B_{\mathrm{dR}}$, and $t_\varepsilon \in B_{\mathrm{crys}}$.
- $B_{\mathrm{crys}}^{\mathrm{Gal}_K} = K_0$.
- $(B_{\mathrm{crys}} \cap B^+_{\mathrm{dR}})^{\varphi=1} = \mathbb{Q}_p$.

⌟

Proof: ? □

5 deRham Representations

Lemma (18.4.5.1). Let V be a finite $\mathbb{Q}_p$-vector space with an action of Gal_K, then the action is continuous iff the induced action on $V \otimes_{\mathbb{Q}_p} B^+_{\mathrm{dR}}$ is continuous. ⌟

Proof: This is because the action of Gal_K on B^+_{dR} is continuous, and V has the induced topology in $V \otimes_{\mathbb{Q}_p} B^+_{\mathrm{dR}}$. □

Prop. (18.4.5.2) [$\mathbb{C}_K$-admissible Representations are deRham]. $\mathrm{Rep}^{\mathbb{C}_K\text{-adm}}_{\mathbb{Q}_p}(\mathrm{Gal}_K) \subset \mathrm{Rep}^{\mathrm{dR}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$. ⌟

Proof: For $V \in \mathrm{Rep}^{\mathbb{C}_K}_{\mathbb{Q}_p}$, by(18.4.1.2), there exists a finite extension L/K s.t. V is $L\widehat{K^{\mathrm{ur}}}$-admissible. Thus V is deRham as $L\widehat{K^{\mathrm{ur}}} \subset B_{\mathrm{dR}}$(18.4.4.13). □

Prop. (18.4.5.3) [Potentially deRham are deRham]. Let $K' \subset \mathbb{C}_K$ be another p-adic field, then

$$\mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_K) \cap \mathrm{Rep}^{\mathrm{dR}}_{\mathbb{Q}_p}(\mathrm{Gal}_{K'}) = \mathrm{Rep}^{\mathrm{dR}}_{\mathbb{Q}_p}(\mathrm{Gal}_K).$$

In particular, being deRham is not sensible to ramifications, which is a bad feature compared to being crystalline or semistable. ⌟

Proof: Because $\widehat{K^{\mathrm{ur}}} \subset \widehat{(K')^{\mathrm{ur}}}$ is of finite degree, it suffices to prove for two cases: K'/K is finite or $K' = \widehat{K^{\mathrm{ur}}}$. But the finite case follows from Galois descent the same as??. The second case follows from [Conrad, P80]? □

Prop. (18.4.5.4) [Filtered D_{dR}]. For $V \in \mathrm{Rep}^{\mathrm{fd}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$, there is a finite filtration Fil on $D_{\mathrm{dR}}(V)$ s.t.

$$\mathrm{Fil}^m D_{\mathrm{dR}}(V) = (t^m B_{\mathrm{dR}} \otimes_E V)^{\mathrm{Gal}_K} \subset D_{\mathrm{dR}}(V).$$

⌟

Prop. (18.4.5.5) [deRham Representations are Hodge-Tate]. For $V \in \mathrm{Rep}^{\mathrm{fd}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$,

- there is an injection of graded vector spaces

$$\mathrm{gr}(D_{\mathrm{dR}}(V)) \hookrightarrow D_{\text{H-T}}(V),$$

- If $V \in \mathrm{Rep}^{\mathrm{dR}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$, the map in item1 is an isomorphism, and V is Hodge-Tate.
- If $V \in \mathrm{Rep}^{\mathrm{dR}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$,

$$B_{\mathrm{dR}} \otimes_K D_{\mathrm{dR}}(V) \cong B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$$

  identifies filtrations.

⌟

Proof: 1: Consider the exact sequences

$$0 \to \mathrm{Fil}^{m+1} B_{\mathrm{dR}} \to \mathrm{Fil}^m B_{\mathrm{dR}} \to \mathbb{C}_p(m) \to 0 (18.4.4.13).$$

Tensoring V and taking Gal_K-invariants give injections

$$h : \mathrm{gr}^m(D_{\mathrm{dR}}(V)) \hookrightarrow V(m)^{\mathrm{Gal}_K},$$

giving the injection $\mathrm{gr}(D_{\mathrm{dR}}(V)) \hookrightarrow D_{\text{H-T}}(V)$.

2: If $V \in \mathrm{Rep}^{\mathrm{dR}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$, this is an isomorphism by dimension reason, and V is Hodge-Tate by dimension reason.

3: Firstly notice $\mathrm{Fil}^m(B_{\mathrm{dR}} \otimes_K D_{\mathrm{dR}}(V)) \subset \mathrm{Fil}^m(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)$ is trivial, thus it suffices to show that the induced map

$$f : \mathrm{gr}(B_{\mathrm{dR}} \otimes_K D_{\mathrm{dR}}(V)) \to \mathrm{gr}(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V) = B_{\text{H-T}} \otimes_{\mathbb{Q}_p} V$$

is an isomorphism. But notice

$$B_{\text{H-T}} \otimes \mathrm{gr}(D_{\mathrm{dR}}(V)) \xrightarrow{g} \mathrm{gr}(B_{\mathrm{dR}} \otimes_K D_{\mathrm{dR}}(V)) \xrightarrow{f} B_{\text{H-T}} \otimes_{\mathbb{Q}_p} V$$

equals $B_{\text{H-T}} \otimes h$, so g is an isomorphism because it is surjective, and thus f is also an isomorphism. □

Cor. (18.4.5.6). 1-dimensional Hodge-Tate representations are deRham. ⌟

Proof: This is because if $V \cong \mathbb{Q}_p(\psi)$ where ψ is a character of Gal_K, and $\mathbb{C}_p \otimes_E V \cong \mathbb{C}_p(m)$, then by Sen-Tate(18.4.1.3), $\psi(-m)$ is potentially unramified, thus $\mathbb{C}_p$-admissible by(18.4.1.2), and thus deRham(18.4.5.2). □

Remark (18.4.5.7) [D_{dR} Insensitive to Ramifications]. D_{dR} is far from fully faithful. In fact, any unramified representation V is deRham by(18.4.5.3), and $D_{\mathrm{dR}}(V)$ is a simple filtration with graded ring $K^d[0]$, but V can be different from trivial representation. ⌟

Prop. (18.4.5.8). The functor $D_{\mathrm{dR}} : \mathrm{Rep}^{\mathrm{dR}}_{\mathbb{Q}_p}(\mathrm{Gal}_K) \to \mathrm{Fil}\,\mathcal{V}\mathrm{ect}_K$ is faithful and exact, and commutes with taking tensor products and duals. Moreover, the perfect pairing in(18.1.1.20) is a perfect pairing of filtered vector spaces. ⌟

Proof: Let $0 \to V_1 \to V \to V_2 \to V \in \mathrm{Rep}^{\mathrm{dR}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$ be an exact sequence, then V_i are also Hodge-Tate by(18.4.5.5), so there is an exact sequence

$$0 \to \mathrm{gr}(D_{\mathrm{dR}}(V_1)) \to \mathrm{gr}(D_{\mathrm{dR}}(V)) \to \mathrm{gr}(D_{\mathrm{dR}}(V_2)) \to 0,$$

showing that

$$0 \to D_{\mathrm{dR}}(V_1) \to D_{\mathrm{dR}}(V) \to D_{\mathrm{dR}}(V_2) \to 0$$

is an exact sequence of filtered vector spaces.

For tensor product, it suffices to show that

$$\mathrm{gr}(D_{\mathrm{dR}}(V_1) \otimes D_{\mathrm{dR}}(V_2)) \to \mathrm{gr}(D_{\mathrm{dR}}(V_1 \otimes V_2))$$

is an isomorphism, which reduces to

$$D_{\text{H-T}}(V_1) \otimes D_{\text{H-T}}(V_2) \cong D_{\text{H-T}}(V_1 \otimes V_2)(18.1.1.20).$$

For perfect pairing, it suffices to show that the map

$$D_{\mathrm{dR}}(V^\vee) \to D_{\mathrm{dR}}(V)^\vee$$

is an isomorphism of filtered vector spaces. But then it reduces to the isomorphism

$$D_{\text{H-T}}(V^\vee) \cong D_{\text{H-T}}(V)^\vee(18.1.1.20).$$

□

Prop. (18.4.5.9) [Extensions of deRham Representations]. If $0 \to V_1 \to V \to V_2 \to 0$ is an exact sequence in $\mathrm{Rep}^{\mathrm{fd}}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$ s.t. V_1, V_2 are deRham, and the Hodge-Tate weights of V_1 are strictly larger than that of V_2, then V is deRham.

In particular, any upper-triangular representation with diagonal $(\mathbb{Q}_p(a_1), \mathbb{Q}_p(a_2), \ldots, \mathbb{Q}_p(a_n))$ with $a_1 > a_2 \ldots > a_n$ is deRham. ⌟

Proof: By twisting, we may assume that all Hodge-Tate weights of V_1 are positive and Hodge-Tate weights of V_2 are non-positive. There is an exact sequence

$$0 \to D_{\mathrm{dR}}(V_1) \to D_{\mathrm{dR}}(V) \to D_{\mathrm{dR}}(V_2) = \mathrm{Fil}^0 D_{\mathrm{dR}}(V_2)$$

so it suffices to show that $\mathrm{Fil}^0 D_{\mathrm{dR}}(V) \to \mathrm{Fil}^0 D_{\mathrm{dR}}(V_2)$ is surjective. But it follows from(8.7.3.15) that there is an exact sequence

$$\mathrm{Fil}^0 D_{\mathrm{dR}}(V) \to \mathrm{Fil}^0 D_{\mathrm{dR}}(V_2) \to H^1_{\mathrm{cont}}(\mathrm{Gal}_K, B_{\mathrm{dR}}^+ \otimes_{\mathbb{Q}_p} V_1).$$

So it suffices to show that $H^1(\mathrm{Gal}_K, B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V_1) = 0$. The exact sequence

$$0 \to t_\varepsilon^{m+1} B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V_1 \to t_\varepsilon^m B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V_1 \to \mathbb{C}_p(m) \otimes_{\mathbb{Q}_p} V_1 \to 0$$

induces a surjection $H^1_{\mathrm{cont}}(\mathrm{Gal}_K, t_\varepsilon^{m+1} B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V_1) \twoheadrightarrow H^1_{\mathrm{cont}}(\mathrm{Gal}_K, t_\varepsilon^m B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V_1)$ by hypothesis. Notice B_{dR}^+ is t_ε-complete, so we can use approximation technique similar to(8.7.4.3) to show that $H^1_{\mathrm{cont}}(\mathrm{Gal}_K, t_\varepsilon^m B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V_1) = 0$. □

Remark (18.4.5.10). For an example of $V \in \mathrm{Rep}_{\mathbb{Q}_p}^{\text{H-T}}(\mathrm{Gal}_K)$ that is not deRham, Cf.[Conrad, P78]. ⌟

B_{dR}-Representations

Fontaine in [Arithmétique des représentations galoisiennes p-adiques, 2004] studied $\mathrm{Rep}_{B_{\mathrm{dR}}}(\mathrm{Gal}_K)$ in similar spirit of Sen's theory. He firstly showed that any B_{dR}-representations descends to a $K_\infty((t))$-representation W, and similar to Sen's operator, Fontaine defined a K_∞-linear derivative $\nabla_W : W \to W$.

6 Crystalline Representations

References are [Crystalline Representations and F-crystals, Kisin].

Thm. (18.4.6.1). The Tannakian category of crystalline representations of Gal_K is equivalent to the Tannakian categories of weakly admmisible filtered isocrystals. ⌟

Proof: □

Prop. (18.4.6.2). Let L/K be a finite field extension, then

$$\mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_K) \cap \mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{crys}}(\mathrm{Gal}_L) = \mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{crys}}(\mathrm{Gal}_K).$$

⌟

Proof: Cf.[Period Rings, P52].? □

Prop. (18.4.6.3) [Unramified Representations are crystalline].

$$\mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{fd,ur}}(\mathrm{Gal}_K) \subset \mathrm{Rep}_{\mathbb{Q}_p}^{\mathbb{C}_p\text{-adm}+\mathrm{crys}}(\mathrm{Gal}_K).$$

⌟

Proof: By(18.4.1.1), any unramified $V \in \mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{fd}}(\mathrm{Gal}_K)$ is $\widehat{K^{\mathrm{ur}}}$-admissible, thus B_{crys}-admissible as $\widehat{K^{\mathrm{ur}}} \subset B_{\mathrm{crys}}$(18.4.4.14). And V is also $\mathbb{C}_p$-admissible by(18.4.1.1).

To show the converse inclusion, use(18.4.1.2)(18.1.1.16) and the fact $L\widehat{K^{\mathrm{ur}}} \cap B_{\mathrm{crys}} = \widehat{K_0^{\mathrm{ur}}}$?. □

Remark (18.4.6.4). For examples of $V \in \mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{dR}}(\mathrm{Gal}_K)$ that is not crystalline, Cf.[Period Rings, P52].? ⌟

Prop. (18.4.6.5) [Crystalline Representation]. The functor

$$\mathcal{D} : \mathrm{Rep}_{B_e}(G_K)' \to \varphi\text{-}\mathcal{M}\mathrm{od}_{K_0} : W \mapsto (W \otimes_{B_e} B_{\mathrm{crys}})^{\mathrm{Gal}_K}$$

are left adjoint to the functor

$$\mathcal{V} : \varphi\text{-}\mathcal{M}\mathrm{od}_{K_0} \to \mathrm{Rep}_{B_e} G'_K : (D, \varphi_D) \mapsto (D \otimes_{K_0} B_{\mathrm{crys}})^{\varphi_D \otimes \varphi = \mathrm{id}}$$

Moreover, $\mathcal{V}$ is fully faithful, $\mathrm{id} \cong \mathcal{D} \circ \mathcal{V}$, $\mathcal{V} \circ \mathcal{D} \hookrightarrow \mathrm{id}$, and $M \in \mathrm{Rep}_{B_e}(\mathrm{Gal}_K)$ is in the image of $\mathcal{V}$ iff $\mathcal{V}(\mathcal{D}(M)) \cong M$. $\lrcorner$

Proof: Cf.[Laurent Fargues and Jean-Marc Fontaine Prop10.2.12]. □

Cor. (18.4.6.6). In particular, a B_e-representation is crystalline iff it is in the image of $\mathcal{V}$. Now we define a Vector bundle $\mathcal{E}$ on X to be crystalline iff the $H^0(X \backslash \{\infty\}, \mathcal{E})$ is crystalline. $\lrcorner$

7 Semistable Representations

Thm. (18.4.7.1) [deRham $\iff$ potentially Semistable(Fontaine's Potentially Semistable Theorem), Colmez/André-Kedlaya-Mebkhout]. $V \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$ is deRham iff it is potentially semistable. $\lrcorner$

Proof: □

Cor. (18.4.7.2). For $V \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$, we have the following implications:

$$\begin{array}{ccccc}
\text{unramified} = \mathbb{C}_p\text{-adm} + \text{crystalline} & \Longrightarrow & \text{crystalline} & \Longrightarrow & \text{semistable} \\
\Downarrow & & \Downarrow & & \Downarrow \\
\mathbb{C}_p\text{-adm} = \text{pot.unramified} = \text{Hodge-Tate with weights } 0 & \Longrightarrow & \text{pot.crys} & \Longrightarrow & \text{de Rham} = \text{pot.semistable} \\
 & & & & \Downarrow \\
 & & & & \text{Hodge-Tate}
\end{array}$$

$\lrcorner$

Prop. (18.4.7.3) [deRham Representation gives Weil-Deligne Representations]. For $K \in p\text{-}\mathtt{LField}$, there is a functor

$$\mathrm{WD} : \mathrm{Rep}^{\mathrm{dR}}_{\mathbb{Q}_\ell}(\mathrm{Gal}_K) \to \mathfrak{wd}(W_K).$$

$\lrcorner$

Proof: ? Cf.[Fontaine-Mazur, Geometric Galois Representations] □

8 (φ, Γ)-Modules

Main References are [Fontaine90: Représentations p-adiques des corps locaux],[Fontaine94a: Le corps des périodes p-adiques] and [Fonatine94b: Repésentations p-adiques semi-stables]. I'm mostly following [Berger, Galois representations and (φ, Γ)-modules].

Def. (18.4.8.1) [φ-module]. Let M be a A-module and $\sigma : A \to A$ is a ring map. Then an additive map $\varphi : M \to M$ is called **σ-semi-linear** iff $\varphi(am) = \sigma(a)\varphi(m)$ for $a \in A$. A **φ-module** over (A, σ) is an A-module M with a σ-semi-linear φ. The category of φ-modules over A is denoted by $\varphi\text{-}\mathcal{M}\mathrm{od}_A$.

Giving a A-module M and a $\varphi : M \to M$, there is a map $\Phi : A \otimes_{\sigma,A} M = \sigma_* M \to M : \lambda \otimes m \to \lambda\varphi(m)$, which is a A-module map iff φ is σ-semi-linear.

If we define a ring $A_\sigma[\varphi]$ as the free group $A[X]$ modulo the relation $Xa = \sigma(a)X$ and ring relations in A, then it is a ring. Then a φ-module over (A, σ) is equivalent to a left $A_\sigma[\varphi]$-module.

Thus $\varphi\text{-}\mathcal{M}\mathrm{od}_A$ is a Grothendieck Abelian category with tensor products, and moreover, the kernel as $A_\sigma[\varphi]$-module is the same as the kernel as a A-module. ⌟

Def. (18.4.8.2). If there is a map $\alpha : (A_1, \sigma_1) \to (A_2, \sigma_2)$ that commutes with σ_i, then we have a **pullback** from $\Phi\mathcal{M}_1$ to $\Phi\mathcal{M}_2$: $\alpha^*(M) = (A_2)_{\sigma_2}[\varphi] \otimes_{(A_1)_{\sigma_1}[\varphi]} M$(18.4.8.1). ⌟

Def. (18.4.8.3) [Étale φ-Modules]. If A is Noetherian, then a φ-module M is called **étale** iff it is f.g and the corresponding $\Phi : \sigma_* M \to M$ in(18.4.8.1) is a bijection. The subcategory of étale φ-modules is denoted by $\varphi\text{-}\mathcal{M}\mathrm{od}^{\text{ét}}(A)$.

In case when σ is a bijection, Φ is a bijection iff φ is a bijection. ⌟

Proof: If σ is a bijection, then $M \to \sigma_* M$ is a bijection by $\lambda \otimes m \to \sigma^{-1}(\lambda)m$. □

Prop. (18.4.8.4). If A is Noetherian and A_σ is flat, then $\varphi\text{-}\mathcal{M}\mathrm{od}^{\text{ét}}(A)$ is a Tannakian category. ⌟

Proof: 0 is the zero object, the canonical sum&product are clearly étale . And we need to check the kernel and cokernel are étale . But we have an exact sequence $0 \to \ker \to M \to N \to \mathrm{Coker} \to 0$ so we tensor with A_σ to get a morphism of sequences that $\sigma_* M \to M, \sigma_* N \to N$ are both bijective, so by 5-lemma, it is bijection at kernel and cokernel, so they are étale . □

Def. (18.4.8.5) [Dual Étale φ-Modules]. For $E \in \texttt{Field}, M \in \varphi\text{-}\mathcal{M}\mathrm{od}^{\text{ét}}(E)$, the isomorphism $\Phi : M_\varphi \cong M$ induces an isomorphism

$$\Phi^t : M^\vee \cong (M_\varphi)^\vee = M_\varphi^\vee.$$

Thus the dual $\Phi^{-t} : M_\varphi^\vee \cong M^\vee$ shows $M^\vee$ is also an étale φ-module. ⌟

Prop. (18.4.8.6) [$\mathbb{F}_p$-Representations and Étale φ-Modules]. Let $E \in \texttt{Field}^p$, then

- For any $V \in \mathrm{Rep}^{\mathrm{fd}}_{\mathbb{F}_p}(\mathrm{Gal}_E)$, V is E^{sep}-admissible, and

$$D_{E^{\mathrm{sep}}}(V) = (E^{\mathrm{sep}} \otimes V)^{\mathrm{Gal}_E}$$

  has a φ-action, and it is an étale φ-module.

- For any $M \in \varphi\text{-}\mathcal{M}\mathrm{od}(E)$,

$$\mathbb{V}(M) = (E^{\mathrm{sep}} \otimes_E M)^{\varphi = \mathrm{id}}$$

  is a $\mathbb{F}_p$-representation of Gal_E, and there is an injection

$$\alpha_M : E^{\mathrm{sep}} \otimes_{\mathbb{F}_p} \mathbb{V}(M) \hookrightarrow E^{\mathrm{sep}} \otimes_E M.$$

- These two functors define an equivalence of Tannakian categories(4.2.1.13)

$$D_{E^{\mathrm{sep}}} : \mathrm{Rep}_{\mathbb{F}_p}(\mathrm{Gal}_E) \cong \varphi\text{-}\mathcal{M}\mathrm{od}^{\text{ét}}(E) : \mathbb{V}.$$

⌟

Proof: 1: V is E^{sep}-admissible by(18.1.1.14). To show it is étale , it suffices to show that $\varphi : D_{E^{\text{sep}}}(V) \to D_{E^{\text{sep}}}(V)$ is bijective. Let $e_1, \dots, e_n$ be a basis of $D_{E^{\text{sep}}}(V)$, and $v_1, \dots, v_n$ be a basis of V, then $\underline{e} = \underline{v}B$ for some matrix $B \in \text{GL}(n; E^{\text{sep}})$. Then if $[\varphi]\underline{e} = A\overline{e}$ for $A \in \text{Mat}(n; E)$, then $A = B^{-1}\varphi(B)$, and $\det(A) = \det(B)^{p-1} \neq 0$, so φ is bijective.

2: It suffices to show that if $v_1, \dots, v_h \in \mathbb{V}(M)$ are linearly dependent over E^{sep}, then they are dependent over $\mathbb{F}_p$. For this, we use induction on h: Suppose $\sum \lambda_i v_i = 0$, we may assume that $v_h = -1$, so $v_h = \sum_{i=1}^{h-1} \lambda_i v_i$, and by an action of φ, then $\sum_{i=1}^{h-1} (\lambda_i^p - \lambda_i) v_i = 0$, so by induction hypothesis, $\lambda_i \in \mathbb{F}_p$.

3: For $V \in \text{Rep}_{\mathbb{F}_p}(\text{Gal}_E)$, because E is E^{sep}-admissible,

$$\mathbb{V}(D_{E^{\text{sep}}}(V)) = (E^{\text{sep}} \otimes_E D_{E^{\text{sep}}}(V))^{\text{Gal}_E} \cong (E^{\text{sep}} \otimes_{\mathbb{F}_p} V)^{\text{Gal}_E} = V.$$

Conversely, there is a

To show these are isomorphisms of Tannakian categories, one can easily show that both $D_{E^{\text{sep}}}$ and $\mathbb{V}$ preserve tensor products and they identify identity elements $\mathbb{F}_p$ and E. □

Cor. (18.4.8.7). Isomorphism classes of d-dimensional p-adic representations of Gal_E are in bijection with the isomorphism classes of matrixes in $\text{GL}(d; E)$ where

$$A \sim B \iff \exists P \in \text{GL}(d; E), B = P^{-1} A \varphi(P).$$

⌟

Galois Representations and Étale φ-Modules

Notation (18.4.8.8). Let $E \in \texttt{Field}^p$, denoted $\mathcal{O}_{\mathcal{E}} = \text{Coh}(E)$(5.5.3.27), and $\mathcal{E} = \text{Frac}(\mathcal{O}_{\mathcal{E}}) = \mathcal{O}_{\mathcal{E}}[\frac{1}{p}]$. $\mathcal{E}$ has a natural Frobenius. ⌟

Prop. (18.4.8.9). By the functoriality of Cohen rings**?**, if $\mathcal{O}_{\mathcal{E}^{\text{ur}}} = \text{Coh}(\overline{E})\mathcal{E}^{\text{ur}} = \mathcal{O}_{\mathcal{E}^{\text{ur}}}[\frac{1}{p}]$, then there is a bijection $\text{Gal}(\mathcal{E}^{\text{ur}}/\mathcal{E}) \cong \text{Gal}_E$. Thus there are Gal_K-action and φ-action on $\mathcal{O}_{E^{\text{ur}}}, \mathcal{E}_{\text{ur}}$ and by continuity extends to actions on $\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}}, \widehat{\mathcal{E}_{\text{ur}}}$, and

$$(\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}})^{\text{Gal}_E} = \mathcal{E}, \quad (\mathcal{E}^{\text{ur}})^{\text{Gal}_E} = \mathcal{O}_E, (\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}})^{\varphi=\text{id}} = \mathbb{Q}_p, \quad (\mathcal{E}^{\text{ur}})^{\varphi=\text{id}} = \mathbb{Z}_p.$$

⌟

Proof: **?** □

Prop. (18.4.8.10). For $M \in \varphi\text{-}\mathfrak{Mod}^{\text{ft}}(\mathcal{O}_{\mathcal{E}})$, M is étale over $\mathcal{O}_E$ iff $M/(p)$ is étale over E. ⌟

Proof: This is because étale is equivalent to the matrix of φ is a bijection, which is equivalent to its reduction modulo p is a bijection. □

Def. (18.4.8.11) [Effective φ-Modules]. An **effective φ-module** over $\mathcal{E}$ is a φ-module $(D, \varphi) \in \varphi\text{-}\mathfrak{Mod}_{\mathcal{E}}$ s.t. there is a complete $\mathcal{O}_E$-lattice M of D that $\varphi(M) \subset M$. ⌟

Def. (18.4.8.12) [Stably-Étale φ-Modules]. A **stably-étale φ-module** over $\mathcal{E}$ is a φ-module over $\mathcal{E}$ s.t. there exists a φ-stable $\mathcal{O}_{\mathcal{E}}$-lattice in $\mathcal{E}$ that is an étale φ-module over $\mathcal{O}_E$. Then the category of stably-étale φ-modules is a Tannakian category, denoted by $\varphi\text{-}\mathfrak{Mod}^{\text{st}\,.\,\text{ét}}(\mathcal{O}_{\mathcal{E}})$. ⌟

Proof: For $\mathcal{O}_\mathcal{E}$ this follows from(18.4.8.4), and for $\mathcal{E}$, notice if $D = M[\frac{1}{p}], D' = M'[\frac{1}{p}]$, then

$$\mathrm{Hom}_{\varphi\,\mathcal{M}\mathrm{od}^{\text{ét}}(\mathcal{E})}(D, D') = \mathrm{Hom}_{\varphi\,\mathcal{M}\mathrm{od}^{\text{ét}}(\mathcal{O}_\mathcal{E})}(L, L')[\frac{1}{p}]$$

and $p : D' \to D'$ is an isomorphism, so it follows that $\varphi\,\mathcal{M}\mathrm{od}^{\text{ét}}(\mathcal{O}_\mathcal{E})$ is also Abelian. □

Prop. (18.4.8.13). Any $V \in \mathrm{Rep}_{\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}}(\mathrm{Gal}_E)$ is trivial. ⌟

Proof: Cf.[Fontaine-Ouyang]P34.? □

Thm. (18.4.8.14) [Classification of $\mathrm{Rep}_{\mathbb{Z}_p}(\mathrm{Gal}_E)$]. For $V \in \mathrm{Rep}_{\mathbb{Z}_p}(\mathrm{Gal}_E)$,

$$\mathbb{M}(V) = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} V)^{\mathrm{Gal}_E}$$

is an étale φ-module over $\mathcal{O}_\mathcal{E}$, and for any $M \in \varphi\text{-}\mathcal{M}\mathrm{od}^{\text{ét}}(\mathcal{O}_\mathcal{E})$,

$$\mathbb{V}(M) = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_\mathcal{E}} M)^{\varphi=\mathrm{id}}$$

is a $\mathbb{Z}_p$-representation of Gal_E. And these two functors define an equivalence of categories:

$$\mathbb{M} : \mathrm{Rep}_{\mathbb{Z}_p}(\mathrm{Gal}_E) \cong \varphi\text{-}\mathcal{M}\mathrm{od}^{\text{ét}}(\mathcal{O}_\mathcal{E}) : \mathbb{V}.$$

⌟

Proof: To show $\mathbb{M}(V)$ is étale , Cf.[Fontaine]P35.

By(18.4.8.15), we have an isomorphism

$$\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} \mathbb{V}(M) \cong \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_\mathcal{E}} M,$$

and by(18.4.8.13),

$$\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_\mathcal{E}} \mathbb{M}(V) \cong \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} V.$$

Thus

$$\mathbb{V}(\mathbb{M}(V)) = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_\mathcal{E}} \mathbb{M}(V))^{\varphi=\mathrm{id}} \cong (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} V)^{\varphi=\mathrm{id}} = V (18.4.8.9),$$
$$\mathbb{M}(\mathbb{V}(M)) = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} \mathbb{V}(M))^{\mathrm{Gal}_E} \cong (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_\mathcal{E}} M)^{\mathrm{Gal}_E} = M (18.4.8.9).$$

□

Lemma (18.4.8.15). Situation as in(18.4.8.14),

$$\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} V(M) \cong \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_\mathcal{E}} M.$$

⌟

Proof: Cf.[Fontaine-Ouyang]P36.? □

Thm. (18.4.8.16) [Classification of $\mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_E)$].

- For $V \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_E)$,

$$\mathbb{D}(V) = (\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V)^{\mathrm{Gal}_E}$$

is an stably-étale φ-module over $\mathcal{E}$, and there is a natural isomorphism

$$\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_\mathcal{E} \mathbb{D}(V) \cong \widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V.$$

- for any $D \in \varphi\text{-}\mathcal{M}\mathrm{od}^{\mathrm{st\,.\,\acute{e}t}}(\mathcal{E})$,
$$\mathbb{V}(D) = (\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathcal{E}} D)^{\varphi=\mathrm{id}}$$
is a $\mathbb{Q}_p$-representation of Gal_E, and there is a natural isomorphism
$$\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} \mathbb{V}(D) \cong \mathcal{E}^{\mathrm{ur}} \otimes_{\mathcal{E}} D,$$
- These two functors define an equivalence of Abelian Tannakian categories(4.2.1.13):
$$\mathbb{M} : \mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_E) \cong \varphi\text{-}\mathcal{M}\mathrm{od}^{sst.\,\acute{e}t}(\mathcal{E}) : \mathbb{D}.$$

⌟

Proof: For any $V \in \mathrm{Rep}^{\mathrm{fd}}_{\mathbb{Q}_p}(\mathrm{Gal}_E)$, by(18.3.1.3), there exists a stable $\mathbb{Z}_p$-lattice, thus
$$\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T)[\frac{1}{p}], \quad \mathbb{D}(V) = \mathbb{D}(T)[\frac{1}{p}] = \mathcal{E} \otimes_{\mathcal{O}_{\mathcal{E}}} \mathbb{D}(T).$$
and for any $D \in \varphi\text{-}\mathcal{M}\mathrm{od}^{\mathrm{st\,.\,\acute{e}t}}(\mathcal{E})$, there exists an $\mathcal{O}_{\mathcal{E}}$-lattice stable under φ, which is an étale φ-module over $\mathcal{O}_E$. Thus
$$\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathcal{E}} D = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M)[\frac{1}{p}], \quad \mathbb{V}(D) = V(M)[\frac{1}{p}] = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbb{V}(M).$$
Thus it is clear that the assertion follows from that of(18.4.8.14). □

Cor. (18.4.8.17). Étale modules over E of rank d are of the form $M_A = \oplus_{i=1}^d E e_i$ with
$$\varphi : M \to M : \varphi(\lambda e_j) = \lambda^p \sum_{i=1}^d a_{ij} e_i.$$

Isomorphism classes of d-dimensional $\mathbb{Q}_p$-representations of Gal_E are in bijection with the isomorphism classes of matrixes in $\mathrm{GL}(d; \mathcal{O}_{\mathcal{E}})$ where
$$A \sim B \iff \exists P \in \mathrm{GL}(d; \mathcal{E}), B = P^{-1} A \varphi(P).$$

⌟

(φ, Γ)-Modules

Def. (18.4.8.18) [(φ, Γ)-modules]. If A is a topological ring with a Frobenius φ, and A has an action of a topological group Γ that commutes with σ, then a (φ, Γ)**-module** M is a φ-module M over A with a semi-linear action of Γ that commutes with φ.

If A is complete and φ is flat, then an **étale** (φ, Γ)**-module** M is a (φ, Γ)-module that the φ-module structure is étale (18.4.8.3).

Similar to φ-modules, (φ, Γ)-modules form a Tannakian category.? ⌟

Thm. (18.4.8.19) [Classification of $\mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$]. Cf.[Fontaine, Ouyang]. ⌟

Overconvergent (φ,Γ)-Modules

Filtered (φ,N)-Modules

Def. (18.4.8.20) [$(\varphi, N, \mathrm{Gal}(L/K))$**-Modules**]. Let L/K be a Galois extension with residue field k_L and $L_0 = L \cap K_0$.

Then the category (φ,N)-$\mathcal{M}\mathrm{od}_{L/K}$ of $(\varphi, N, \mathrm{Gal}(L/K))$-modules consists of f.d. L_0-spaces V_0 with

- a σ-semi-linear endomorphism,
- a L_0-linear endomorphism N,
- a semi-linear continuous action of $\mathrm{Gal}(L/K)$ (w.r.t the discrete topology).

That satisfies:

- $N\varphi = p\varphi N$,
- N, φ commutes with $\mathrm{Gal}(L/K)$-actions.

Notice that the condition implies N maps the subspace of φ-slope l to the subspace of φ-slope $l-1$, in particular, N is nilpotent. ⌟

Prop. (18.4.8.21). Situation as in(18.4.8.20), (φ,N)-$\mathcal{M}\mathrm{od}_{L/K}$ is an Abelian Tannakian category, where the actions on the tensor is defined to as follows:

$$\varphi(v\otimes w) = \varphi(v)\otimes\varphi(w), \quad N(v\otimes w) = N(v)\otimes w + v\otimes N(w), \quad g(v\otimes w) = g(v)\otimes g(w).$$

⌟

Def. (18.4.8.22) [Filtered $(\varphi, N, \mathrm{Gal}(L/K))$**-Modules].** The category (φ,N)-$\mathrm{Fil}\,\mathcal{M}\mathrm{od}_{L/K}$ of **filtered** $(\varphi, N, \mathrm{Gal}(L/K))$**-module** consists of tuples

$$(V, \varphi, N, \mathrm{Gal}(L/K), \mathrm{Fil}^\bullet)$$

where

- $(V, \varphi, N, \mathrm{Gal}(L/K)) \in (\varphi,N)$-$\mathcal{M}\mathrm{od}_{L/K}$(18.4.8.20),
- $(V\otimes_{L_0} L, \mathrm{Fil}^\bullet) \in \mathrm{Fil}_L$.

The category φ-$\mathrm{Fil}\,\mathcal{M}\mathrm{od}_{L/K}$ of **filtered** φ**-modules(isocrystals)** over K is the Abelian subcategory of $(\varphi, N, \mathrm{Gal}(L/K))$-$\mathrm{Fil}\,\mathcal{M}\mathrm{od}_{L/K}$ with $N=0$. φ-$\mathrm{Fil}\,\mathcal{M}\mathrm{od}_{K/K}$ is also denoted by φ-$\mathrm{Fil}\,\mathcal{M}\mathrm{od}_K$. ⌟

Prop. (18.4.8.23) [HN-Formalism for Filtered φ**-Modules].** The category φ-$\mathrm{Fil}\,\mathcal{M}\mathrm{od}_{L/K}$(18.4.8.22) is a HN-formalism where $\mathcal{A}$ is the Abelian category φ-$\mathcal{M}\mathrm{od}(L_0)$(18.4.8.20), the rank is defined as usual and

$$\deg((V,\varphi,\mathrm{Fil}^\bullet)) = t_{\text{H-T}}(V_L, \mathrm{Fil}^\bullet) - t_N(V,\varphi)$$

where $t_{\text{H-T}}$ is the Hodge-Tate degree(4.3.4.27) and $t_N = v_p(\det(\varphi; V))$. This is a HN-formalism. ⌟

Proof: The proof is clear, the same as that of(4.3.4.27). □

Def. (18.4.8.24) [Weakly Admissible φ**-Modules].** The cateogory φ-$\mathrm{Fil}\,\mathcal{M}\mathrm{od}_{L/K}^{\mathrm{weak.\,adm}}$ of **weakly admissible** φ**-modules** is the subcategory of φ-$\mathrm{Fil}\,\mathcal{M}\mathrm{od}_{L/K}$ consisting of objects that are semistable of slope 0 w.r.t the HN-formalism(18.4.8.23). It is an Abelian category by(4.3.4.33). ⌟

Prop. (18.4.8.25) [Faltings]. The subcategory (φ,N)-$\mathrm{Fil}\,\mathcal{M}\mathrm{od}_{L/K}^{\mathrm{weak.\,adm}} \subset (\varphi,N)$-$\mathrm{Fil}\,\mathcal{M}\mathrm{od}_{L/K}$ is stable under tensor products. In particular, (φ,N)-$\mathrm{Fil}\,\mathcal{M}\mathrm{od}_{L/K}^{\mathrm{weak.\,adm}}$ is an Tannakian category. ⌟

Proof: [Tensor Products in p-adic Hodge, Totaro, P9,12]. □

Cor. (18.4.8.26). The subcategory $\varphi\text{-Fil}\,\mathcal{M}\text{od}_K^{\text{weak. adm}} \subset \varphi\text{-Fil}\,\mathcal{M}\text{od}_K$ is stable under tensor products and duals. ⌟

Cor. (18.4.8.27). Tensor product of semistable filtered isocrystals in $(\varphi, N)\text{-Fil}\,\mathcal{M}\text{od}_{L/K}$ is also semistable. ⌟

Proof: This is because shifting the filtration of a semistable filtered isocrystal of slope c down by c gives a weakly admissible filtered isocrystal. □

9 (φ, Γ)-Modules over the Robba Ring

Notation (18.4.9.1).

- Let $p \in \mathbf{P}$, $\mathbb{Q}_p \subset_{\text{fin}} K$, $\Gamma = \mathbb{Z}_p^*$.
- Use notations on Robba rings as in Robba Ring.
- Let $H_p = \ker(\text{cycl}_p) \subset \text{Gal}_{\mathbb{Q}_p}$.

⌟

Prop. (18.4.9.2) [Fontaines Ring $B^{\dagger,\text{rig}}$]. There exists a $(\text{Gal}_{\mathbb{Q}_p}, K)$-regular ring $B^{\dagger,\text{rig}}$ with an action of $\text{Gal}_{\mathbb{Q}_p}$ and Frobenius φ s.t. $(B^{\dagger,\text{rig}})^{H_p} = \mathcal{R}_K$, and we can define

$$D_{\dagger,\text{rig}} : \text{Rep}_K^{\text{fd}}(\text{Gal}_K) \to (\varphi, \Gamma)\text{-}\mathcal{M}\text{od}^{\text{ét}}(\mathcal{R}_K) : V \mapsto (V \otimes_{\mathbb{Q}_p} B^{\dagger,\text{rig}})^{H_p}.$$

⌟

Proof: Cf.[Ber02]Section3.4.**?** □

Thm. (18.4.9.3) [Colmez]. The functor $D_{\dagger,\text{rig}}$ induces a tensor equivalence

$$\text{Rep}_K^{\text{fd}}(\text{Gal}_{\mathbb{Q}_p}) \cong (\varphi, \Gamma)\text{-}\mathcal{M}\text{od}^{\text{ét,slope}=0}(\mathcal{R}_K).$$

⌟

Proof: Cf.[P. Colmez, S´erie principale unitaire pour GL2(Qp) et repr´esentations triangulines de dimension 2]Prop2.7.**?** □

<u>**Triangularizable (φ, Γ)-Modules**</u>

Def. (18.4.9.4) [Classification of 1-Dimensional (φ, Γ)-Modules]. Let $\delta : \mathbb{Q}_p^* \to K^*$ be a continuous character, then there is a 1-dimensional (φ, Γ)-module over $\mathcal{R}_K$ with basis x s.t. $\varphi(a) = \delta(p)a, \gamma(a) = \delta(\gamma)a$. Then

- Any (φ, Γ)-module of rank 1 over $\mathcal{R}_K$ is isomorphic to $R_K(\delta)$ for a unique δ. And it is isoclinic of slope $v(\delta(p))$**?**.
- $\text{Ext}_{(\varphi,\Gamma)}(\mathcal{R}_K(\delta_2), \mathcal{R}_K(\delta_1))$ has dimension 1 except when $\delta_1\delta_2^{-1} = x^{-i}$ or $\chi_{\text{cycl}}x^i$ for $i \in \mathbb{N}$(where $x : \mathbb{Q}_p^* \to K^*$ is the natural inclusion), in which case it has dimension 2.

⌟

Proof: Cf.[P. Colmez, S´erie principale unitaire pour GL2(Qp) et repr´esentations triangulines de dimension 2]Section0.1.**?** □

Def. (18.4.9.5) [Triangularizable Representations]. A (φ, Γ)-module D over $\mathcal{R}_K$ is called a **triangularizable** (φ, Γ)**-module** if there is a complete flag of (φ, Γ)-submodules which are direct summands of D.

A Galois representation $V \in \mathrm{Rep}_K^{\mathrm{fd}}(\mathrm{Gal}_{\mathbb{Q}_p})$ is called triangularizable if $D_{\dagger,\mathrm{rig}}(V)$ is triangularizable.

For any triangularizable (φ, Γ)-module D over $\mathcal{R}_K$, the graded pieces $\mathrm{gr}_i(D)$ are isomorphic to $\mathcal{R}_K(\delta_i)$ where $\delta_i : \mathbb{Q}_p^\times \to L^\times$ by(18.4.9.4). These characters δ_i are called the **parameters of** D. ⌟

<u>p**-adic Hodge Theory of** (φ, Γ)**-Modules**</u>

Thm. (18.4.9.6) [Comparison of Fontaine's Functors]. For $V \in \mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{fd}}(\mathrm{Gal}_{\mathbb{Q}_p})$ and $* \in \{\mathrm{crys}, \mathrm{dR}, \mathrm{Sen}\}$,

$$D_*(D_{\dagger,\mathrm{rig}}(V)) = D_*(V).$$

⌟

Proof: Cf.[Ber02]Thm0.2 and Section5.3, [L. Berger, E´quations diff´erentielles p-adiques et (φ, N)-modules filtr´es] and [P. Colmez, Les conjectures de monodromie p-adiques]Prop5.6.**?** □

18.5 Representations of Algebraic Groups

References are[Mil17].

1 Basics

Throughout this subsection, G is an affine algebraic group over a field k if not said.

Def. (18.5.1.1) [Linear Representations of Algebraic Groups]. Let R be a ring and V a free R-module, let $\mathrm{GL}(V)$ be the group functor

$$\mathcal{CA}\mathrm{lg}_R \to \mathcal{G}\mathrm{rp} : R' \mapsto \mathrm{Aut}(V \otimes_R R').$$

Then a **linear representation** (r, V) of an algebraic group G over R is a homomorphism of group functors $r : G \to \mathrm{GL}(V)$. It is called **faithful representation** if r is a monomorphism as natural transformation of functors.

If V is of f.d., this is equivalent to a homomorphism $G \to \mathrm{GL}(V)$. And by(9.1.5.6), it is faithful iff $G \to GL(V)$ is a closed embedding.

For a linear representation (r, V), let $\mathrm{End}(V) = \mathrm{Aut}(r)$. ⌟

Prop. (18.5.1.2) [Representations and Co-modules]. A representation of G on V is equivalent to a right $\Gamma(G)$-comodule structure on V(3.11.2.22). ⌟

Proof: Let $A = \Gamma(G)$. For any representation $r : G \to GL(V)$, it induces a map $G(A) \to GL_A(V \otimes A)$, which maps id_A to a map $\rho : V \to V \otimes A$. Now if $\rho(e_j) = \sum e_i \otimes a_{ij}$, then by funtoriality, the map $G(R') \to GL_R(V \otimes R')$ is given by $g \mapsto (e_j \mapsto e_i \otimes a_{ij}(g))$.

And it can be verified that this is a group homomorphism iff the comodule condition is satisfied. □

Def. (18.5.1.3) [Stabilizers]. Let (r, V) be a representation of an affine group scheme G over R, W a subspace of V, consider the functor

$$\mathrm{Stab}_G(W) : R' \mapsto \{g \in G(R') | g(W_{R'}) = W_{R'}\},$$

then if V is of f.d., $\mathrm{Stab}_G(W)$ is representable by a closed subgroup of G, called the **stabilizer group scheme** of W in V. ⌟

Proof: Let $\rho : \Gamma(G) \to V \otimes \Gamma(G)$ be the comodule action corresponding to r, let $\{e_i\}_{i \in I}$ be a basis for W, and extends it to a basis $\{e_i\}_{J \coprod I}$ of V, and

$$\rho(e_j) = \sum e_i \otimes a_{ij}, \quad a_{ij} \in \Gamma(G).$$

Let $g \in \mathrm{Hom}(\Gamma(G), R')$, then $ge_j = \sum e_i \otimes g(a_{ij})$, and then clearly G_W is represented by the quotient of $\Gamma(G)$ by the ideal generated by $\{a_{ij} | i \in I, j \in J\}$. □

Cor. (18.5.1.4). If S is a scheme and G is an affine group scheme over S, $\mathcal{V}$ a locally free sheaf on S and $\mathcal{W}$ a locally free subsheaf of $\mathcal{V}$, then similarly $\mathrm{Stab}_G(\mathcal{W})$ is representable by a closed subgroup of G over S, by considering affine-locally. ⌟

Cor. (18.5.1.5). Let (ρ, V) be a f.d. representation of G and $S \subset G(k)$ be a subset schematically dense in G, then a subspace $W \subset V$ is stable under G iff it is stable under S. ⌟

Prop. (18.5.1.6) [Fixed Subspace]. Let (r, V) be a linear representation of an algebraic group, define the **fixed subspace** by G:

$$V^G = \{v \in V | gv_R = v_R, \forall R \in \mathcal{CA}\mathrm{lg}_k, g \in G(R)\}.$$

Then for any $R \in \mathcal{CA}\mathrm{lg}_k$, $V^G \otimes R$ is the submodule of $V \otimes R$ that is fixed by elements of $G(R')$ for any $R' \in \mathcal{CA}\mathrm{lg}_R$. ⌟

Proof: Cf.[Mil17]P96. □

Cor. (18.5.1.7). The fixed subspace is compatible with base change of fields. ⌟

Def. (18.5.1.8) [Subrepresentations]. A subspace W of a linear representation V of an algebraic group G is called a **subrepresentation** of V if $\widetilde{G} = \mathrm{Stab}_G(W)$.

A linear representation is called **simple** if has no non-trivial subrepresentations. ⌟

Prop. (18.5.1.9). Let U be a normal subgroup of an algebraic group G, then for any representation V of G, V^U is a subrepresentation of V. ⌟

Prop. (18.5.1.10) [Union of F.D. Subrepresentations]. Let (r, V) be a linear representation of G, then V is a filtered union of its f.d. subrepresentations. ⌟

Proof: It suffices to consider comodules and prove any vector $v \in V$ is contained in a f.d. subcomodule. Let $\{e_i\}$ be a basis of $\Gamma(G)$, let

$$\Delta(e_i) = \sum_{i,k} r_{ijk} e_j \otimes e_k, \quad \rho(v) = \sum_i v_i \otimes e_i, \quad v_i \in V.$$

Because $(\mathrm{id}_V \otimes \Delta) \circ \rho = (\rho \otimes \mathrm{id}_{\Gamma(G)}) \circ \rho$(3.11.2.22), thus

$$\sum_{i,j,k} r_{ijk} v_i \otimes e_j \otimes e_k = \sum_k \rho(v_k) e_k$$

which means

$$\rho(v_k) = \sum_{j,k} r_{ijk} v_i \otimes e_j.$$

Thus $\mathrm{span}\{e_i\}$ is a f.d. comodule of V containing v. □

Cor. (18.5.1.11). Any simple representations of an algebraic group is of f.d. ⌟

Prop. (18.5.1.12) [Schur's Lemma]. Let (V, r) be a simple representation of an algebraic group G, then $\mathrm{End}(V)$ is a f.d. division algebra D over k. In particular, if $k = \overline{k}$, then $\mathrm{End}(V) = k$. ⌟

Prop. (18.5.1.13) [Simple Representations of Product Groups]. Let G_1, G_2 be algebraic groups and V_1, V_2 are simple representations of G_1, G_2 resp., then $V_1 \otimes V_2$ is a simple representation of $G_1 \times G_2$.

Conversely, if $\mathrm{End}(V) = k$ for any simple representation (V, r) of G_1, then any simple representation of $G_1 \times G_2$ is of this form. ⌟

Proof: Cf.[Mil17]P91. □

Def. (18.5.1.14)[Semisimple Representations]. A linear representation (r, V) of an algebraic group is called **semisimple** if it is a direct sum of simple representations. Equivalently, it is a sum of simple subrepresentation.(The proof is the same).

Or equivalently, every submodule has a complement. ⌟

Prop. (18.5.1.15)[Base Change]. Let (V, r) be a f.d. linear representation of an algebraic group over a field k, k'/k a field extension, then $(V', r') = (V, r) \otimes_k k'$ is a representation of $G_{k'}$, and

- If (V', r') is simple, and (V, r) is simple.
- If (V, r) is simple and $\mathrm{End}(V) = k$, then (V', r') is simple.
- If (V, r) is semisimple and k'/k is separable or $\mathrm{End}(V)$ is a separable algebra over k, then (V', r') is semisimple.

⌟

Proof: Cf.[Mil17]P90. □

Prop. (18.5.1.16)[Constructing All F.D. Representations]. Let V be a faithful f.d. representation of G, then every f.d. representation of G is a subquotient of $V^m \otimes (V^\vee)^n$. ⌟

Proof: Cf.[Mil17]P88. □

Def. (18.5.1.17) [Diagonalizable Representation]. A representation of an algebraic group is called **diagonalizable** if it is a direct sum of 1-dimensional representations.

Let G be an algebraic group over a field k and $r : G \to GL(V)$ be a representation. If V is a sum of 1-dimensional representations, then r is diagonalizable(18.5.1.17). ⌟

Proof: Let $V = \sum_{\chi \in X(G)} V_\chi$. If the sum is not direct, then there is are some relation $v_1 + v_2 + \ldots + v_m = 0$ for $v_i \in V_{\chi_i}$. Applying ρ shows

$$0 = v_1 \otimes a(\chi_1) + \ldots + v_m a(\chi_m)$$

so any coordinate of v_i is 0 by(9.1.1.13). □

Prop. (18.5.1.18) [Chevalley]. Let G be an algebraic group, then every algebraic subgroup $H \subset G$ arises as the stabilizer of a 1-dimensional subspace in a f.d. representation of G. ⌟

Proof: Cf.[Mil17]P94. □

Cor. (18.5.1.19). Let G be an algebraic group over a field of characteristic0, then an algebraic subgroup H of G is normal in G iff for any linear representation V of G and a character $\chi \in X(H)$, the eigenspace V_χ is stable under G. ⌟

Proof: □

Prop. (18.5.1.20). Let G be an algebraic group over a field k s.t. the order of $\pi_0(G)$ is prime $\mathrm{char}\, k$, then any representation V of G is semisimple iff it's semisimple when restricted to G^0. ⌟

Linear Algebraic Group

Def. (18.5.1.21) [Linear Algebraic Groups]. Let k be a field, then a **linear algebraic group** over k is a closed subgroup scheme of GL_n for some n.

Notice a linear algebraic group over a field of characteristic 0 is automatically smooth, by Cartier theorem(9.1.4.2). ⌟

Prop. (18.5.1.22) [Affine Algebraic Group is Linear]. If G is an affine group scheme, then the regular representation(9.2.1.2) contains a faithful f.d. subrepresentation. In particular, the regular representation is itself faithful. ⌟

Proof: Let e_i be a generator of $\Gamma(G)$ as a k-algebra, let V be a f.d. subrepresentation of the regular representation containing e_i(18.5.1.10), let v_i be a basis for V, and suppose $\Delta(e_j)=\sum e_i\otimes a_{ij}$, then the image of $\Gamma(GL(V))\to\Gamma(G)$ contains a_{ij}. Now because $\varepsilon: A\to k$ is the counit,

$$e_j=(\varepsilon\otimes\mathrm{id})\Delta(e_j)=\sum\varepsilon(e_i)a_{ij},$$

so the image contains V, so it contains $\Gamma(G)$, so this is a closed immersion, thus a faithful representation, by(18.5.1.1). □

2 Tannakian Duality

In this subsection, let G be an affine group scheme, and k is a field.

Lemma (18.5.2.1). Let G be an affine group scheme over ring R corresponding to a Hopf algebra A. If u is an R-endomorphism of A that the following diagram commutes:

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A\otimes A \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle 1\otimes u} \\ A & \xrightarrow{\Delta} & A\otimes A \end{array},$$

then there exists a $g\in G(R)$ that $u=r_A(g)$, where r_A is the regular action of G on A. ⌟

Proof: Let $\varphi: G\to G$ be the morphism corresponding to u, then the commutative diagram shows $\varphi_S(xy)=x\varphi_S(y)$ for $x,y\in G(S)$. Then $\varphi_S(x)=xg_S$ where $g_S=\varphi_S(e)$.

Then for $f\in A, x\in G(R)$, $x(uf)=\varphi_R(x)(f)=(xg)(f)=x(r_A(f))$, thus $u=r_A(g)$. □

Prop. (18.5.2.2). Let G be an algebraic group over k and R is a k-algebra. Suppose that for any f.d. representation (V,r_V) of G, we are given an R-linear map $\lambda_R: V_R\to V_R$ that satisfies:

- $\lambda_{V\otimes W}=\lambda_V\otimes\lambda_W$.
- $\lambda_1=\mathrm{id}$.
- For G-invariant maps $u: V\to W$, $\lambda_W\circ u_R=u_R\circ\lambda_V$.

then there exists a unique $g\in G(R)$ that $\lambda_V=r_V(g)$ for any V. ⌟

Proof: Cf.[Milne, P164].**?** □

Cor. (18.5.2.3) [Reconstruction Theorem]. Let $\omega:\mathrm{Rep}_k(G)\to Vect_k$ be the forgetful functor, and for any k-algebra R, let $\omega_R=R\otimes\omega$, then this proposition says the canonical morphism $G(R)\to\mathrm{End}^{\otimes}(\omega_R)$ is an isomorphism. Now if $\underline{\mathrm{Aut}}^{\otimes}(\omega)$ is the functor $R\mapsto\mathrm{End}^{\otimes}(\omega_R)$, then $G\cong\underline{\mathrm{Aut}}^{\otimes}(\omega)$. ⌟

Cor. (18.5.2.4). Let G, G' be affine algebraic groups over k and let $F : \mathrm{Rep}_k(G') \to \mathrm{Rep}_k(G)$ be a tensor functor that $\omega^G \circ F = \omega^{G'}$, then there exists a unique homomorphism $f : G \to G'$ that $F = \omega^f$. ⌟

Proof: Such a tensor functor defines a homomorphism

$$F^* : \underline{\mathrm{Aut}}^{\otimes}(\omega^G)(R) \to \underline{\mathrm{Aut}}^{\otimes}(\omega^{G'})(R)$$

functorial in R, thus defines a homomorphism $f : G \to G'$ by Yoneda lemma and(18.5.2.4). □

Lemma (18.5.2.5). Let μ be a cocharacter $\mathbb{G}_m \to G$ over $\overline{\mathbb{Q}_p}$, then the conjugacy class $\{\mu\}$ of μ is defined over a finite extension $E/\mathbb{Q}_p$. ⌟

Proof: By Tannakian duality, two cocharacters are conjugate over a field K iff the filtrations they defined on $V \otimes \overline{\mathbb{Q}_p}$ for some faithful $V \in \mathrm{Rep}_{\mathbb{Q}_p}(G)$ are isomorphic by an action of $G(K)$. Now this action of $G(\overline{\mathbb{Q}_p})$ on $V_{\overline{\mathbb{Q}_p}}$ is defined over a f.d. field extension $E/\mathbb{Q}_p$, so the filtrations are isomorphic by an action of $G(E)$. □

Prop. (18.5.2.6) [Abstract Jordan Decompositions]. Let G be an algebraic group over a perfect field k and $g \in G(k)$, then there exists unique elements $g_s, g_u \in G(k)$ that for any representation (V, r_V) of G, $r_V(g_s) = r_V(g)_s$ and $r_V(g_u) = r_V(g)_u$. Furthermore,

$$g = g_s g_u = g_u g_s.$$

The elements g_s, g_u are called the semisimple and unipotent parts of g, and this decomposition is called the abstract Jordan decomposition of g. $g \in G(k)$ is called a **semisimple or unipotent element** if $g = g_s$ or $g = g_u$. ⌟

Proof: This follows from the functoriality of Jordan decompositions(3.5.8.7) and the reconstruction theorem(18.5.2.2). □

Cor. (18.5.2.7). To check a decomposition is Jordan decomposition, it suffices to check for a single faithful representation of G. ⌟

Remark (18.5.2.8). Let G be a group variety over an alg.closed field k. In general, the set $G(k)_s$ of semisimple elements in $G(k)$ is not closed for the Zariski topology, but the set $G(k)_u$ of unipotent elements are closed for the Zariski topology. To see this, embed G into GL_n for some n, then the set of unipotent elements are the matrices with characteristic polynomial $(T-1)^n$, and this is a polynomial condition. ⌟

Tannakian Reconstruction

Prop. (18.5.2.9) [Tannakian Reconstruction]. Let $(\mathcal{C}, \otimes)$ be a rigid Abelian tensor category that $k = \mathrm{End}(1)$ and $\omega : \mathcal{C} \to \mathcal{V}\mathrm{ect}_k$ an exact faithful k-linear tensor functor, then the functor $\underline{\mathrm{Aut}}^{\otimes}(\omega)$ is representable by an affine groups scheme G, and $\mathcal{C} \cong \mathrm{Rep}_k(G)$. ⌟

Proof: Cf.[Milne, Tannakian category, P21].**?** □

Cor. (18.5.2.10) [Tannakian Reconstruction]. Let $\mathcal{C}$ be a k-linear Abelian category where k is a field, and $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ a k-bilinear functor. Suppose there are given a faithful exact k-linear functor $\mathcal{C} \to \mathcal{V}\mathrm{ect}_k$ and functorial isomorphisms $\varphi_{X,Y,Z} : X \otimes (Y \otimes Z) \to (X \otimes Y) \otimes Z$ and $\psi_{X,Y} : X \otimes Y \to Y \otimes X$ that

- F commutes with $\otimes$, and maps φ and ψ to the natural associativity and commutativity isomorphism in $Vect_k$.
- There exists an identity object $1 \in \mathcal{C}$ that $k \to \mathrm{End}(1)$ is an isomorphism and $F(1)$ has dimension 1.
- Any object $L \in \mathcal{C}$ that $F(L)$ has dimension 1 is an invertible object.

Then $\mathcal{C}$ is equivalent to $\mathrm{Rep}_k(G)$ for some affine group scheme G over k. In fact, $G \cong \underline{\mathrm{Aut}}^{\otimes}(\omega)$ as in(18.5.2.3) ⌟

Proof: The proof of(18.5.2.9) shows F defines an equivalence of categories $\mathcal{C} \to \mathrm{Rep}_k(G)$ where G is an affine monoid scheme representing $\mathrm{End}_k^{\otimes}(\omega)$. Thus we may assume $\mathcal{C} = \mathrm{Rep}_k(G)$. For the rest, Cf.[Tannakian Categories, Milne, P24]. □

Cor. (18.5.2.11) [Real Algebraic Envelope]. Let K be a topological group, then the category $\mathrm{Rep}_{\mathbb{R}}(K)$ of f.d. continuous real representations, together with the forgetful functor satisfies the hypothesis of(18.5.2.10), thus there is an algebraic group $\widetilde{K}$ over $\mathbb{R}$, called the **real algebraic envelope** of K, and an equivalence of categories

$$\mathrm{Rep}_{\mathbb{R}}(\widetilde{K}) \to \mathrm{Rep}_{\mathbb{R}}(K)$$

induced by a homomorphism $K \to \widetilde{K}(R)$, which is an isomorphism when K is compact**?**. ⌟

Cor. (18.5.2.12) [Hochschild-Mostow Group]. Similar as(18.5.2.11), if G is a complex Lie group or a f.g. abstract group, and $\mathcal{C}$ the category of f.d. complex representations, then it satisfies the hypothesis of(18.5.2.10), thus it is the category of representations of an affine group scheme $A(G)$ over $\mathbb{C}$, together with a homomorphism $P : G \to A(G)$, called the **Hochschild-Mostow group** of G. ⌟

Prop. (18.5.2.13). Let $\mathcal{C}$ be a small k-linear Abelian category, and let $\omega : \mathcal{C} \to \mathcal{V}ect_k$ be an exact faithful k-linear functor, then there exists a coalgebra C s.t. $\mathcal{C}$ is equivalent to the category of C-comodules of f.d. ⌟

Proof: Cf.[Mil17] P175. □

<u>**Properties of G and $\mathrm{Rep}_k(G)$**</u>

Prop. (18.5.2.14). Let G be an affine group scheme over k, then

- G is finite iff there exists an object $X \in \mathrm{Rep}_k(G)$ that every object of $\mathrm{Rep}_k(G)$ is isomorphic to a subquotient of X^n for some $n > 0$.
- G is algebraic iff there exists an object $X \in \mathrm{Rep}_k(G)$ that every object of $\mathrm{Rep}_k(G)$ is isomorphic to a subquotient of $X^n \otimes (X^\vee)^m$ for some $m, n \geq 0$.

⌟

Proof: Cf.[Milne, Tannakian categories, P25]. □

Prop. (18.5.2.15). Let $f : G \to G'$ be a homomorphism of affine group schemes over k, and let ω^f be the corresponding functor $\mathrm{Rep}_k(G') \to \mathrm{Rep}_k(G)$. Then

- f is faithfully flat iff ω^f is fully faithful and each ω^f induces an equivalence of subobjects of X' and $\omega^f(X')$.

- f is a closed immersion iff every object of $\mathrm{Rep}_k(G)$ is isomorphic to a subquotient of an object $\omega^f(X')$.

⌟

Proof: Cf.[Milne, Tannakian categories, P25]. □

Cor. (18.5.2.16). Let k has characteristic 0, then G is connected iff for any non-trivial representation X of G, $\langle X\rangle$ is not stable under $\otimes$. ⌟

Proof: Cf.[Milne, Tannakian categories, P25]. □

3 Unipotent Groups

Def. (18.5.3.1)[Unipotent Groups]. A **unipotent algebraic group** is an algebraic group G s.t. for any non-zero linear representation V of G, $V^G\neq 0$. Equivalently, every such representation sends G into $\mathrm{Unip}(n)$ in some coordinates. ⌟

Prop. (18.5.3.2). Let G be an algebraic group over k and k'/k a field extension, then G is unipotent iff $G_{k'}$ is unipotent. ⌟

Proof: This follows from the fact that for any representation V of G, $(V\otimes k')^{G_{k'}}=V^G\otimes k'$(18.5.1.7). □

Prop. (18.5.3.3). For an affine algebraic group G over a field k, the following are equivalent:

- G is unipotent.
- G is isomorphic to a subgroup of $\mathrm{Unip}(n)$ for some n.
- The Hopf algebra $\Gamma(G)$ is coconnected.

⌟

Proof: Cf.[Mil17]P281. □

Prop. (18.5.3.4). If U is a normal unipotent subgroup of an algebraic group G, then for any semisimple representation V of G, U acts trivially. ⌟

Proof: Consider a simple subrepresentation W of V, then $W^U\neq 0$ is a subrepresentation of G by(18.5.1.9), thus U acts trivially on W. As V is a sum of simple representations(18.5.1.14), U acts trivially on V. □

Prop. (18.5.3.5). Representations of $\mathbb{G}_a$ over a field of characteristic 0 corresponds to locally nilpotent endomorphisms. ⌟

Proof: https://qchu.wordpress.com/2017/11/26/the-representation-theory-of-the-additive-group-s
□

4 Reductive Groups

Prop. (18.5.4.1). A group variety G is reductive if it has a faithful representation that is semisimple over $\overline{k}$, by(18.5.3.4). ⌟

Prop. (18.5.4.2). Let $k\in \mathtt{Field}^0, G\in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/k$ is connected, then the following are equivalent:

- G is a reductive group.

- Every f.d. representation of G is semisimple(18.5.1.14).
- Some faithful representation of G is semisimple(18.5.1.14).

⌟

Proof: □

18.6 Representations of Finite Groups of Lie Type

References are [Bon11], [Introduction to Deligne-Lustig Theory, David Schwein], [Representations of finite groups of Lie type, Dign/Michel, 1991].

Notation (18.6.0.1).
- Use notations defined in Étale Cohomology Theory.
- Let $p \in \mathbf{P}, q \in p^{\mathbb{Z}Z_+}, k \in \texttt{Field}, \#k = q, G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/k$.
- Let $\ell \in \mathbf{P}\backslash p$, K an ℓ-adic local field with ring of integers $\mathcal{O}_K$ and residue field k.

⌟

1 Finite Groups of Lie Type

Def. (18.6.1.1) [Finite Groups of Lie Type]. For a reductive group $G/\overline{k}$, if $F \in \mathrm{End}(G)$ satisfies the fixed point of $F(\overline{k})$ is finite, then its fixed points G^F is called a **finite group of Lie type**.

If G is defined over some finite subfield k, i.e. $G = G_0 \times_k \overline{k}$, and $F = \mathrm{Fr}_{G_0}$, then $G^F = G_0(k)$ is called a **Chevalley group**. If moreover $G_0 \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/k$ is reductive and simply-connected, then $G_0(k)$ is called a **universal finite group**(of Lie type).

If G is a a finite group of Lie type that is not a Chevalley group, then it is called a **twist group**(of Lie type). ⌟

Prop. (18.6.1.2). If $p \in \texttt{Prime}$ and $q \in p^{\mathbb{Z}_+}$,
- $\#GL(2;q) = q(q-1)^2(q+1)$.
- $\#SL(2;q) = \#PGL(2;q) = q(q^2-1)$.
- $\#PSL(2;q) = \begin{cases} q(q^2-1) & ,2|q \\ \frac{1}{2}q(q^2-1) & ,2\nmid q \end{cases}$.

⌟

Thm. (18.6.1.3) [Steinberg]. If $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/\overline{k}$ is simple reductive group, and $F \in \mathrm{End}(G)$ satisfies the fixed point of $F(\overline{k})$ is finite, then there are exactly the following possibilities:
- (Chevalley Groups)F is a standard Frobenius: $A_n, B_n, C_n, D_n, G_2, F_4, E_6, E_7, E_8$.
- (**Steinberg Groups**)$^2A_n, {}^2D_n, {}^3D_4, {}^2_6$.
- (**Suzuki Groups**)$^2B_2, p = 2$.
- (**Ree Groups**)$^2G_2, p = 3$.
- (**Ree Groups**)$^2F_4, p = 2$.

⌟

Proof: □

Examples

Prop. (18.6.1.4) [SL(n)].
- $\mathrm{PSL}(2,\mathbb{F}_2) \cong \mathrm{Sym}(3)$,
- $\mathrm{PSL}(2,\mathbb{F}_3) \cong \mathrm{Alt}(4)$,
- (Jordan1861) For $k \in \texttt{Field}$, $\mathrm{PSL}(n,k)$ is a simple group except for $n = 2$ and $k \cong \mathbb{F}_2$ or $\mathbb{F}_3$.

- $\mathrm{PSL}(2,\mathbb{F}_4)\cong\mathrm{PSL}(2,\mathbb{F}_5)\cong\mathrm{Alt}(5)$.
- $\mathrm{SU}(n)_{\mathbb{F}_q}$ is a twist of $\mathrm{SL}(n)_{\mathbb{F}_q}$, denoted by ${}^2A_{n-1}(\mathbb{F}_{q^2})$.

⌟

Proof: Cf.[DSV03]P74. □

Prop. (18.6.1.5). ⌟

2 Conjugacy Classes

3 Deligne-Lustig Varieties

Def. (18.6.3.1) [Deligne-Lustig Varieties]. ⌟

Affineness of Deligne-Lustig Varieties

4 Deligne-Lustig Theory

Main references are [Finite Groups of Lie Type, Carter], [P. Deligne and G. Lusztig, Representations of reductive groups over finite fields, Ann. of Math. (2) 103 (1976), no.1, 103–161.], [D-L76], https://www.dpmms.cam.ac.uk/~dbms2/deligne_lusztig/.

Deligne and Lustig used the ℓ-adic étale cohomology theory to construct all cuspidal representations of $G(\mathbb{F}_q)$.

Remark (18.6.4.1). Because $G(\mathbb{F}_q)$ is finite and $\mathbb{C}\cong\overline{\mathbb{Q}_\ell}$, we can consider representations $\mathrm{Rep}(G(\mathbb{F}_q))=\{\theta:G(\mathbb{F}_q)\to\mathrm{GL}(\overline{\mathbb{Q}}_\ell)$. ⌟

Def. (18.6.4.2) [Induction Pairs]. A **induction pair for** $G(\mathbb{F}_q)$ is a pair (T,θ), where $T\subset G$ is a maximal torus and θ is an ℓ-adic character $T(\mathbb{F}_q)\to\overline{\mathbb{Q}}_\ell^\times$. ⌟

Deligne-Lustig Inductions

Def. (18.6.4.3) [Deligne-Lustig Inductions]. Let (T,θ) be an induction pair(18.6.4.2), the action of $G(\mathbb{F}_q)$ and $T(\mathbb{F}_q)$ on $\widetilde{X}_S$ commutes, so for any $\theta\in\mathrm{Irr}(T(\mathbb{F}_q))$, the θ-isotopic part of $H^i_{\text{ét},c}(\widetilde{X}_T,\overline{\mathbb{Q}}_\ell)$ is $G(\mathbb{F}_q)$-invariant, thus we can define a **Deligne-Lustig Induction map** that on $\mathrm{Irr}(G(\mathbb{F}_q))$ is defined by

$$R_T^G:\mathrm{Irr}(T(\mathbb{F}_q))\to K_0(\mathrm{Rep}(G(\mathbb{F}_q))):\theta\mapsto\sum_i(-1)^iH^i_{\text{ét},c}(X_T,\overline{\mathbb{Q}}_\ell)^\theta.$$

⌟

Prop. (18.6.4.4). Let (T,θ) be an induction pair, if $\theta^\omega\neq\theta$ for any $w\in W$, then $R_T^G(\theta)\in\mathrm{Irr}(G(\mathbb{F}_q))$. ⌟

Proof: □

Prop. (18.6.4.5). If $(T,\theta),(T',\theta')$ are two induction pairs that are note $G(\mathbb{F}_q)$-conjugate, then $(R_T^G(\theta),R_{T'}^G(\theta'))=0$. ⌟

Proof: □

Def. (18.6.4.6) [Geometrically Conjugate Pairs]. If $(T,\theta),(T',\theta')$ are two induction pairs, they are called **geometrically conjugate** if $(T_{k'},\theta\circ\mathrm{Nm}_{k'/k}),(T'_{k'},\theta'\circ\mathrm{Nm}_{k'/k})$ are $G(k')$-conjugate for some finite extension $k'/\mathbb{F}_q$. ⌟

Prop. (18.6.4.7). If $(T,\theta),(T',\theta')$ are two induction pairs that are not geometrically conjugate, then $R_T^G(\theta), R_{T'}^G(\theta')$ are disjoint. ⌟

Proof: Cf.[D-L76]Cor6.3. □

Def. (18.6.4.8) [Dual Groups]. ⌟

Prop. (18.6.4.9). The geometric conjugacy classes of induction pairs of G corresponds to the geometric conjugacy classes of semisimple elements of G^*(18.6.4.8). ⌟

Proof: □

Def. (18.6.4.10) [Lustig Series]. Let S be a semisimple conjugacy class of G^*, the **Lustig series** $\mathcal{E}(G,S)$ is the set of irreducible representations of G occurring in $R_T^G(\theta)$ for any (T,θ) in the geometric conjugacy class corresponding to S via(18.6.4.9). By(18.6.4.7),

$$\mathrm{Irr}(G(\mathbb{F}_q)) = \coprod_{S\in G^*_{\text{ss-conj}}} \mathcal{E}(G,S).$$

$\mathcal{E}(G,(1))$ is called the set of **unipotent representations**, which are all the irreducible representations appearing in $R_T^G(\mathbb{1})$ for various T. ⌟

5 Howlett-Lehler Theory

This theory decomposes Deligne-Lustig inductions into irreducible components.

6 Character Sheaves(Lustig)

References are [Introduction to character sheaves, Lustig], [Algebraic And Geometric Methods In Representation Theory, Lustig, 2014].

Remark (18.6.6.1). Let (S,θ) be an induction pair(18.6.4.2), there is in fact an isomorphism

$$H^i_{\text{ét},c}(\widetilde{X}_S,\overline{\mathbb{Q}}_\ell) \cong H^i_{\text{ét},c}(X_S,\mathcal{F}_\theta) \in \mathrm{Rep}(G(\mathbb{F}_q))$$

where $\mathcal{F}_\theta$ is the ℓ-adic local system on X_S corresponding to the $S(\mathbb{F}_q)$-torsor and θ. Thus much of the Deligne-Lustig theory can be interpreted in the language of sheaves, called **character sheaves**. ⌟

7 Gelfand-Graev representations

8 Alvis-Curtis Duality

Cf.[Duality for representations of a reductive group over a finite field, I, II, Deligne-Lustig].

9 Deligne-Lustig Varieties

Prop. (18.6.9.1). Let ⌟

10 GL(n)

Notation (18.6.10.1). The notation is the same as in(18.11.0.1). ⌟

Principal Series Representations

Prop. (18.6.10.2). Let $(\pi, V) \in \mathrm{Rep}^{\mathrm{fd}}(GL(2,k))$, then

- if the representation (π_1, V) is defined by $\pi_1(g) = \pi(g^{-t})$, then $\pi_1 \cong \widehat{\pi}$.
- if $n = 2$ and (π, V) is irreducible, let ω be the central character of π. If (π_2, V) is defined by $\pi_2(g) = \omega(\deg g)^{-1}\pi(g)$, then $\pi_2 \cong \widehat{\pi}$.

⌟

Proof: The proof of(18.11.1.15) applies to this case, noticing a finite group is profinite hence locally profinite. □

Lemma (18.6.10.3). Let $\chi_1, \chi_2, \mu_1, \mu_2$ be characters of F^*, consider the principal representations $\mathcal{B}(\chi_1, \chi_2), \mathcal{B}(\mu_1, \mu_2)$ of $GL(2,k)$ defined in(18.11.4.6), then

$$\dim \mathrm{Hom}_{GL(2,k)}(\mathcal{B}(\chi_1, \chi_2), \mathcal{B}(\mu_1, \mu_2)) = \delta_{\chi_1,\mu_1}\delta_{\chi_2,\mu_2} + \delta_{\chi_1,\mu_2}\delta_{\chi_2,\mu_1}.$$

⌟

Proof: Let χ, μ be characters of $B(k)$ defined as in(18.11.4.6), then by**??**, the dimension is just the dimension of space of functions $\Delta : GL(2,k) \to \mathbb{C}$ that

$$\Delta(b_2 g b_1) = \mu(b_1)\Delta(g)\chi(b_1), \quad b_1, b_2 \in B(k).$$

Then by the Bruhat decomposition(12.11.5.5), Δ is determined by its values on 1 and w_0. Notice that if $\chi_1 \neq \mu_1$ or $\chi_2 \neq \mu_2$, we can use this condition to show $\Delta(1) = 0$, and if $\chi_1 \neq \mu_2$ or $\chi_2 \neq \mu_1$, we can use this condition to show $\Delta(w_0) = 0$, and also the construction of Δ is clear in other cases. □

Prop. (18.6.10.4) [Principal Series Representations]. Let $\chi_1, \chi_2, \mu_1, \mu_2$ be characters of F^*, then $\mathcal{B}(\chi_1, \chi_2)$ is an irreducible representation of degree $q = |F| + 1$ unless $\chi_1 = \chi_2$, in which case it is the direct sum of two irreducible representations having degree 1 and q. And $\mathcal{B}(\chi_1, \chi_2) \cong \mathcal{B}(\mu_1, \mu_2)$ iff $\{\chi_1, \chi_2\} = \{\mu_1, \mu_2\}$. ⌟

Proof: Use(18.6.10.3), then

$$\dim \mathrm{End}_{GL(2,k)}(\mathcal{B}(\chi_1, \chi_2)) = 1 + \delta_{\chi_1,\chi_2}.$$

Now by Peter-Weyl, if a representation V is isomorphic to $\sum d_i\pi_i$, where π_1 are irreducible, then $\dim_G(V) = \sum d_i^2$(11.10.4.5). Then we now $\mathcal{B}(\chi_1, \chi_2)$ decomposes into two representations if $\chi_1 = \chi_2$ and is irreducible if $\chi_1 \neq \chi_2$.

In case $\chi_1 = \chi_2$, there is an invariant subspace of dimension 1, generated by the function $f(g) = \chi(\deg g)$. so the rest representation is of dimension q, because $G(2,k)/B(k) = q + 1$. □

Def. (18.6.10.5) [Steinberg Representation]. We call the q-dimensional subrepresentation of $\mathcal{B}(1,1)$ the **Steinberg representation**. It is verified that the q dimensional subrepresentation of $\mathcal{B}(\chi, \chi)$ is the twist of the Steinberg representation. ⌟

Weil Representations

Prop. (18.6.10.6) [Weil Representation for $SL(2,k)$]. In situation (20.7.3.5), let $W = L^2(E)$, define the modified Fourier transform w.r.t. ψ as in (11.10.3.33):

$$\widehat{\Phi}(x) = q^{-1} \sum_{y \in E} \Phi(y)\psi(\mathrm{tr}(\overline{x}y)).$$

Then there is a **Weil representation** $\omega : SL(2,k) \to \mathrm{End}(W)$:

$$(\omega(t(a))\Phi)(x) = \Phi(ax), \quad w(n(z)\Phi)(x) = \psi(zN(x))\Phi(x), \quad (\omega(w_1)\Phi)(x) = \varepsilon\widehat{\Phi}(x).$$

where we are using the presentation as in 5, and $\varepsilon = 1$ is E/F is split, and -1 if it is anisotropic. ⌟

Remark (18.6.10.7). When F has characteristic $\neq 2$, this is just the Weil representation in (20.7.3.3). ⌟

Proof: This follows from direct verification, Cf.[Bump, P407]. □

Prop. (18.6.10.8) [Dihedral Weil Representations for $GL(2,k)$]. Situation as in (20.7.3.5), Define

$$W(\chi) = \{\Phi \in W | \Phi(yx) = \chi(y)^{-1}\Phi(x), y \in E_1^*\},$$

then by considering the order of E_1^*, $\dim W(\chi) = q + \varepsilon$. Also it is verified that $W(\chi)$ is stable under the Weil representation of $SL(2,k)$ (18.6.10.6).

Now we want to extend this representation to $GL(2,k)$ by defining

$$(\omega(\begin{bmatrix} a & \\ & 1 \end{bmatrix})\Phi)(x) = \chi(b)\Phi(bx)$$

where b is arbitrary that $N(b) = a$. ⌟

Remark (18.6.10.9). This is related to (20.7.3.7) and Howe duality. ⌟

Proof: It must be shown that this is truly a representation of $GL(2,k)$, it suffices to show that

$$\omega(\begin{bmatrix} a & \\ & 1 \end{bmatrix})\omega(g)\omega(\begin{bmatrix} a^{-1} & \\ & 1 \end{bmatrix}) = \omega(\begin{bmatrix} a & \\ & 1 \end{bmatrix} g \begin{bmatrix} a^{-1} & \\ & 1 \end{bmatrix}),$$

where g is a generator of $SL(2,k)$. This is clear for $g = t(a)$, and also clear for $g = n(z)$. For $g = w_1$, it suffices to check

$$\omega(\begin{bmatrix} a & \\ & 1 \end{bmatrix}) \circ \wedge \circ \omega(\begin{bmatrix} a^{-1} & \\ & 1 \end{bmatrix})\Phi(x) = \widehat{\Phi}(ax)$$

which is subtle but also clear. □

Prop. (18.6.10.10) [Split Weil Representation]. In the split case, the character χ of E^* is of the form $\chi((x,y)) = \chi_1(x)\chi_2(y)$, and then condition in (20.7.3.5) just says $\chi_1 \neq \chi_2$. Then:

$$(\pi(\chi), W(\chi)) \cong \mathcal{B}(\chi_2, \chi_1)$$

⌟

Proof: The intertwining operator is given by

$$L : W(\chi) \to \mathcal{B}(\chi_2, \chi_1) : (L\Phi)(g) = (\omega(g)\Phi)((1, 0)).$$

Firstly $L\Phi \in \mathcal{B}(\chi_2, \chi_1)$ by direct verification for $t(a), T_1(k)$ and $n(z)$. Then it is an intertwining operator is clear.

Then this is an isomorphism because both are of dimension $q + 1$(18.6.10.8) and $\mathcal{B}(\chi_2, \chi_1)$ is irreducible(18.6.10.4). □

Def. (18.6.10.11) [Cuspidal Representation]. $(\pi, V) \in \mathrm{Rep}^{\mathrm{fd}}(GL(2, k))$ is called a **cuspidal representation** if the Jacquet module $J(V) = 0$. Notice in this finite case, this is equivalent to V has no $N(k)$-fixed vector, because the contragradient is well-known as $\mathrm{Rep}(G)$ is semisimple, and the trivial isotropic parts correspond, unlike the p-adic case. ⌟

Lemma (18.6.10.12). If (π, V) is a cuspidal representation of $GL(2, k)$, then the dimension of V is a multiple of $q - 1$. ⌟

Proof: Because $N(k) \cong F$, any character of $N(k)$ is of the form $\psi_a(n(x)) = \psi(ax)$. Now decompose the contragradient representation V^* of G into isotypic parts of $N(k)$:$V^* = \oplus_{a\in F} V^*(a)$, then the hypothesis implies $V^*(0) = 0$.

Notice that the group $T_1(k)$ acts transitively on the spaces $V^*(a), a \neq 0$ by $\widehat{\pi}(\begin{bmatrix} t & \\ & 1 \end{bmatrix})l$, because

$$\begin{bmatrix} t & \\ & 1 \end{bmatrix} \begin{bmatrix} 1 & x/t \\ & 1 \end{bmatrix} = \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} \begin{bmatrix} t & \\ & 1 \end{bmatrix}.$$

So the dimension of V is a multiple of $q - 1$. □

Prop. (18.6.10.13) [Anisotropic Representation]. In the anisotropic case, the Weil representation $(\pi(\chi), W(\chi))$ is cuspidal and irreducible. ⌟

Proof: Suppose it is not cuspidal, then it contains a non-zero $N(k)$-fixed vector Φ_0(18.6.10.11), which means $\Phi_0(x) = w(n(z)\Phi_0)(x) = \psi(zN(x))\Phi(x)$. Now $\Phi_0(0) = 0$ because χ is nontrivial on E_1^*, and if $x \neq 0$, then there is a z that $\psi(zN(x)) \neq 1$ because ψ is non-trivial, so $\Phi_0(x) = 0$ also, so $\Phi_0 = 0$, contradiction.

Finally, subrepresentation of cuspidal representation is cuspidal by(18.6.10.11), then $(\pi(\chi), W(\chi))$ is irreducible, by the fact it is of dimension $q - 1$(18.6.10.8) and lemma(18.6.10.12). □

Prop. (18.6.10.14) [Classification of Representations of $GL(2, k)$]. There is a list of all irreducible representations of $GL(2, k)$:

- $q - 1$ 1-dimensional representations $\chi(\deg g)$, where χ is a character of $k^\times$.
- $\frac{(q-1)(q-2)}{2}$ principal series representations of dimension $q + 1$.
- $q - 1$ Steinberg representations(with twists) of dimension q.
- $\frac{q(q-1)}{2}$ cuspidal Weil representations of dimension $q - 1$.

⌟

Proof: All these are irreducible representations by(18.6.10.4)(18.6.10.5) and(18.6.10.13). It suffices to show they are not isomorphic. Notice different kind of representation have different dimensions, thus it suffices to compare the same representations.

For principal series representations $\mathcal{B}(\chi_1,\chi_2),\chi_1 \neq \chi_2$, their isomorphisms are known by(18.6.10.4). For Steinberg representations, twisting are clearly different. For cuspidal Weil representations, there are q^q-q way of choosing χ(20.7.3.5) and **?** Cf.[Local Langlands For GL(2)].

Finally, they are all the irreducible representations by the fact $\sum d_\sigma^2 = |G| = (q-1)^2 q(q+1)$(18.1.3.4). □

Whittaker Models

Def. (18.6.10.15) [Whittaker Functionals & Whittaker Models]. Let (π, V) be an irreducible representation of $GL(2,k)$, then the notion of **Whittaker functional** and **Whittaker model** is defined as in(18.11.3.1). ⌟

Prop. (18.6.10.16) [Existence and Uniqueness of Whittaker Models]. Let $\mathcal{G}$ be the representation of $GL(2,k)$ induced from the character $\psi_N(n(z)) = \psi(z)$ on $N(k)$, then it is multiplicity-free, and every irreducible representation of dimension> 1 occurs in it. Notice that this is just the existence and uniqueness of Whittaker models. ⌟

Proof: To show multiplicity free, it suffices to show $\mathrm{End}_{GL(2,k)}(\mathcal{G})$ is commutative, by Shur's lemma(11.10.2.4). Then we use**??**, which says this ring is isomorphic to the ring of functions Δ on G that

$$\Delta(n_2 g n_1) = \psi_N(n_2)\Delta(g)\psi_N(n_1).$$

where the multiplication is convolution**??**.

Notice it follows from the the Bruhat Decomposition(12.11.5.5) that the double coset $N(k)\backslash GL(2,k)/N(k)$ is uniquely represented by matrices with exactly two non-zero entries. Then it is clear a diagonal coset can support a function Δ iff it is a scalar multiple of I. In other words, the representatives are

$$\begin{bmatrix} a & \\ & a \end{bmatrix}, \quad \begin{bmatrix} & b \\ c & \end{bmatrix}.$$

Consider the involution of G given by

$$\iota(g) = w_1 g^t w_1^{-1},$$

then it is an anti-involution of G and it induces isomorphism on $N(k)$, so it induces an anti-involution of order two on the ring of functions Δ by $\iota(\Delta)(g) = \Delta(\iota(g))$. Notice this is an anti-involution because of(11.10.1.27) and the fact a finite group is unimodular. But this anti-involution fixes the representatives as above, so it is in fact identity on these Δ, which proves the convolution is commutative.

For the last assertion, just notice the dimension of $\mathcal{G}$ is $(q-1)(q^2-1)$, and the sum dimensions of irreducible representations of dimension> 1 is just $(q-1)(q^2-1)$ by(18.6.10.14). □

Cor. (18.6.10.17). Frobenius reciprocity(11.10.5.5) implies that the space of Whittaker functionals is of dimension 1 for any irreducible representation of dimension> 1. ⌟

11 SL(n)

Def. (18.6.11.1) [Drinfeld Curves]. The **Drinfeld curve** is defined to be the affine plane curve $\mathrm{Dri}/\mathbb{A}_q^2$

$$\mathrm{Dri} : x^q y - x y^q = 1$$

with completion $\overline{\mathrm{Dri}} = \mathrm{Dri} \cup \{\infty\} \subset \mathbb{P}_q^2$. ⌟

Prop. (18.6.11.2). There is a natural $\mu_{q+1} \times SL(2,\mathbb{F}_q)$-action on Dri, which induces a map on $H^*_{\text{ét},c}(\text{Dri},\mathbb{Q}_\ell)$. Then we get the Deligne-Lustig induction

$$R^G_{T'} : \mu^*_{q+1} \to K_0(\text{Rep}^{\text{fd}}(SL(2,\mathbb{F}_q)).$$

⌟

Proof: □

Reps\Classes	$\begin{bmatrix}1 & \\ & 1\end{bmatrix}$	$\begin{bmatrix}-1 & \\ & -1\end{bmatrix}$	$\begin{bmatrix} & -1\\ 1 & \end{bmatrix}$	$\begin{bmatrix}1 & 1\\ & 1\end{bmatrix}$	$\begin{bmatrix}1 & -1\\ & 1\end{bmatrix}$	$\begin{bmatrix}-1 & 1\\ & -1\end{bmatrix}$	$\begin{bmatrix}-1 & -1\\ & -1\end{bmatrix}$
size	1	1	6	4	4	4	4
1	1	1	1	1	1	1	1
χ	1	1	1	ω	ω^2	ω^2	ω
χ^2	1	1	1	ω^2	ω	ω	ω^2
ρ rational quaternionic	2	-2	0	-1	-1	1	1
$\chi\rho$	2	-2	0	$-\omega$	$-\omega^2$	ω^2	ω
$\chi^2\rho$	2	-2	0	$-\omega^2$	$-\omega$	ω	ω^2
π	3	3	-1	0	0	0	0

Figure (18.6.11.1): Character Table of $SL(2,\mathbb{F}_3)$

12 GL(n)

References are [Representations of the Finite Classical Groups, Zelevinsky, 1981].

Thm. (18.6.12.1) [Irreducible Characters of $GL(n,\mathbb{F}_q)$, Green]. ⌟

13 Sp$_{2n}$

Thm. (18.6.13.1) [Irreducible Characters of $Sp(2n,\mathbb{F}_q)$, Green]. ⌟

18.7 Bruhat-Tits Theory

1 Buildings

Main references are [Serre, Trees].

2 Bruhat-Tits Buildings

Main references are [Reductive Groups over Local Fields, Tits] and [A Compatification of the Bruhat-Tits Building], [the Bruhat-Tits Buildings of a p-adic Chevalley Group and an Application to Representation Theory, Rabinoff].

Def. (18.7.2.1)[Bruhat-Tits Buildings]. For a Chevalley group $G = G(F)$, the **Bruhat-Tits building** $\mathcal{B}(G)$ is a building that

- vertices of $\mathcal{B}(G)$ corresponds to the set of compact open subgroups of G.
- $\mathcal{B}(G)$ is a union of subcomplexes called **apartments**, corresponding to the set of split maximal tori T of G.
-

⌟

Prop. (18.7.2.2)[$\mathcal{B}(SL(2,\mathbb{Q}_p))$]. The Bruhat-Tits building $\mathcal{B}(SL(2,\mathbb{Q}_p))$ is a $(p+1)$-regular tree where

- vertices of $\mathcal{B}(SL(2,\mathbb{Q}_p))$ corresponds to homothety classes of lattices $[\Lambda]$ in $\mathbb{Q}_p^2$.
- edges of $\mathcal{B}(SL(2,\mathbb{Q}_p))$ corresponds to adjacent pairs of lattices in $\mathbb{Q}_p^2$.

⌟

3 Compactifications

18.8 Representations of Semisimple Lie Algebras and Category $\mathcal{O}$

Main references are[Eti21] and[Car05].

This section studies representations of split semisimple Lie algebras. For a split semisimple Lie algebra $(\mathfrak{g},\mathfrak{h})$, we use notations as in(3.7.3.30).

1 Semisimple Representations

Lemma (18.8.1.1). If $\mathfrak{g}$ is a semisimple Lie algebra over k, then every 1-dimensional representation of $\mathfrak{g}$ is trivial. ⌟

Proof: Such a representation vanishes at $[\mathfrak{g},\mathfrak{g}]$, which equals $\mathfrak{g}$ by(3.7.2.4). □

Prop. (18.8.1.2) [Weyl]. For a Lie algebra $\mathfrak{g}$ over a field k,

- If the adjoint representation $\mathfrak{g}\to\mathfrak{gl}_{\mathfrak{g}}$ is semisimple, then $\mathfrak{g}$ is semisimple.
- If $\mathfrak{g}$ is semisimple and k has characteristic 0, then $\mathrm{Rep}(\mathfrak{g})$ is semisimple.

⌟

Proof: If the adjoint representation of $\mathfrak{g}$ is semisimple, then every ideal of $\mathfrak{g}$ has a complement, thus if $\mathfrak{g}$ is not semisimple, it has a dimension 1 quotient. But notice the Lie algebra k of dimension 1 has non-semisimple representations, for example $c\mapsto\begin{bmatrix}0&0\\c&0\end{bmatrix}$, contradiction.

Semisimplicity of a Lie algebra is invariant under base change, also does simplicity of the category of representations(18.8.1.4), so we can assume that k is alg.closed. Now we need to show that any proper submodule W of a $\mathfrak{g}$-module V has a complement.

Assume first that $\dim V/W=1$ and W is a simple $\mathfrak{g}$-module. This implies $\mathfrak{g}$ acts trivially on V/W by(18.8.1.1). Let c_V be the Casimir element of V(3.7.9.11), then c_V is also trivial on V/W. And c_V acts as a nonzero scalar on W as W is simple, by(3.7.9.11). Then the kernel of c_V is of 1-dimensional, and is a $\mathfrak{g}$-complement of W in V.

Next if $\dim V/W=1$ but W is not simple $\mathfrak{g}$-module, then there is a submodule $W'\subset W$. By induction, the $\mathfrak{g}$-submodule W/W' has a complement V'/W' in V/W'. Then V'/W' has dimension 1, thus by induction, $V'=W'\oplus L$ for some 1-dimensional $\mathfrak{g}$-module. Then L is complementary to W in V.

Finally for the general case, let $\mathfrak{g}$ acts on $\mathrm{Hom}_k(V,W)$, consider the subspaces V_1,W_1 of $\mathrm{Hom}_k(V,W)$, where V_1 is the subspace of maps that restriction to W is a constant multiple of identity, and W_1 is the subspaces of W consisting of maps vanishing on W. They are both $\mathfrak{g}$-modules and $\dim V_1/W_1=1$. Then the above case shows $V_1=W_1\oplus L$ for some 1-dimensional $\mathfrak{g}$-module L. Because $\mathfrak{g}$ acts trivially on L(18.8.1.1), this means $L=\mathbb{F}f$ consists of $\mathfrak{g}$-homomorphisms. But $f|_W$ is non-zero constant, so the kernel of f is a complement of W in V. □

Cor. (18.8.1.3). Let (V,ρ) be a representation of a semisimple Lie algebra $\mathfrak{g}$ and $f:\mathfrak{g}\to V$ a linear map that

$$f([x,y])=\rho(x)f(y)-\rho(y)f(x),$$

then there exists a $v_0\in V$ that $f(x)=\rho(x)v_0$. ⌟

Proof: The condition on f is equivalent to $(f,\rho):\mathfrak{g}\to\mathfrak{af}(V)$(3.7.1.11) is a homomorphism of Lie algebras. And this induces a representation ρ' of $\mathfrak{g}$ on $V'=V\oplus k$ that $\rho'(x)(V')\subset V$ for all $x\in\mathfrak{g}$. Because $\mathfrak{g}$ is semisimple, there is a line $L\subset V'$ that $V'=V\oplus L$ and $\mathfrak{g}$ acts trivially on L(18.8.1.1).

In other words, there is a vector $(-v_0, 1)$ that $\rho'(x)(-v_0, 1) = 0$ for all $x \in \mathfrak{g}$. So $f(x) = \rho(x)(v_0)$ for all x. So we are done. □

Prop. (18.8.1.4) [Semisimplicity and Extension]. Let $\mathfrak{g}$ be a Lie algebra over a field k. If $\mathrm{Rep}(\mathfrak{g}_K)$ is semisimple for some extension field K/k, then also is $\mathrm{Rep}(\mathfrak{g})$. ⌟

Proof: This is because for any representation (V, ρ) of $\mathfrak{g}$, $K \otimes_k \mathrm{End}(\rho) \cong \mathrm{End}(\rho_K)$, because this is true for $\mathrm{End}(V)$, and being $\mathfrak{g}$-equivariant is a linear condition. Then we can use(3.6.1.25) and(3.6.1.26). □

Prop. (18.8.1.5) [Semisimple Representations]. The following conditions on a representation $\mathfrak{g} \to \mathfrak{gl}_V$ are equivalent:

- ρ is semisimple.
- $\rho(\mathfrak{g})$ is reductive and its center consists of semisimple endomorphisms.
- $\rho(\mathfrak{r})$ consists of semisimple endomorphisms.
- The restriction of ρ to $\mathfrak{r}$ is semisimple.

⌟

Proof: $1 \to 2$: If ρ is semisimple, then $\rho(\mathfrak{g})$ is reductive by(3.7.4.4). Its center consists of semisimple endomorphisms by [Mil13]P60**?**.

$2 \to 3$: This is because if $\rho(\mathfrak{g})$ is reductive, then its center equals its radical and contains $\rho(\mathfrak{r})$, so $\rho(\mathfrak{r})$ consists of semisimple endomorphisms.

$3 \to 4$: [Mil13]P60**?**.

$4 \to 1$: [Mil13]P60**?**. □

Cor. (18.8.1.6). Let ρ and ρ' be representations of $\mathfrak{g}$. If ρ and ρ' are semisimple, then so are $\rho \otimes \rho'$ and $\rho^\vee$.

In particular, the category $\mathrm{Rep}^{ss}(\mathfrak{g})$ of semisimple representations of a Lie algebra $\mathfrak{g}$ form a Tannakian category, thus there is an algebraic group G that $\mathrm{Rep}^{ss}(\mathfrak{g}) = \mathrm{Rep}(G)$. ⌟

Proof: Use the third criterion, for any $x \in \mathfrak{r}$, as $\rho(x), \rho'(x)$ are semisimple, so is $\rho(x) \otimes \rho'(x)$, so $\rho \otimes \rho'$ is also semisimple by(18.8.1.5). □

representations of $\mathfrak{sl}_2(\mathbb{C})$

Def. (18.8.1.7) [Primitive Element]. Let V be a $\mathfrak{sl}_2$-module, an element $v \in V$ is called **primitive of weight** λ if it is non-zero and $Xe = 0, He = \lambda e$. ⌟

Prop. (18.8.1.8). Every non-zero f.d. $\mathfrak{sl}_2$-module contains a primitive element. ⌟

Proof: en element e is primitive iff the line generated by e is stable under the action of $\{X, H\}$: if $Xe = \lambda e$ and $He = \mu e$, then using the $[H, X] = 2X$, we see that $2\lambda 0$, thus $\lambda = 0$, and e is primitive. So each f.d. $\mathfrak{sl}_2$-module contains a primitive element, by Lie's theorem(3.7.1.24). □

Prop. (18.8.1.9) [Submodule Generated by Primitive Element]. Let V be a $\mathfrak{sl}_2$-module and $e \in V$ a primitive element of weight λ. Let $e_n = Y^n e/n!$, and $e_{-1} = 0$, then we have

$$He_n = (\lambda - 2n)e_n, \quad Ye_n = (n+1)e_{n+1}, \quad Xe_n = (\lambda - n + 1)e_{n-1}.$$

⌟

Proof: By induction on n,

$$HY^n e = ([H,Y]+YH)Y^{n-1}e = (\lambda-2(n-1)-2)Y^n e = (\lambda-2n)e.$$

$Ye_n = (n+1)e_{n+1}$ is obvious.

And

$$\begin{aligned} nXe_n &= XYe_{n-1} = [X,Y]e_{n-1} + YXe_{n-1} \\ &= He_{n-1} + (\lambda-n+2)Ye_{n-2} \\ &= (\lambda-2n+2+(\lambda-n+2)(n-1))e_{n-1} \\ &= n(\lambda-n+1)e_{n-1} \end{aligned}$$

□

Cor. (18.8.1.10). Only two cases arise: either

- The elements $\{e_n\}$ are linearly independent.
- The elements $e_0, e_1, \ldots, e_m$ are linearly independent, and $e_{m+1} = e_{m+2} = \ldots = 0$, and weight λ of e equals m.

And if V is f.d., then case 1 cannot happen, and the subspace W generated by $e_0, \ldots, e_m$ is a $\mathfrak{g}$-module and it is irreducible. ⌟

Proof: Because each e_i has different eigenvalue under action of H, thus if they are all nonzero, then they are linearly independent. If $e_0, e_1, \ldots, e_m$ are linearly independent, and $e_{m+1} = e_{m+2} = \ldots = 0$, then by the proposition,

$$Xe_{m+1} = (\lambda - m)e_m$$

and $e_{m+1} = 0$ with $e_m \neq 0$, thus $\lambda = m$. Now the formulas in(18.8.1.9) shows that W is a $\mathfrak{g}$-module. And if $W' \subset W$ is a subspace invariant under $\mathfrak{g}$, then it contains some eigenvalues e_k of H, and then the formulas in(18.8.1.9) shows it contains all $e_0, e_1, \ldots, e_m$, thus $W' = W$. Thus W is irreducible. □

Prop. (18.8.1.11) [Irreducible Representations of $\mathfrak{sl}_2(\mathbb{C})$]. Let $W_m = \{e_0, \ldots, e_m\}$ be a $m+1$-dimensional vector space and $\mathfrak{sl}_2$ acts on W_m by

$$He_n = (m-2n)e_n, \quad Ye_n = (n+1)e_{n+1}, \quad Xe_n = (m-n+1)e_{n-1}.$$

Then W_n is a f.d. irreducible representation of $\mathfrak{sl}_2$, and any f.d representation of $\mathfrak{sl}_2$ of dimension $m+1$ is isomorphic to one of W_m. ⌟

Proof: The first assertion follows from(18.8.1.10) and the fact e_0 is a primitive element. For the second assertion, notice any f.d. representation W of $\mathfrak{g}$ contains a primitive element(18.8.1.8) thus by(18.8.1.10) generates an irreducible $\mathfrak{sl}_2$-submodule W_n, thus this submodule equals W, and $n+1 = m+1$, thus $n = m$. □

Remark (18.8.1.12). Notice this is special case of(18.8.2.15). ⌟

Cor. (18.8.1.13). W_0 is the just trivial action of $\mathfrak{sl}_2$, W_1 is isomorphic to the natural action of $\mathfrak{sl}_2$ on $\mathbb{C}^2$, and W_2 is isomorphic to the adjoint action of $\mathfrak{sl}_2$ on itself. ⌟

Proof: In fact, W_1 can be identified with the vector space $\mathbb{C}\{x,y\}$ where

$$Hx = x, Hy = -y, Yx = y, Yy = 0, Xy = x, Xx = 0.$$

Then the m-th symmetric tensor of W_1 is isomorphic to the vector space of polynomials in x, y of degree m, and by(3.7.9.2),

$$H(C_m^k y^k x^{m-k}) = (m-2k)(C_m^k y^k x^{m-k}),$$

$$Y(C_m^k y^k x^{m-k}) = (k+1)(C_m^{k+1} y^{k+1} x^{m-k-1}),$$
$$X(C_m^k y^k x^{m-k}) = (m-k+1)(C_m^{k-1} y^{k-1} x^{m-k+1}).$$

So it is isomorphic to W_{m+1}. □

Cor. (18.8.1.14) [Representations of $\mathfrak{sl}_2(\mathbb{K})$]. Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$,

- Any f.d. representation V of $\mathfrak{sl}_2(\mathbb{K})$ is isomorphic to a direct sum of W_ms, and Thus
- The endomorphism on V induced by H is diagonalizable and with integral eigenvalues. if $\pm n$ are eigenvalues of H, then so are $n-2, n-4, \ldots, 4-n, 2-n$.
- For any $n \geq 0$, the linear maps

  $$Y^n : V^n \to V^{-n}, X^n : V^{-n} \to V^n$$

  are isomorphisms. In particular, V^{-n} and V^n have the same dimensions.

⌟

Proof: by Weyl's theorem(18.8.1.2), any representation of $\mathfrak{sl}_2(\mathbb{K})$ is isomorphic to a direct sum of irreducible representations, and the irreducible representations of $\mathfrak{sl}_2(\mathbb{C})$ clearly comes from real representations of $\mathfrak{sl}_2(\mathbb{R})$, thus irreducible representations of $\mathfrak{sl}_2(\mathbb{R})$ must be of the same form(otherwise tensor with $\mathbb{C}$ and decompose, and use conjugation).

Because we can assume V is one of W_m, so the other assertions are clear. □

2 Verma Modules

Def. (18.8.2.1) [Weights]. Let $(\mathfrak{g}, \mathfrak{h})$ be a semisimple Lie algebra with root system R and V is a $\mathfrak{g}$-module. If $\lambda \in \mathfrak{h}^*$, a vector $v \in V$ is said to have weight λ iff $hv = \lambda(h)v$ for any $h \in \mathfrak{h}$. The space of vectors in V of weight λ is denoted by $V[\lambda]$. An **integral weight** is a weight λ of the form $\lambda = \sum n_i \alpha_i^\vee$, where $\alpha_i \in R$, equivalently its values on h_i are all integers.

V is said to have a **weight decomposition** if $V = \oplus_{\lambda \in \mathfrak{h}^*} V[\lambda]$. ⌟

Prop. (18.8.2.2). Any f.d. $\mathfrak{g}$-module V has a weight decomposition, and the weights are all integral. ⌟

Proof: For any i, V is a $\mathfrak{s}_i = \{e_i, h_i, f_i\}$-module(3.7.3.20), so by the representation theory of $\mathfrak{sl}_2$, h_i acts semisimply on V, and the eigenvalues are integers. Thus $\mathfrak{h}$ acts semisimply on V, thus there is a weight decomposition, and the weights are all integral. □

Def. (18.8.2.3) [Highest Weight Representations]. A vector $v \in V$ is called a **highest weight vector** if it is a weight vector and $\mathfrak{n}_+ v = 0$, or equivalently $e_i v = 0$ for any e_i. A **highest weight representation** with highest weight λ is a representation that is generated by a highest weight vector of weight λ. ⌟

Prop. (18.8.2.4). Any f.d. $\mathfrak{g}$-module contains a highest weight vector, thus any irreducible f.d $\mathfrak{g}$-representation is a highest weight representation. ⌟

Proof: Let $P = \sum_i \alpha_i^\vee$, and choose a weight λ that (λ, P) is maximal, then $e_i v$ has weight $\lambda + \alpha_i$, thus $e_i v = 0$ for any i. □

Verma Modules

Def. (18.8.2.5) [Verma Modules]. Let $\lambda \in \mathfrak{h}^*$, $I_\lambda \subset U(\mathfrak{g})$ be the left ideal generated by the elements $h - \lambda(h)$ and e_i, then the **Verma module** $M_\lambda = U(\mathfrak{g})/I_\lambda$. has a weight decomposition, and it is a highest weight representation with highest vector $v_\lambda = \overline{1}$ with weight λ. ⌟

Prop. (18.8.2.6) [M_λ is Noetherian]. M_λ satisfies ascending chain condition on f.d. submodules. ⌟

Proof: This is because $U(\mathfrak{g})$ is left Noetherian(3.7.8.16) and $M_\lambda = U(\mathfrak{g})/I_\lambda$. □

Prop. (18.8.2.7). The map $\varphi : U(\mathfrak{n}_-) \to W_\lambda : \varphi(x) = xv_\lambda$ is an isomorphism of left $U(\mathfrak{n}_-)$-modules. ⌟

Proof: This follows from PBW theorem. □

Cor. (18.8.2.8). M_λ has a weight decomposition with $P(M_\lambda) = \lambda - Q^+$, and weight spaces of M_λ are all of f.d.. ⌟

Prop. (18.8.2.9). If V is a $\mathfrak{g}$-module and $v \in V$ is a highest weight vector, then there is a unique homomorphism $M_\lambda \to V$ of $\mathfrak{g}$-modules that maps v_λ to v. ⌟

Cor. (18.8.2.10). Every highest weight representation has a decomposition into f.d. weight spaces. And they have a unique highest weight vector up to a scalar. ⌟

Prop. (18.8.2.11) [Quotient of Verma Modules]. M_λ has a unique irreducible quotient L_λ. In particular, L_λ is a quotient of every highest weight representation of $\mathfrak{g}$ with weight λ, by(18.8.2.9). ⌟

Proof: As M_λ has a weight decomposition, any submodule Y of M_λ has a weight decomposition, and cannot has weight λ, otherwise it generates M_λ by(18.8.2.10). Then the sum J_λ of all proper submodules of M_λ also cannot have weight λ, thus also proper. Then $L_\lambda = M_\lambda/J_\lambda$ is the unique irreducible quotient of M_λ. □

Cor. (18.8.2.12) [Classification of Irreducible Highest Weight Representations]. Any irreducible highest weight representation of $\mathfrak{g}$ is of the form L_λ where $\lambda \in \mathfrak{h}^*$. ⌟

Prop. (18.8.2.13) [Composition Factors of Verma Modules]. The Verma module M_λ has a finite composition series $M_\lambda = N_0 \supset N_1 \supset \ldots \supset N_r = 0$ that each N_i/N_{i+1} is irreducible and isomorphic to $L_{\omega(\lambda+\rho)-\rho}$ for some $\omega \in W$. ⌟

Proof: We can find a(not necessarily finite) series of submodules of M_λ that the subquotients are irreducible as M_λ satisfies ascending chain condition on submodules(18.8.2.6). □

Lemma (18.8.2.14). Let V be a $\mathfrak{g}$-module with weight decomposition into f.d. weight spaces. If V is a sum of f.d. $\mathfrak{s}_i$-modules for each i, then for each $\lambda \in P$ and $w \in W$, $\dim V[\lambda] = \dim V[w\lambda]$. ⌟

Proof: As W is generated by s_i, it suffices to prove for $w = s_i$, $\dim V[\lambda] = \dim V[w\lambda]$.

If $(\lambda, \alpha_i^\vee) = m \geq 0$ for some i, consider the operator $f_i^m : V[\lambda] \to V[s_i\lambda]$ is an isomorphism by hypothesis and the representation theory of $\mathfrak{sl}_2$. Similarly, if $(\lambda, \alpha_i^\vee) = -m \leq 0$, then $e_i^m : V[\lambda] \to V[s_i\lambda]$ is an isomorphism. □

Prop. (18.8.2.15) [Classification of F.D. Irreducible Representations]. F.d. irreducible representations of $\mathfrak{g}$ are classified by their highest dominant integral weights $\lambda \in P^+$ via the bijection $\lambda \mapsto L_\lambda$. Moreover, for any $\mu \in P$ and $w \in W$, $\dim L_\lambda[\mu] = \dim L_\lambda[w\mu]$. ⌟

Proof: Firstly if V is a f.d. $\mathfrak{g}$-module, then $\lambda \in P^+$ by(18.8.2.2). Now if $\lambda \in P^+$, then in L_λ, $f_i^{\lambda(h_i)+1} v_\lambda = 0$ for any i, because by(18.8.1.9), $e_i f_i^{\lambda(h_i)+1} v_\lambda = 0$, and $e_j f_i^{\lambda(h_i)+1} v_\lambda = 0$ for $j \neq i$ as v_λ is a highest weight vector. So $f_i^{\lambda(h_i)+1} v_\lambda$ generates a proper submodule of L_λ, which must be 0 as it cannot contain v_λ, and L_λ is irreducible.

Thus v_λ generate the $\mathfrak{s}_i$-module of highest weight $\lambda(h_i)$, and any element of $\mathfrak{g}$ generate a f.d. $\mathfrak{s}_i$-module, so V is a sum of f.d. $\mathfrak{s}_i$-modules for each i, thus by lemma(18.8.2.14), $\dim L_\lambda[\mu] = \dim L_\lambda[w\mu]$. To show L_λ is of f.d., first notice $P(L_\lambda) \cap P^+$ is finite, and $WP^+ = P$(3.9.2.16), and the fact $P(L_\lambda)$ is W-invariant. □

Prop. (18.8.2.16). $L_\lambda^* = L_{-w_0\lambda}$. ⌟

Proof: It suffices to show the lowest weight of L_λ is $w_0\lambda$: $w_0\lambda$ is a weight by(18.8.2.15), and if $\lambda' < w_0\lambda$, then $w_0\lambda' > \lambda$. □

Lemma (18.8.2.17). The representation L_n of $\mathfrak{sl}_2$ is of real type if n is even and of quaternion type if n is odd. ⌟

Proof: $L_n = \mathrm{Sym}^n L_1$, thus we can take the bilinear form $\mathrm{Sym}^n B$, where B is the alternating form on $L_1 \cong \mathbb{C}^2$, which is symmetric if n is even and alternating if n is odd. □

Prop. (18.8.2.18) [Type of Irreducible Representations]. Let $\lambda \in P^+$ that $\lambda = -w_0\lambda$, so L_λ is self-dual by(18.8.2.16), and it is of real type if $n = (2\rho^\vee, \lambda)$ is even and of quaternion type if $(2\rho^\vee, \lambda)$ is odd. ⌟

Proof: The number n is the eigenvalue of h on v_λ, where $\{h, e, f\}$ is the principal $\mathfrak{sl}_2$-subalgebra, and the other eigenvalues are all smaller. Then $L_\lambda \cong L_n \oplus \bigoplus_{-i<n} L_{m_i}$, so the invariant form on L_λ restricts to a non-zero invariant form on L_n, so the assertion follows from(18.8.2.17). □

Fundamental Representations

Prop. (18.8.2.19) [Fundamental Representations]. The following are equivalent for a dominant integral weight ω of a split semisimple Lie algebra $\mathfrak{g}$:

- ω is minuscule(3.9.3.15).
- All weights of the representation L_ω belongs to the orbit $W\omega$.
- The restriction of L_ω to $\mathfrak{s}_i$ is a direct sum of 1-dimensional and 2-dimensional subrepresentations.

Such a representation L_ω is called a **fundamental representation** of $\mathfrak{g}$. ⌟

Proof: $1 \to 2$: By(18.8.2.15), for any weight μ of L_ω, there is a $w \in W$ that $w\mu$ is dominant and $\omega - w\mu \in Q^+$. Thus $w\mu = \omega$ by(3.9.3.17), and $\mu \in W\omega$.

$2 \to 1$: If ω is not minuscule, then there is some positive α that $(\omega, \alpha^\vee) > 1$, so $2(\omega, \alpha) < (\alpha, \alpha)$, and $\omega - \alpha$ is a weight of L_ω(the weight of $f_\alpha v_\omega$, and it is not conjugate to ω, as $(\omega-\alpha, \omega-\alpha) = (\omega,\omega) - 2(\alpha,\omega) + (\alpha,\alpha) < (\omega,\omega)$.

$2 \iff 3$: If ω is minuscule and $v \in L_\omega$ be a highest weight vector for $\mathfrak{s}_i$, then $h_{\alpha_i} v = \omega(h_\alpha) = (\omega, \alpha^\vee) = 0$ or v(3.7.3.21). Thus we get 4 by the representation theory of $\mathfrak{sl}_2$. The reverse argument is also true. □

Cor. (18.8.2.20). The character for a fundamental representation L_ω is

$$\chi_\omega = \sum_{w \in W} e^{w\omega}.$$

⌟

Prop. (18.8.2.21). Let ω be a minuscule weight, then for any dominant integral weight λ,

$$L_\omega \otimes L_\lambda \cong \oplus_{w \in W, \lambda + w\omega \in P^+} L_{\lambda + w\omega}.$$

⌟

Proof: By Weyl's character formula and(18.8.2.20),

$$\chi_{L_\omega \otimes L_\lambda} = \frac{\sum_{\mu \in W\omega} \sum_{w \in W} \varepsilon(w) e^{w(\lambda+\rho)+\mu}}{\Delta} = \frac{\sum_{\gamma \in W\omega} \sum_{w \in W} \varepsilon(w) e^{w(\lambda+\rho+\gamma)}}{\Delta}$$

If $\lambda+\gamma \notin P^+$, then $(\lambda+\gamma, \alpha_i^\vee) < 0$ for some i. But $(\gamma, \alpha_i^\vee) \geq -1$ as ω is minuscule, so $(\lambda+\gamma, \alpha_i^\vee) = -1$, and $(\lambda+\gamma+\rho, \alpha_i^\vee) = 0$. Then for such γ, in the summand the w term cancels with ws_i term. Thus the summand equals the character for $\sum_{w \in W} e^{w\omega}$. Then we finish by(18.8.3.3). □

Prop. (18.8.2.22) [Fundamental Representations for Simple Lie Algebras]. By(3.9.3.20),

- for B_n, the fundamental representation corresponding to the minuscule weights ω_n is called the **Spin representation**, denoted by S.
- for C_n, the fundamental representation corresponding to the minuscule weights ω_1 is the standard representation of $\mathfrak{sp}_{2n}$.
- for D_n, the fundamental representation corresponding to the minuscule weights $\omega_1, \omega_{n-1}, \omega_n$ are the standard representation and two Spin representations S^+, S^-.
- for E_7, the unique fundamental representation has dimension 56**?**.
- for E_6, the two fundamental representations are dual, and have dimensions 27**?**.

⌟

Prop. (18.8.2.23) [Bott Periodicity for Spin Representations]. Let $\mathfrak{g} = \mathfrak{so}_m$, then the behavior of the spin representation of $\mathfrak{g}$ is

- S is of real type if $m \equiv 1, 7 \mod 8$.
- S is of quaternionic type if $m \equiv 3, 5 \mod 8$.
- S_+, S_- are of real type if $m \equiv 0 \mod 8$.
- $S_+^* \cong S_-$ are of complex type if $m \equiv 2, 6 \mod 8$.
- S_+, S_- are of quaternionic type if $m \equiv 4 \mod 8$.

⌟

Proof: We use(18.8.2.18). If $\mathfrak{g} = \mathfrak{so}_{2n}$, then $\rho^\vee = \rho = sum\omega_i = (n-1, n-2, \ldots, 1, 0)$, so $(2\rho^\vee, \omega_{n-1}) = (2\rho^\vee, \omega_n) = \frac{n(n-1)}{2}$.

If $\mathfrak{g} = \mathfrak{so}_{2n+1}$, then it can be verified that $\rho^\vee = (n, n-1, \ldots, 0)$, so $(2\rho^\vee, \omega_n) = \frac{n(n+1)}{2}$.

Also we need to consider w_0, so $\mathfrak{so}_{4n+2}$ are of complex type. □

3 Weyl Character Formula

Def. (18.8.3.1) [Central Characters of a Representation]. Let $V = \oplus_{\mu\in P} V[\mu]$ be a f.d. representation of a split semisimple Lie algebra $\mathfrak{g}$, the **central character** is an analytic function on $\mathfrak{h}$ that

$$\chi_V(h) = \sum_{\mu\in P} \dim V[\mu] e^{\mu(h)}.$$

In fact χ is an element in $\mathbb{Z}[e^{\alpha_1}, \ldots, e^{\alpha_r}, e^{-\alpha_1}, \ldots, e^{-\alpha_r}]$. ⌟

Thm. (18.8.3.2) [Weyl Characteristic Formula, Weyl1925]. Let $\lambda \in P^+$, then the character $\chi_\lambda = \chi_{L_\lambda}$ of the f.d. irreducible representation L_λ of $\mathfrak{g}$(18.8.2.15) is given by

$$\chi_\lambda = \frac{\sum_{w\in W} \varepsilon(w) e^{w(\lambda+\rho)}}{\Delta}.$$

where Δ is the Weyl denominator(18.8.4.3). ⌟

Proof: We already know that $\Delta\chi_\lambda \sum_{\mu\in P} c_\mu e^\mu$ is W-anti-invariant, $c_{\lambda+\rho} = 1$, and $c_\mu = 0$ unless $\mu \in \lambda + \rho - Q^+$, so it suffices to show $c_\mu = 0$ if $\mu \in P^+ \cap (\lambda + \rho - Q^+)$ and $\mu \neq \lambda + \rho$.? □

Cor. (18.8.3.3) [Characters Determine Representations]. F.d. representations of a semisimple Lie algebra is determined by its characters, as the maximal exponent of χ_λ are different for different λ. ⌟

Cor. (18.8.3.4). For $\mathfrak{sl}_2(\mathbb{C})$, $\chi_{W_n}(z) = e^{nz} + e^{(n-2)z} + \ldots + e^{-nz} = \frac{e^{(n+1)z} - e^{-(n+1)z}}{e^z - e^{-z}}$. Notice these functions are linearly independent, so by(18.8.1.14), representations of $\mathfrak{sl}_2(\mathbb{C})$ are determined by their characters. ⌟

Cor. (18.8.3.5) [Weyl Denominator Formula].

$$\Delta = \sum_{w\in W} \varepsilon(w) e^{w\rho}.$$

⌟

Proof: This follows from the Weyl character formula by setting $\lambda = 0$. □

Prop. (18.8.3.6) [Kostant's Multiplicity Theorem]. Let $\mathfrak{g}$ be a split semisimple Lie algebra and $\lambda \in P^+$, then

$$\dim L_\lambda[\gamma] = \sum_{w\in W} \varepsilon(w) \mathfrak{P}(w(\lambda+\rho) - \rho - \gamma).$$

where $\mathfrak{P}$ is the Kostant's partition function(3.9.2.19). ⌟

Proof: This follows from the formula

$$\Delta^{-1}=e^{-\rho}\frac{1}{\prod_{\alpha\in R^+}(1-e^{-\alpha})}=e^{-\rho}\sum_{\alpha\in Q(R)}\mathfrak{P}(\alpha)e^{-\alpha}.$$

applied to Weyl's character formula(18.8.3.2). □

Prop. (18.8.3.7) [Steinberg's Multiplicity Formula]. Let $\lambda,\mu\in P^+$, then

$$L_\lambda\otimes L_\mu\cong\sum_{\nu\in P^+}c_{\lambda\mu\nu}L_\nu,$$

where

$$c_{\lambda\mu\nu}=\sum_{w,w'\in W}\varepsilon(w)\varepsilon(w')\mathfrak{P}(w(\lambda+\rho)+w'(\mu+\rho)-(\nu+2\rho)).$$

where $\mathfrak{P}$ is the Kostant's partition function(3.9.2.19). ⌟

Proof: Cf.[Cartar, P265]. □

Cor. (18.8.3.8) [Clebsch-Gordan Rule]. The tensor products of representations of $\mathfrak{sl}_2(\mathbb{C})$ satisfy

$$W_m\otimes W_n\cong\bigoplus_{i=0}^{\min(m,n)}W_{|m-n|+2i}.$$

⌟

Proof: This follows from(18.8.3.7) or from(18.8.3.4). □

Prop. (18.8.3.9) [Weyl Dimension Formula]. Let $\mathfrak{g}$ be a split semisimple Lie algebra and $\lambda\in P^+$, then

$$\dim L_\lambda=\frac{\prod_{\alpha\in R^+}(\alpha,\lambda+\rho)}{\prod_{\alpha\in R^+}(\alpha,\rho)}$$

⌟

Proof: Choose an element $h_\rho\in\mathfrak{h}$ that corresponds to $\rho\in\mathfrak{h}^*$ via the Killing form, then

$$\chi_\lambda(2th_\rho)=\frac{\sum_{w\in W}\varepsilon(w)e^{2t(w(\lambda+\rho),\rho)}}{\prod_{\alpha\in R^+}(e^{t(\alpha,\rho)}-e^{-t(\alpha,\rho)})}.$$

The crucial fact is that we can use Weyl's denominator formula(18.8.3.5) on the nominator, to get

$$\chi_\lambda(2th_\rho)=\frac{\prod_{\alpha\in R^+}(e^{t(\alpha,\lambda+\rho)}-e^{-t(\alpha,\lambda+\rho)})}{\prod_{\alpha\in R^+}(e^{t(\alpha,\rho)}-e^{-t(\alpha,\rho)})}.$$

Now taking limit $t\to 0$, we get the desired formula. □

Remark (18.8.3.10). The Weyl dimension formula can be used to determine a representation V is irreducible or not: First calculate the maximal weight, then used the Weyl dimension formula to calculate the dimension to see if it is equal to the dimension of V. ⌟

4 Category $\mathcal{O}$

Def. (18.8.4.1) [$\mathcal{O}_{int}$]. Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebras, the category $\mathcal{O}_{int}$ is the category of representations V of $\mathfrak{g}$ that with weight decomposition into f.d. weight spaces that the weights $P(V)$ is contained in the union of sets $\lambda^i - Q^+$ for f.m. weights $\lambda^1, \ldots, \lambda^N \in P^\vee(R)$. ⌟

Def. (18.8.4.2)[Characters]. The character for a f.d. representation can be extended to category $\mathcal{O}_{int}$ as a formal Laurent series

$$\chi \in \mathbb{Z}[[e^{-\alpha_1^\vee}, \ldots, e^{-\alpha_r^\vee}]][e^{\alpha_1^\vee}, \ldots, e^{\alpha_r^\vee}] : \chi_V(h) = \sum \dim V[\mu] e^{\mu(h)}.$$

⌟

Prop. (18.8.4.3). The character of M_λ is given by

$$\chi_{M_\lambda} = \frac{e^\lambda}{\prod_{\alpha \in R^+}(1 - e^{-\alpha})} = \frac{e^{\lambda+\rho}}{\Delta}, \quad \Delta = \prod_{\alpha \in R^+} (e^{\alpha/2} - e^{-\alpha/2}).$$

where Δ is called the **Weyl denominator** of $\mathfrak{g}$. ⌟

18.9 Representations of (Non-Compact)Lie Groups

Notation (18.9.0.1).

- Use notations as in Lie Groups.

⌟

Remark (18.9.0.2) [Non-compact Lie Groups]. The feature of representations of non-compact Lie groups is most intersecting representations are infinite dimensional and involves topologies. The vector space V is assumed to be Hausdorff, second countable and complete, locally convex, and separable. ⌟

1 Basics

Prop. (18.9.1.1) [Left Invariant Differential Operators]. For a connected Lie group G, consider its left and right regular action λ, ρ on $C^\infty(G)$(11.10.1.1). We may write $\mathrm{d}X$ for $X \in \mathfrak{g}$ as the representation of $\mathfrak{g}$ via ρ, then it commutes with λ. Then it induces a map of $U(\mathfrak{g})$ to the ring of left G-invariant differential operators on G.(3.7.8.1). ⌟

Prop. (18.9.1.2) [Center element Bi-invariant]. If G is a connected Lie group with Lie algebra $\mathfrak{g}$ and $D \in Z(U(\mathfrak{g}))$, then the differential operator D defined in(18.9.1.1) is invariant under both left and right regular representations of G. ⌟

Proof: The left invariance is general from(18.9.1.1), for the right invariance, Because G is connected, it suffices to prove invariance for a nbhd of identity of G, thus suffices to prove

$$\rho(g_t)D = D\rho(g_t), \quad g_t = \exp(tX).$$

For this, let $\varphi(g,t) = (\rho(g_t)D - D\rho(g_t))(g)$ and take derivative w.r.t t, then it reads:

$$\frac{\partial}{\partial t}\varphi(g,t) = (DdX\rho(g_t)f - dX\rho(g_t)Df)(g) = dX\varphi(g,t)$$

because dX commutes with D. And also $\varphi(g,0) = 0$, so by lemma(18.9.1.3), $\varphi(g,t) = 0$ for any t, g. □

Lemma (18.9.1.3). If G is a connected Lie group with Lie algebra $\mathfrak{g}$, and $\varphi \in C^\infty(G \times \mathbb{R})$ satisfies

$$\frac{\partial}{\partial t}\varphi(g,t) = \mathrm{d}X.\varphi(g,t)$$

for some $X \in \mathfrak{g}$ and $\varphi(g,0) = 0$, then $\varphi = 0$. ⌟

Proof: Let $\varphi_g(u,v) = \varphi(g\exp(uX), v)$, then the condition says

$$\frac{\partial}{\partial u}\varphi_g(u,v) = \frac{\partial}{\partial v}\varphi_g(u,v),$$

which means $\varphi_g(u,v) = F(u+v)$, and the fact $\varphi_g(u,0) = 0$ shows $F = 0$. □

Cor. (18.9.1.4). If $G = GL(2,\mathbb{R})^+$, then $\mathfrak{g} = \mathfrak{gl}_2(\mathbb{R})$, and the Casimir element(3.7.8.20) $\Delta = -1/2(1/2h^2 + ef + fe)$ corresponds via(18.9.1.1) to a bi-invariant differential operator on $C^\infty(G)$, and it is called the **Laplace-Beltrami operator**. ⌟

Differential Vectors

Def. (18.9.1.5) [Smooth Vectors]. Let V be a continuous representation of G on a locally convex TVS. we define the space V^∞ of **smooth vectors** of V as $V^\infty = \cap_n V^n$ where

$$V^0 = \{v \in V^{n-1}, \frac{d}{dt}\exp(t\xi)v \text{ exists,}\} \quad V^n = \{v \in V^{n-1}, T_\xi(v) \in V^{n-1}, \forall \xi \in \mathfrak{g}\}.$$

And V^∞ is given the inverse limit topology. ⌟

Prop. (18.9.1.6) [Action of Distribution on Smooth Vectors]. There is a continuous action of $Distr_c(G)$ on V^∞: $T \mapsto \pi(T)$ compatible with the convolution structure on $Distr_c(G)$. ⌟

Proof: For $v \in V^\infty$, define $F^v(g) = g(v)$. For $T \in Distr_c(G)$, define

$$\pi(T)v = (T, F^v)$$

. For example,

- $\pi(\delta_x) = \pi(x)$.
- $\pi(u) = u$ for $u \in U(\mathfrak{g})$.
- $\pi(fdg)v = \int_G f(g)\pi(g)vdg$ for $f \in C_c(G)$.
- $\pi(f * g) = \pi(f)\pi(g)$.

□

Cor. (18.9.1.7). If $f \in C_c^\infty(G)$, then for any $v \in V$, the vector $T_{f\mu_{Haar}}(v) \in V^\infty$. ⌟

Proof: Notice $X\pi(f)v = \pi(X * f)v$, and we calculate $X * f$:

$$(X * f, v) = \int \frac{d}{dt}\pi(e^{tX}y)vf(y)dy = \frac{d}{dt}\int f(y)\pi(e^{tX}y)vdy = \frac{d}{dt}\int f(e^{-tX}y)\pi(y)vdy = \pi(f_X)v$$

where $f_X(g) = \frac{d}{dt}(e^{-tX}g)|_{t=0}$ is smooth. Iterating, we can show $\pi(f)v \in V^\infty$. □

Cor. (18.9.1.8) [Smooth Vectors Dense]. V^∞ is dense in V. ⌟

Proof: Choose a Dirac sequence $\{f_n\}$, then $T_{f_n\mu_{Haar}}v \in V^\infty$ converges to v, by(18.9.1.6). □

Cor. (18.9.1.9). If V is a f.d. vector space, then $V^\infty = V$. ⌟

Prop. (18.9.1.10) [Smooth Vectors in S^1]. Let $K = S^1$ and ρ be the regular representation on the Hilbert space $L^2(K) = L^2[0, 2\pi]$, then the smooth vectors in ρ are just precisely the elements of $C^\infty(K)$. ⌟

Proof: Take a Fourier expansion $f(x) = \sum a_n e^{2\pi inx}$. Suppose f is a C^1 vector, then there is a $g(x) = \sum b_n e^{2\pi inx}$ that $\lim \frac{1}{t}(f_t - f) = g$, so

$$\lim \sum_n |\frac{1}{t}(e^{2\pi int} - 1)a_n - b_n|^2 = 0.$$

which means $b_n = 2\pi ina_n$.

So if f is a C^∞ vector, then $|a_n|$ decay rapidly, and f and all its derivatives converge absolutely so f is smooth. Conversely, integration shows the Fourier coefficients of any smooth function f decay rapidly. □

Examples

Prop. (18.9.1.11) [Store-Newmann]. The Heisenberg representation of H acting on $L^2(\mathbb{R})$ is unitary and irreducible, where $\pi(p_a) = e^{iax}\cdot$, and $\pi(r_b) = T_b$. ⌟

Prop. (18.9.1.12) [$\widetilde{SL_2(\mathbb{R})}$]. Let $\widetilde{SL_2(\mathbb{R})}$ be the universal covering of $SL_2(\mathbb{R})$. Then $\mathrm{Rep}_f(\widetilde{SL_2(\mathbb{R})}) = \mathrm{Rep}_f(SL_2(\mathbb{R}))$. In particular, $\widetilde{SL_2(\mathbb{R})}$ admits no f.d. faithful representations, and the only quotient groups of it that admit f.d. faithful representations are $SL_2(\mathbb{R})$ and $PSL_2(\mathbb{R})$. ⌟

Proof: Let $\rho : \widetilde{SL_2(\mathbb{R})} \to GL(n, \mathbb{R})$ be a representation inducing a real Lie algebra representation ρ_*. Consider its complexification $\rho \otimes \mathbb{C} : \widetilde{SL_2(\mathbb{R})} \to GL(n, \mathbb{C})$. Because $SL(2, \mathbb{C})$ is simply connected(12.12.2.1), $\rho_* \otimes \mathbb{C}$ corresponds to a complex representation $\rho' : SL(2, \mathbb{C}) \to GL(n, \mathbb{C})$ by(12.11.3.13). Now because $\widetilde{SL_2(\mathbb{R})}$ is simply connected, so there is a real Lie group homomorphism $\gamma : \widetilde{SL_2(\mathbb{R})} \to SL(2, \mathbb{C})$ that $\rho' \circ \gamma = \rho$. But because ρ, ρ' both commutes with conjugation, so does γ. Thus the image of γ is in $GL(2, \mathbb{R})$, and ρ factors through $SL(2, \mathbb{R})$.

There is a quotient map $\pi : \widetilde{SL_2(\mathbb{R})} \to PSL_2(\mathbb{R})$, and $PSL_2(\mathbb{R})$ has trivial center, so the center of $\widetilde{SL_2(\mathbb{R})}$ is contained in $\ker(\pi)$, which is isomorphic to $\pi_1(PSL_2(\mathbb{R})) = \mathbb{Z}$, and is central in $\widetilde{SL_2(\mathbb{R})}$ by(12.11.1.6). so the center of $\widetilde{SL_2(\mathbb{R})}$ is just $\mathbb{Z}$. By what has been proved, for any representation of other covering space of $PSL_2(\mathbb{R})$, the induced representation on $\widetilde{SL_2(\mathbb{R})}$ factors through $SL_2(\mathbb{R})$, thus trivial on the subgroup $2\mathbb{Z} \subset \mathbb{Z}$, and the original representation factors through $SL_2(\mathbb{R})$ or $PSL_2(\mathbb{R})$. So the only possibility of faithful representation is $SL_2(\mathbb{R})$ or $PSL_2(\mathbb{R})$. For $PSL_2(\mathbb{R})$, take the □

Prop. (18.9.1.13) [F.D. Representations of $SL_2(\mathbb{K})$]. Let $\mathbb{K} = \mathbb{C}$ or $\mathbb{R}$, then the representations of $SL(2, \mathbb{K})$ are isomorphic to direct representations (ρ_n, V_n), where V_n =homogeneous polynomials of degree n in indeterminants x, y, and

$$\rho_n(\begin{bmatrix} a & b \\ c & d \end{bmatrix})(x^k y^{n-k}) = (ax + by)^k (cx + dy)^{n-k}.$$

⌟

Proof: We can check these representations truly induce irreducible representations of their Lie algebras $\mathfrak{sl}_2(\mathbb{K})$. Notice $SL(2, \mathbb{C})$ is simply connected(12.12.2.1), so(18.9.1.12) and(12.11.3.13) gives the result. □

2 Finite-Dimensional Representations

Prop. (18.9.2.1). Finite dimensional representations of a semisimple Lie group is completely reducible. ⌟

Proof: This is because its Lie algebra representation is completely reducible(18.8.1.2), and each subrepresentation corresponds to a Lie group subrepresentation. □

3 $(\mathfrak{g}, K)$-Modules

$(\mathfrak{g}, K)$-Modules

Def. (18.9.3.1) [$(\mathfrak{g}, K)$-Modules]. If G is a Lie group that may not be connected, and $K \subset G$ be a maximal compact Lie subgroup(9.3.6.11), then K acts on $\mathfrak{g}$. Then a $(\mathfrak{g}, K)$**-module** is a $\mathbb{C}$-vector space that has a K-finite action and a $\mathfrak{g}$ action that satisfies:

- for $k\in K,\eta\in\mathfrak{g}$, $T_kT_\eta T_{k^{-1}}=T_{Ad_k(\eta)}$.
- The action of $\mathfrak{k}$ on V induced by K agrees with the restriction of the action of $\mathfrak{g}$.

A $(\mathfrak{g},K)$-module is called **admissible** iff every V^ρ is of f.d.. ⌟

Def. (18.9.3.2) [Contragradient $(\mathfrak{g},K)$-Module]. If M is an admissible $(\mathfrak{g},K)$-module, then we can define its **contragradient $(\mathfrak{g},K)$-module** as

$$M^\vee=(M^*)^\infty=\oplus_\rho(M^\rho)^*,$$

which is the K-finite part of the usual dual of M, and $\mathfrak{g}$ clearly acts on it. ⌟

$(\mathfrak{g},K)$-Modules and $\mathfrak{g}$-Modules

Def. (18.9.3.3). Let K_0 be the unital component of K, then there are forgetful functors

$$\mathcal{M}\mathrm{od}_{(\mathfrak{g},K)}\to\mathcal{M}\mathrm{od}_{(\mathfrak{g},K_0)}\to\mathcal{M}\mathrm{od}_{\mathfrak{g}}.$$

⌟

Prop. (18.9.3.4). The functor $(\mathfrak{g},K_0)-mod\to\mathfrak{g}-mod$ is fully faithful, and its essential image is stable under taking submodules. ⌟

Proof: Cf.[Gaitsgory P39]. □

Cor. (18.9.3.5). If $M\in(\mathfrak{g},K)-mod$ is irreducible as a $\mathfrak{g}$-module, then it is irreducible. ⌟

Prop. (18.9.3.6). The functor $\mathcal{M}\mathrm{od}_{(\mathfrak{g},K)}\to\mathcal{M}\mathrm{od}_{\mathfrak{g}}$ sends f.g. objects to f.g. objects. ⌟

Proof: By(18.9.3.4), it suffices to consider the functor $(\mathfrak{g},K)-mod\to(\mathfrak{g},K_0)-mod$. Let M be f.g. $(\mathfrak{g},K)$-module, and $\cup M_i=M$ be a chain of $(\mathfrak{g},K_0)$-submodules. Pick $k\in K$ for each element of $\pi_0(K)$(f.m.), then each $M_i'=\sum_k k(M_i)$ is a $(\mathfrak{g},K)$-submodule, thus $M_i'=M$ for some i. Now we can choose j large that $k(M_i)\in M_j$ for any k, then $M_j=M$(because we may choose M_i be f.g. $(\mathfrak{g},K_0)$-modules)?. □

Cor. (18.9.3.7). The category $\mathcal{M}\mathrm{od}_{(\mathfrak{g},K)}$ is Noetherian. ⌟

Proof: If $M\in(\mathfrak{g},K)-mod$ is f.g. and $M_1\subset M$, then M is f.g. as $\mathfrak{g}$-module, then M_1 is f.g. as $\mathfrak{g}$-module by(3.7.8.16). So clearly it is also f.g. as a $(\mathfrak{g},K)$-module. □

Prop. (18.9.3.8). For an irreducible $(\mathfrak{g},K)$-module M, the underlying $\mathfrak{g}$-module is a direct sum of f.m. irreducibles. ⌟

Proof: By(18.9.3.4), it suffices to prove M is a direct sum of f.m. irreducible $(\mathfrak{g},K_0)$-modules. M is f.g. as a $(\mathfrak{g},K_0)$-modules by the proof of(18.9.3.6), so it has a maximal submodule M' that $N=M/M'$ is irreducible. Pick $k\in K$ for each component of K, consider

$$M''=\cap_k k(M')$$

which is a proper $(\mathfrak{g},K)$-submodule of M, so it is 0, Hence the map

$$M\to\oplus(N)^k$$

is injective, where N^k is N twisted by conjugate action of k, so it is a submodule of a semisimple-module, thus semisimple. □

Properties of $(\mathfrak{g}, K)$-Modules

Cor. (18.9.3.9) [Schur's Lemma]. Schur's lemma holds for irreducible $(\mathfrak{g}, K)$-modules. ⌟

Proof: It suffice to show any endomorphism S of an irreducible $(\mathfrak{g}, K)$-module M has an eigenvalue. But S preserves M^ρ for any ρ, and M^ρ is of f.d, thus it has an eigenvalue over $\mathbb{C}$. □

Cor. (18.9.3.10) [Irreducible Unitary Representation Determined by Finite Part]. If V_1, V_2 are two irreducible unitary representations of G that are infinitesimal equivalent, then they are isomorphic. ⌟

Proof: Firstly they are admissible by(18.9.4.7), so we can talk about their corresponding $(\mathfrak{g}, K)$-modules M_i, then V_i are the Hilbert space completion of M_i by(18.9.3.24).

Now M_i has Hermitian forms, so $M_i \cong (M^*)^{alg}$, and if $S: M_1 \cong M_2$, then S^*S is an automorphism of M_1, thus by(18.9.3.25)(18.9.3.9) it is a scalar map, so after a scalar change, we may assume S preserves Hermitian structure thus induces an isomorphism of vector spaces $V_1 \cong V_2$, so by(18.9.3.24) it is an isomorphism of G-representations. □

Prop. (18.9.3.11). Any irreducible $(\mathfrak{g}, K)$-module has a Banach space structure. ⌟

Proof: □

Action of $Z(U(\mathfrak{g}))$

Prop. (18.9.3.12). Let M be an admissible $(\mathfrak{g}, K)$-module, then

$$M \cong \oplus_{\chi \in \mathrm{Spec}(Z(\mathfrak{g}))} M_\chi$$

s.t. $Z(\mathfrak{g})$ acts on each M_χ with a generalized character χ.

Now let $(\mathfrak{g}, K) - \mathcal{M}\mathrm{od}_\chi$ be the full subcategory of $(\mathfrak{g}, K)$-modules on which $Z(\mathfrak{g})$ acts with a generalized character χ.**?** Cf.[Gaitsgory P42]. ⌟

Proof: $Z(\mathfrak{g})$ commutes with G thus K action, so it preserves each M^ρ, which are of f.d.. □

Prop. (18.9.3.13). The category $(\mathfrak{g}, K) - \mathcal{M}\mathrm{od}_\chi$ has only f.m. isomorphism classes of irreducible objects. ⌟

Proof: Cf.[Gaitsgory]. □

Prop. (18.9.3.14). If M is a f.g. $(\mathfrak{g}, K)$-module, then for any ρ of K, M^ρ is f.g. over $Z(\mathfrak{g})$. ⌟

Proof: Cf.[Gaitsgory P43]. □

Prop. (18.9.3.15). For $M \in (\mathfrak{g}, K) - mod_\chi$, the following are equivalent:

- M is f.g..
- M is of finite length.
- M is admissible.

⌟

Proof: $2 \to 1$ is trivial, $1 \to 3$ is by(18.9.3.14).

For $3 \to 2$: Use(18.9.3.13), there are only f.m. irreducible classes ρ_α, let $\rho = \oplus_\alpha \rho_\alpha$, then if there is a chain of length n, then there are at least n linearly independent morphisms in $\mathrm{Hom}_K(\rho, M)$. Thus n is bounded, because $\dim_K \mathrm{Hom}_K(\rho, M)$ is finite because M is admissible. □

Cor. (18.9.3.16). The category $(\mathfrak{g}, K) - mod_\chi$ is Artinian(4.8.3.19). ⌟

Cor. (18.9.3.17). Every irreducible $(\mathfrak{g}, K)$-module is admissible. ⌟

Proof: Firstly irreducible module are in $(\mathfrak{g}, K) - mod_\chi$ for some χ, and then use the proposition and(18.9.3.8). □

Cor. (18.9.3.18) [Harish-Chandra Modules]. For a $(\mathfrak{g}, K)$-module, the following conditions are equivalent:

- M is f.g. and admissible.
- M is f.g. and its support over $\mathrm{Spec}(Z(\mathfrak{g}))$ is finite.
- M is admissible and its support over $\mathrm{Spec}(Z(\mathfrak{g}))$ is finite.
- M is of finite length.

Then such modules are called a **Harish-Chandra module**. ⌟

Proof: ? □

Real Reductive Groups

Def. (18.9.3.19) [Admissible Representation]. Let G be a connected real reductive group(which is relevant, thus the complex representations of G and $G(\mathbb{R})$ are the same(9.3.6.8)), Let $K \subset G(\mathbb{R})$ be a maximal compact subgroup. Define $V^\infty, V^\rho, V^{K-fin}$ as in(11.10.4.7)(18.9.1.5).

An **admissible representation** of G is a representation V that for any f.d. irreducible representation ρ of K, V^ρ is of f.d. ⌟

Prop. (18.9.3.20). For any ρ, $V^\infty \cap V^\rho$ is dense in V^ρ. ⌟

Proof: ? □

Cor. (18.9.3.21). If V is admissible, then $V^{K-fin} \subset V^\infty$ by(18.9.1.9). ⌟

Prop. (18.9.3.22). If V is admissible, then V^{K-fin} is a $(\mathfrak{g}, K)$-module(18.9.3.1), and the map $V \mapsto V^{K-fin}$ induces a functor

$$Rep(G)_{adm} \to (\mathfrak{g}, K) - mod_{adm}.$$

And we call two admissible representations V_1, V_2 of G **infinitesimal equivalent** iff they are isomorphic after this functor. ⌟

Proof: By(18.9.3.21), $\mathfrak{g}$ can act on V^{K-fin}, and $U(\mathfrak{g})$ fixes V^{K-fin}: if $f \in V^{K-fin}$, let R be a f.d. K-subspace of V containing f, then $\mathfrak{k}f \in R$. Let R_1 be the f.d. vector space spanned by $\mathfrak{g}R$, then R_1 is invariant under $\mathfrak{k}$: for $X \in \mathfrak{k}, Y \in \mathfrak{g}, \varphi \in R$

$$X(Y\varphi) = [X, Y]\varphi + Y(X\varphi) \in R_1$$

so $R_1 \subset V^{K-fin}$, so $\mathfrak{g}$ fixes V^{K-fin}.

Also we check

$$T_k T_\eta T_{k^{-1}} = T_{Ad_k \eta}$$

which is by definition, and the second condition in(18.9.1.9) is also obvious. □

Lemma (18.9.3.23). Let V be an admissible representation of G, and $v \in V^{K-fin}$, then for any $\eta \in V^*$, the function $g \mapsto \eta(g(v))$ is real analytic. ⌟

Proof: Cf.[Gaitsgory P37]. □

Prop. (18.9.3.24) [$\mathrm{Rep}^{\mathrm{adm}}(G)$ **and** $(\mathfrak{g},K)$**-Modules].**

- If V_1,V_2 be two admissible representations of G, if $S:V_1\to V_2$ is a continuous map of TVS. Assume $S(V_1^{K-fin})\subset V_2^{K-fin}$ and induces a $(\mathfrak{g},K)$-module map, then the initial S is a map of G-representations.
- If $V\in Rep(G)_{adm}, M=V^{K-fin}$, then the functors

$$(V_1\subset V)\mapsto (V_1)^{K-fin}\subset M;\quad (M_1\subset M)\mapsto \overline{M}_1\subset V$$

induces mutually inverse bijections between closed G-subrepresentations of V and $(\mathfrak{g},K)$-submodules of M.

⌟

Proof: 1: It suffices to show for $v_1\in V^{K-fin}$, $T_gS(v_1)ST_g(v_1)$. So by Hahn-Banach it suffices to show for any $\eta\in V_2^*$,

$$\eta(T_gS(v_1))=\eta(ST_g(v_1)).$$

Both sides are analytic in g by(18.9.3.23), so it suffices to show all their derivatives at 1 are equal, and use the fact $\pi_0(K)\to\pi_0(G)$ is surjective(9.3.6.11). And the derivatives equal because S commutes with $\mathfrak{g}$-action.

2: Firstly $\overline{M}_1$ is a G-representation: because $\overline{M}_1=((M_1)^\perp)^\perp$ by Hahn-Banach. so it suffices to show for $v_1\in M_1,\eta(g(v_1))=0$ for any $\eta\in(M_1)^\perp$. Then this uses analyticity(18.9.3.23) as above and the fact M_1 is a $(\mathfrak{g},K)$-subrepresentation.

For the bijection, notice V_1^{K-fin} is dense in V_1 by(11.10.4.17). Conversely, for a submodule M_1, it suffices to show the image of $T_{\xi_\rho\mu_{Haar}}(\overline{M}_1)\subset M_1^\rho$ by(11.10.4.13). However $T_{\xi_\rho\mu_{Haar}}(M_1)\in M_1^\rho$ by(11.10.4.13), so this is true by continuity. □

Cor. (18.9.3.25)[Irreducibility of $(\mathfrak{g},K)$**-Modules].** An admissible G-representation V is irreducible iff V^{K-fin} is irreducible as $(\mathfrak{g},K)$-modules. ⌟

Irreducible Admissible $(\mathfrak{g},K)$-Modules of $GL(2,\mathbb{R})$

Prop. (18.9.3.26) [Lie Theory]. Let V be an irreducible admissible $(\mathfrak{g},K)$-module for $GL(2,\mathbb{R})^+$, then

- V^k is the space of all vectors $x\in V$ that $Hx=kx$.
- If $x\in V^k$, then $Rx\in V^{k+2}, Lx\in V^{k-2}$.
- If $0\neq x\in V^k$, then $\mathbb{C}x=V^k,\mathbb{C}R^nx=V^{k+2n},\mathbb{C}L^nV^{k-2n}$ and

$$V=\mathbb{C}x\oplus\bigoplus_{n>0}\mathbb{C}R^nx\oplus\bigoplus_{n>0}\mathbb{C}L^nx.$$

- Suppose $\Delta=\lambda$ on V, then if $x\in V^k$, then

$$LRx=(-\lambda-\frac{k}{2}(1+\frac{k}{2}))x,\quad RLx=(-\lambda+\frac{k}{2}(1-\frac{k}{2}))x.$$

⌟

Proof: 1: Let $W = iH$. If $x \in V^k$, then

$$Wx = \frac{d}{dt}\pi(e^{tW})x = \frac{d}{dt}\pi(k_t)x = \frac{d}{dt}e^{ikt}x = ikx$$

thus $Hx = kx$. And we know V decomposes as direct sums of representations of K(11.10.4.4), thus the result follows.

2: clear from(3.7.2.11).

3: Because the RHS is a $\mathfrak{g}$-submodule, by representation of $\mathfrak{sl}_z(\mathbb{C})$(18.8.1.11). And it is also a K-subrepresentation, by item1.

4: By(18.8.1.11). □

Cor. (18.9.3.27) [Non-Discrete Case]. For any $\lambda, \mu \in \mathbb{C}$ that $\lambda \neq \frac{k}{2}(1+\frac{k}{2})$ for k even/odd, there exists at most one isomorphism class of irreducible admissible even/odd $(\mathfrak{g}, K)$-module V on which Δ, I acts by λ, μ respectively, and the K-type is one vector f_k for each $k \in \mathbb{Z}$. ⌟

Proof: This follows from the classification of representation of $\mathfrak{sl}_2(\mathbb{C})$(18.8.1.11). Notice the action of K is controlled by(18.9.3.26) item1. □

Cor. (18.9.3.28) [Discrete Case]. Let $k \geq 1$ be an integer and $\lambda = \frac{k}{2}(1+\frac{k}{2})$. Let V be an irreducible admissible $(\mathfrak{g}, K)$-module with parity equals k, Let Σ be the K-types of V, then Σ is one of the following sets:

- $\Sigma^+(k) = \{l \in \mathbb{Z} | l \equiv k \mod 2, l \geq k\}$
- $\Sigma^-(k) = \{l \in \mathbb{Z} | l \equiv k \mod 2, l \leq -k\}$
- $\Sigma^0(k) = \{l \in \mathbb{Z} | l \equiv k \mod 2, -k < l < k\}$

And there are at most one isomorphism class with each Σ. ⌟

Proof: This follows from the classification of representation of $\mathfrak{sl}_2(\mathbb{C})$(18.8.1.11). Notice the action of K is controlled by(18.9.3.26) item1. □

Def. (18.9.3.29) [$H(s_1, s_2, \varepsilon)$]. If $\lambda \geq 1/4$, let $s - 1/2$ be the square root of $1/4 - \lambda$ which is imaginary, and let s_1, s_2 be determined that $\mu = s_1 + s_2, s = \frac{1}{2}(s_1 - s_2 + 1)$.

Consider the 1-dimensional representation σ of $B(\mathbb{R})^+$ that

$$\sigma(\begin{bmatrix} y_1 & x \\ & y_2 \end{bmatrix}) = \operatorname{sgn}(y_1)^\varepsilon |y_1|^{s_1} |y_2|^{s_2},$$

If s_1, s_2 are purely imaginary(i.e. μ is purely imaginary), then this representation is unitary, and we can consider the induced representation on $GL(2, \mathbb{R})^+$(11.10.5.3), then it is a unitary representation of $GL(2, \mathbb{R})^+$. For $f \in \operatorname{ind}_{B(\mathbb{R})^+}^G$,

$$f(\begin{bmatrix} y_1 & x \\ & y_2 \end{bmatrix} g) = \operatorname{sgn}(y_1)|y_1|^{s_1+1/2}|y_2|^{s_2-1/2}f(g)$$

and

$$(f_1, f_2) = \frac{1}{2\pi}\int_0^{2\pi} f_1(k_\theta)\overline{f_2(k_\theta)}d\theta.$$

so $H(s_1, s_2, \varepsilon)$ is identical to $L^2[-\pi/2, \pi/2]$ by Iwasawa decomposition(12.12.0.4). Then its K-finite vectors can be determined, which are sums of

$$f_l(g) = u^{s_1+s_2}y^s e^{il\theta}, l \equiv \varepsilon \mod 2.$$

so $H(s_1,s_2,\varepsilon)$ is admissible.

Even if μ is not purely imaginary, we can still define $H(s_1,s_2,\varepsilon)$ as above, and we consider its smooth vectors $H^\infty(s_1,s_2,\varepsilon)$, which are just the smooth functions in $H(s_1,s_2,\varepsilon)$, by(18.9.1.10). ⌟

Prop. (18.9.3.30). We can define the regular action of G on $H(s_1,s_2,\varepsilon)$(but may not be unitary), and the subspace $H^\infty(s_1,s_2,\varepsilon)$ is the space of smooth vectors for this representation. ⌟

Proof: It suffices to define the regular action of G on $H^\infty(s_1,s_2,\varepsilon)$ and show it is a bounded operator, so that it can be extended to $H(s_1,s_2,\varepsilon)$ by continuity.

By Cartan decomposition(12.11.5.1), G is generated by K and diagonal matrices of positive entries. $\rho(K)$ clearly preserves the inner product, so it suffices to consider these matrices.

By(20.1.1.20) and the calculation $d\theta'=y_1y_2D(\theta)^{-2}d\theta$, we have

$$\int_0^{2\pi}|\pi(\mathrm{diag}(y_1,y_2))f(k_\theta)|^2d\theta=(y_1y_2)^{s_1-1/2}\int_0^{2\pi}D(\theta)^{-s_1+s_2+1}|f(k_{\theta'})|^2d\theta'.$$

where

$$\theta'=\arctan(\frac{y_1}{y_2}\tan\theta),\quad D(\theta)=\sqrt{y_1^2\sin^2\theta+y_2^2\cos^2\theta}.$$

$D(\theta)$ is bounded above and below, thus $\pi(\mathrm{diag}(y_1,y_2))$ is a bounded operator. Also to show this representation is continuous, it suffices to show for $|f|_2$ small and y_1,y_2 small, $|\pi(\mathrm{diag}(y_1,y_2))f|_2$ is small. And this is also a consequence of the above formula. □

Lemma (18.9.3.31). For $f_l\in H(s_1,s_2,\varepsilon)$ as in(18.9.3.29), we have

$$Hf_l=lf_l,\quad ,Rf_l=(s+\frac{l}{2})f_{l+2},Lf_l=(s-\frac{l}{2})f_{l-2},\Delta f_l=\lambda f_l,\quad If_l=\mu f_l$$

⌟

Proof: Clear from(20.1.1.1) and definition of f_l(18.9.3.29). □

Prop. (18.9.3.32)[Existence of $(\mathfrak{g},K)$-Modules]. Let $s=\frac{1}{2}(s_1-s_2+1),\lambda=s(1-s),\mu=(s_1+s_2)$, then (subquotients) of the $(\mathfrak{g},K)$-module $\mathfrak{H}$ of $H(s_1,s_2,\varepsilon)$ afford classes in(18.9.3.27) and(18.9.3.28). More precisely, Δ and I acts by scalars λ,μ respectively, and

- If s is not of the form $k/2,k\equiv\varepsilon\mod 2$, then $\mathfrak{H}$ is irreducible.
- If $s\geq 1/2$ and $s=\frac{k}{2}$ where $k\geq 1$ is an integer that $k\equiv\varepsilon\mod 2$, then $\mathfrak{H}$ has two irreducible invariant subspaces $\mathfrak{H}_+,\mathfrak{H}_-$ with K-types $\Sigma+,\Sigma_-$ respectively, and the quotient $\mathfrak{H}/\mathfrak{H}_+\oplus\mathfrak{H}_-$ is irreducible and has K-type $\Sigma^0(k)$.
- If $s\leq 1/2$ and $s=1-\frac{k}{2}$ where $k\geq 1$ is an integer that $k\equiv\varepsilon\mod 2$. Then $\mathfrak{H}$ has an invariant subspace $\mathfrak{H}^0$ with K-types $\Sigma^0(k)$ and the quotient $\mathfrak{H}/\mathfrak{H}^0$ decomposes into two irreducible invariant subspaces $\mathfrak{H}^+,\mathfrak{H}^-$ with K-types $\Sigma+,\Sigma_-$ respectively.

⌟

Proof: The action of H,R,L,Δ,I is all clear from(18.9.3.31), and the decomposition and irreducibility is all clear from the representation theory of $\mathfrak{sl}_2$ and(18.9.3.27)(18.9.3.28). □

Prop. (18.9.3.33) [List of Irreducible Admissible $(\mathfrak{g},K)$-Modules for $GL(2,\mathbb{R})^+$]. Every irreducible admissible $(\mathfrak{g},K)$-module may be realized as the space of K-finite vectors in an admissible representation of G on a Hilbert space. Let $\lambda,\mu\in\mathbb{C}$, and $\varepsilon=0,1$.

- If λ is not of the form $\frac{k}{2}(1-\frac{k}{2})$, where $k \equiv \varepsilon \mod 2$, then there exists a unique irreducible admissible $(\mathfrak{g}, K)$-module of parity ε on which Δ, I acts by scalars λ, μ, denoted by $P_\mu(\lambda, \varepsilon)$. These are called the **principal series**.
- If $\lambda = \frac{k}{2}(1-\frac{k}{2})$ for some $1 \leq k \equiv \varepsilon \mod 2$, then there exists three(two for $k=1$) irreducible admissible $(\mathfrak{g}, K)$-module of parity ε on which Δ, I acts by scalars λ, μ. Their K-types are $\Sigma^\pm$, Σ^0 respectively. The irreducible admissible $(\mathfrak{g}, K)$-modules of K-types $\Sigma^\pm$ are denoted by $D_\mu^\pm(k)$. If $k > 1$, $D_\mu^\pm(k)$ are called **discrete series** and for $k = 1$ they are called **limits of discrete series**.

⌟

Proof: This is a consequence of(18.9.3.27)(18.9.3.28) and(18.9.3.32). □

Prop. (18.9.3.34) [List of Irreducible Admissible $(\mathfrak{g}, K)$-Modules for $GL(2,\mathbb{R})$]. Let $\mu \in \mathbb{C}$, and $\varepsilon = 0, 1$.

- The f.d. representations are obtained by tensoring the symmetric powers of the standard representation of G with the 1-dimensional representation of the form $\chi \circ \det$.
- If χ_1, χ_2 are quasi-characters of $\mathbb{R}^*$ that $\chi_1\chi_2^{-1}$ is not of the form $y \mapsto \mathrm{sgn}(y)^\varepsilon |y|^{k-1}$, where $k \equiv \varepsilon \mod 2$, then there is a irreducible $(\mathfrak{g}, O(2,\mathbb{R}))$-module $\pi(\chi_1, \chi_2)$.
- If $\mu \in \mathbb{R}$ and $k \geq 1$ is an integer, then there are representations $D_\mu(k) = (D_\mu^+(k) \oplus D_\mu^-(k))$, called **discrete series** if $k \geq 2$ and **limits of discrete series** if $k = 1$.

⌟

Proof: Use(18.1.1.12) on $SO(2,\mathbb{R}) \subset O(2,\mathbb{R})$. It turns out $P_\mu(\lambda, \varepsilon)$ can be extended in two ways to a representation of $O(2,\mathbb{R})$: $H(s_1, \varepsilon_1, s_2, \varepsilon_2)$, corresponding to item2. It is unitarizable as $H(s_1, s_2, \varepsilon)$ is unitarizable.

The (limits of) discrete series are conjugate in pairs and combined to give a representation of $O(2,\mathbb{R})$, which is item3. It is unitarizable as it is just $H(s_1, s_2, \varepsilon)/\mathfrak{H}^0$.

The case $D_\mu^0(k)$ are also of type I and can be extended, and this irreducible representation are exactly the smooth parts of the symmetric representation of $GL(2,\mathbb{R})$ twisted by $\chi \circ \det$. □

Cor. (18.9.3.35) [Contragradient]. Let $G = GL(2,\mathbb{R}), K = O(2,\mathbb{R})$, (π, V) be an irreducible admissible $(\mathfrak{g}, K)$-module, then the contragradient $\widehat{\pi}$ is isomorphic to the $(\mathfrak{g}, K)$-module $T_k' = T_{k^{-t}}$ and $T_X' = T_{X^{-t}}$.

And it is also isomorphic to $\pi \otimes (\omega \circ \det)$. ⌟

Proof: This is a consequence of the classification of irreducible $(\mathfrak{g}, K)$-modules(18.9.3.33), where the K-type are unchanged, eigenvalues of Δ are unchanged, and eigenvalue of I is changed to $-\mu$, so they are isomorphic. □

4 Unitary Representations

The theory of abstract harmonic analysis applies in this case11.10.

Lemma (18.9.4.1) [Auxiliary Compact Supported Function Approximation]. Let G be a locally compact Lie group and K a compact subgroup. If $\mathcal{H}$ is a unitary representation of G on a Hilbert space, and let $f \neq 0 \in \mathcal{H}$, then for any $\varepsilon > 0$, there is a $\varphi \in C_c^\infty(G)$ s.t. $\pi(\varphi)$ is self-adjoint and $|\varphi(\rho)f - f| < \varepsilon$.

Moreover, if $f \in \mathcal{H}^\xi$ which is the decomposition part for K, we can assume $\varphi(kg) = \varphi(gk) = \xi(k)^{-1}\varphi(g)$. In particular if $\mathcal{H}^\xi$ is f.d., we find a φ that $\pi(\varphi)f = f$. ⌟

Proof: By continuity, there is a nbhd H of 1 that $|\pi(g)f-f|<\varepsilon$, then we can choose a φ positive real valued with support in U with integral 1, then $|\pi(\varphi)f-f|<\varepsilon$ by(11.8.3.22). We can also choose $\varphi(g)=\varphi(g^{-1})$, then $\pi(\varphi)$ is self-adjoint.

For the second case, notice first there is a nbhd V of 1 that $kVk^{-1}\in U$ for any $k\in K$(4.12.1.6), so let φ_1 be a positive real valued function supported in V, and let

$$\varphi_0(g)=\int_K \varphi_1(kgk^{-1})dk$$

then φ_0 is supported in U and $\varphi(kgk^{-1})=\varphi_0(g)$ for any $k\in K$. Assume now that $\pi(k_\theta)=e^{ik\theta}f$, then we can use(11.10.1.39) for $P=G$ to see that

$$\pi(\varphi_0)f=\int_G\varphi_0(h)\pi(h)fdh=\int_G\int_K\varphi_0(hk)\pi(hk)fdkdh=\int_G\int_K\xi(k)\varphi_0(hk)dk\pi(h)fdh=\pi(\varphi)f$$

where

$$\varphi(g)=\int_K\xi(k)\varphi_0(gk)dk=\int_K\xi(k)\varphi_0(kg)dk$$

so $\varphi(k)=\varphi(gk)=\xi^{-1}(k)\varphi(g)$ as required. □

Unitary Irreducible Representation is Admissible

G appearing in this subsubsection are assumed to be a Lie group.

Prop. (18.9.4.2). If V is an irreducible unitary representation of G, then the image of the induced action of $Meas_c(G)$ is dense in $\mathrm{End}(V)$ in the strong topology(11.7.3.4). ⌟

Proof: This follows immediately from the von Neumann theorem(11.16.1.3) and Schur's lemma(11.10.2.4): if we denote the algebra generated by $Meas_c(G)$ by A, then

$$\overline{A}=(A^c)^c=(\mathbb{C})^c=\mathrm{End}(V).$$

□

Prop. (18.9.4.3). If V Is a representation of G that the image of the induced action of $Meas_c(G)$ is dense in $\mathrm{End}(V)$ in the strong topology, then

$$\dim(V^\rho)\leq\dim(\rho)^2.$$

⌟

Proof: Follows directly from the following two lemmas(18.9.4.5)(18.9.4.6). □

Cor. (18.9.4.4)[Irreducible Unitary Representation is Admissible]. For any irreducible unitary representation of G, the K-finite part is an irreducible admissible $(\mathfrak{g},K)$-module, and $\dim(V^\rho)\leq\dim(\rho)^2$. ⌟

Proof: Follows directly from(18.9.3.25),(18.9.4.2) and(18.9.4.3). □

Lemma (18.9.4.5). For any $\rho\in\mathrm{Irrep}(K)$, let $A_\rho=\xi_\rho\cdot Meas_c(G)\cdot\xi_\rho$, this is an algebra that acts on V^ρ by(11.10.4.13). Then there exists a family of f.d. representations π of A_ρ that:

- Each π is of dimension$\leq n=\dim(\rho)^2$.

- For every element $a \in A_\rho$, there exists a π that $\pi(a)$ is non-trivial.

⌟

Proof: Consider the set of all irreducible f.d. representations of G, and π^ρ their ρ-isotopic parts. Then these are representations of A_ρ, and for any $\varphi \in Meas_c(G)$, there is a π that $T_\varphi \neq \mathrm{Id}$?, and each π^ρ has dimension$\leq \dim(\rho)^2$?. Cf.[Gaitsgory P46]. □

Lemma (18.9.4.6). If A is an associative algebra equipped with a family of f.d. modules satisfying conditions in(18.9.4.5), then if V is a representation of A that the image of A is dense in $\mathrm{End}(V)$ in the strong topology, then $\dim V \leq n$. ⌟

Proof: For an associated algebra A, consider the minimal integer r that the property $P(r)$:

$$\sum_{\sigma\in\Sigma_r} \mathrm{sgn}(\sigma) a_{\sigma(1)}\cdots a_{\sigma(r)} = 0$$

for any $a_1,\ldots,a_r$, then Amitsur-Levitski showed that for $A = GL(n,\mathbb{C})$, $r = 2n$(3.7.11.7).

Now the condition of A in(18.9.4.5) shows that P_{2n} is true for A. If $\dim V \geq n+1$, then the image of A satisfies $P(2n)$, so also $\mathrm{End}(V)$ satisfies $P(2n)$ because A is dense in $\mathrm{End}(V)$. But V contains a subgroup $GL(n+1,\mathbb{C})$, so it cannot satisfy $P(2n)$ by(3.7.11.7), contradiction. □

Cor. (18.9.4.7). Let V be an irreducible unitary representation of G, then for any $\rho \in Irrep(K)$,

$$\dim(V^\rho) \leq \dim(\rho)^2.$$

In particular, every unitary irreducible representation of G is admissible. ⌟

Proof: Directly from Lemmas(18.9.4.2) and(18.9.4.3) above, as the action of A_ρ on V^ρ is also have dense image in the strong topology. □

Prop. (18.9.4.8). If M is an irreducible $(\mathfrak{g},K)$-module equipped with an invariant inner product $((km_1,km_2) = (m_1,m_2), (\xi m_1,m_2)+(m_1,\xi m_2) = 0)$, then the Hilbert space completion of M carries a unique unitary G-representation s.t. $V^{K-fin} = M$ as $(\mathfrak{g},K)$-modules. ⌟

Proof: By(18.9.4.9), the Hermitian form can be extended continuously to the Banach space completion of M, It suffices to prove the extended Hermitian form is continuous, because them we can choose its completion w.r.t. $(-,-)$.

For the invariance, consider $f(g) = (gm_1,m_2)-(m_1,g^{-1}m_2)$, then notice $(a,-)$ are continuous functional on V, thus by(18.9.3.23) and similar analytic method as in(18.9.3.24) using the invariance of inner product. □

Lemma (18.9.4.9). Situation as in(18.9.4.8), M has a Banach norm that $(m,m) \leq ||m||^2$. ⌟

Proof: (18.9.3.11) shows M does have a Banach norm. Then let $M \cong V^{K-fin}$ and $M^{*alg} \cong (V^*)^{K-fin}$. However the Hermitian form induces $M \cong M^{*alg}$, thus we can form

$$M \xrightarrow{\Delta} M\oplus M \to V\oplus V^*$$

let V' be the closure of the image of M, then it is a G-representation by(18.9.3.24), and then

$$(m,m) \leq ||i_1(m)||||i_2(m)|| \leq (||i_1(m)||+||i_2(m)||)^2.$$

□

Cor. (18.9.4.10). The above proposition(18.9.4.8) is true for M admissible. ⌟

Hecke Algebras

Prop. (18.9.4.11) [Hecke Algebras of Lie Groups].

- If K is a compact Lie group, then the **Hecke algebra** $\mathcal{H}_K$ is defined to be the ring of smooth functions on K that is K-finite under both left and right translations, where the algebra is given by convolution. By Peter-Weyl theorem, these functions are dense in $C(K)$ and $L^2(K)$, and it is an idempotented algebra over $\mathbb{C}$**?** Cf.[Bump, P309].
- If G is a real reductive group and K is a maximal compact subgroup, then the **Hecke algebra** $\mathcal{H}_G$ is defined to be $\mathcal{H}_G = \mathcal{H}_K \otimes_{U(\mathfrak{k}_\mathbb{C})} U(\mathfrak{g}_\mathbb{C})$, where the right action of $U(\mathfrak{k}_\mathbb{C})$ on $\mathcal{H}_K$ is given by

$$f * D = \rho(D) f,$$

? Cf.[Bump, P312].

⌟

Proof: □

Prop. (18.9.4.12) [Equivalence of Representations Lie Group Case].

- For a compact Lie group K, the category $\mathcal{M}(K)$ of smooth representations of $\mathcal{H}_K$ is equivalent to the category of unitary representations of K.
- For a real reductive group G and a maximal compact subgroup K, the category of (admissible)$(\mathfrak{g}, K)$-modules is equivalent to the category of smooth(admissible) modules of $\mathcal{H}_G$.

⌟

Proof: Cf.[Cohomological Induction and Unitary Representations, P75]. □

Irreducible Unitary Representations of $GL(2,\mathbb{R})^+$

Lemma (18.9.4.13) [Finite Dimensional Case]. The only irreducible f.d. unitary representations of the group $GL(n,\mathbb{R})^+$ are the 1-dimensional characters $g \mapsto \det(g)^r$ where r is purely imaginary. ⌟

Proof: Such a representation defines a continuous map of $GL(n,\mathbb{R})^+$ into the compact unitary group $U(n)$. Now it induces a Lie algebra map $\mathfrak{sl}_n(\mathbb{R}) \to \mathfrak{u}_m$. This map must be trivial because otherwise this is an embedding because $\mathfrak{sl}_n(\mathbb{R})$ is simple. But this is impossible because the adjoint action of $\mathfrak{sl}_n(\mathbb{R})$ has real eigenvalues but the adjoint action of $\mathfrak{u}_m$ are all purely imaginary by(3.7.5.4). So the action is trivial on $SL(n,\mathbb{R})^+$, so induces an irreducible representation of $\det(g)$, which is clearly 1-dimensional. □

Lemma (18.9.4.14). Because for a unitary representation $\mathcal{H}$ of G, for $X \in \mathfrak{g}$, we have

$$(Xu, v) = -(u, Xv),$$

so $(Xv, w) = -(v, \overline{X}w)$ when complexified. So

$$(Rv, w) = -(v, Lw)$$

for any $v, w \in \mathcal{H}$, by(20.1.0.1). ⌟

Lemma (18.9.4.15) [Principal Series]. For the principal series $P_\mu(\lambda, \varepsilon)$ of $GL(2,\mathbb{R})^+$, there exists an irreducible unitary representation in this class if μ is purely imaginary and $\lambda \geq 1/4$ real. ⌟

Proof: Consider the unitary representation $H(s_1, s_2, \varepsilon)$ defined in(18.9.3.29), then it is irreducible and its class is $P_\mu(\lambda, \varepsilon)$ by(18.9.3.32) and(18.9.3.25). □

Lemma (18.9.4.16)[Possibilities of Unitary Representations]. Let $\mathcal{H}$ be a unitary representation of $GL(2,\mathbb{R})^+$. Assume Δ, I acts by scalars λ, μ respectively, then

- μ is purely imaginary and λ is real.
- If the $(\mathfrak{g}, K)$-module type of $\mathcal{H}$ is a principal series $P_\mu(\lambda, \varepsilon)$, then $\lambda > 0$, and if $\varepsilon = 1$, $\lambda > 1/4$. ⌟

Proof: 1: This follows from(18.9.4.14), as action of I is skew-symmetric and action of Δ is symmetric.

2: By(18.9.3.27), $V^k \neq 0$ for $k \equiv \varepsilon \mod 2$, let $f_k \in V^k$. Because $-4\Delta - H^2 + 2H = 4RL$(20.1.0.1), take $k = \varepsilon$, then

$$(-4\lambda - \varepsilon^2 + 2\varepsilon) f_\varepsilon = 4RL f_\varepsilon.$$

But by(18.9.4.14),

$$(4RL f_\varepsilon, f_\varepsilon) = -4(L f_\varepsilon, L f_\varepsilon) < 0$$

thus $4\lambda > 2\varepsilon - \varepsilon^2$. □

Cor. (18.9.4.17) [Reduction of μ]. The infinitesimal equivalence class of representations $P_\mu(\lambda, \varepsilon)$ or $D_\mu^\pm(k)$ contains an irreducible unitary representation iff μ is purely imaginary and the corresponding class $P(\lambda, \varepsilon)$ or $D^\pm(k)$ contains an irreducible unitary representation. ⌟

Proof: μ must be purely imaginary by the proposition. And we may tensoring a unitary representation by a $\deg(g)^r$, it is also unitary iff r is purely imaginary, and this increases the value of action of I by $2r$ and doesn't affect μ and ε because Δ has nothing to do with u(20.1.1.1). □

Prop. (18.9.4.18) [Intertwining Integral]. Let $s = \frac{1}{2}(s_1 - s_2 + 1)$, define for $f \in V$,

$$M(s) : H^\infty(s_1, s_2, \varepsilon) \to H^\infty(s_2, s_1, \varepsilon) : (M(s)f)(g) = \int_{N(F)} f(w_0 u g) du.$$

Then if $\mathrm{Re}(s_1 - s_2) > 0$, the integral is absolutely convergent, and commutes with the action of G. ⌟

Proof: Replacing f with $\rho(h)f$, we see that the convergence of $M(s)(f)(h)$ is equivalent to the convergence of $M(s)(\rho(h)f)$, so we assume $h = 1$.

We use the identity

$$\begin{bmatrix} & -1 \\ 1 & \end{bmatrix} \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} = \begin{bmatrix} \Delta_x^{-1} & -x\Delta_x^{-1} \\ & \Delta_x \end{bmatrix} k_{\theta_x}$$

similar to(20.1.1.20) where

$$\Delta_x = \sqrt{1 + x^2}, \quad \theta(x) = \arctan(-1/x).$$

Then

$$(M(s)f)(1) = \int_{-\infty}^{\infty} (1 + x^2)^{-s} f(k_{\theta(x)}) dx$$

which convergences for $s > 1/2$, that is $\mathrm{Re}(s_1 - s_2) > 0$.

To show $M(s)f \in H(s_2, s_1, \varepsilon)$, we check

$$(M(s)f)(\begin{bmatrix} 1 & \xi \\ & 1 \end{bmatrix} g) = (M(s)f)(g), \quad (M(s)f)(\begin{bmatrix} y_1 & \\ & y_2 \end{bmatrix} g) = \mathrm{sgn}(y_1)^\varepsilon |y_1|^{s_2 + \frac{1}{2}} |y_2|^{s_1 - \frac{1}{2}} (M(s)f)(g).$$

The first one is an easy consequence of change of variable, for the second,

$$\begin{aligned}(M(s)f)(\begin{bmatrix} y_1 & \\ & y_2 \end{bmatrix} g) &= \int f(\begin{bmatrix} & -1 \\ 1 & \end{bmatrix}\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}\begin{bmatrix} y_1 & \\ & y_2 \end{bmatrix} g)dx \\ &= \int f(\begin{bmatrix} & -1 \\ 1 & \end{bmatrix}\begin{bmatrix} y_1 & \\ & y_2 \end{bmatrix}\begin{bmatrix} 1 & y_1^{-1}y_2 x \\ & 1 \end{bmatrix} g)dx \\ &= \frac{y_1}{y_2}\int f(\begin{bmatrix} y_1 & \\ & y_2 \end{bmatrix}\begin{bmatrix} & -1 \\ 1 & \end{bmatrix}\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} g)dx \\ &= \frac{y_1}{y_2}\mathrm{sgn}(y_1)^\varepsilon |y_1|^{s_2-\frac{1}{2}}|y_2|^{s_1+\frac{1}{2}}\int f(\begin{bmatrix} & -1 \\ 1 & \end{bmatrix}\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} g)dx \\ &= \mathrm{sgn}(y_1)^\varepsilon |y_1|^{s_2+\frac{1}{2}}|y_2|^{s_1-\frac{1}{2}}(M(s)f)(g)\end{aligned}$$

To check $M(s)f$ is smooth, notice that the restriction of $M(s)f$ to K equals

$$(M(s)f)(k_t) = \int_{-\infty}^{\infty}(1+x^2)^{-s} f(k_{\theta(x)+t})dx.$$

The convergence is uniform in t, thus is smooth in t.

The commutativity of $M(s)$ with G-action is immediate, because left and right action commutes. □

Prop. (18.9.4.19). Let $f_{k,s}$ be the function f_k in $H(s_1,s_2,\varepsilon)$(18.9.3.29) where $\mathrm{Re}(s_1-s_2)>0$ and $s=\frac{1}{2}(s_1-s_2+1)$, then

$$M(s)f_{k,s} = (-i)^k\sqrt{\pi}\frac{\Gamma(s)\Gamma(s-\frac{1}{2})}{\Gamma(s+\frac{k}{2})\Gamma(s-\frac{k}{2})}f_{k,1-s}$$

⌟

Proof: Because $M(s)$ commutes with G-action, $M(s)f_{k,s}$ is a multiple of $f_{k,1-s}$, thus it suffices to calculate $(M(s)f_{k,s})(1)$, which is

$$(M(s)f)(1) = \int_{-\infty}^{\infty}(1+x^2)^{-s}e^{ik\theta(x)}dx, \quad \theta(x)=\arctan(-1/x)$$

by(18.9.4.18).

This integral then is calculated to be the expression above, by(11.3.10.1). □

Lemma (18.9.4.20) [Complementary Series]. For μ purely imaginary and $0<\lambda<1/4$ and $\varepsilon=0$, there exists an irreducible unitary representation in this class of the $(\mathfrak{g},K)$-module $P_\mu(\lambda,0)$. ⌟

Proof: Let s_1,s_2 be complex numbers, we construct first a Hermitian pairing

$$H(s_1,s_2,\varepsilon)_{fin}\times H(-\overline{s_1},-\overline{s_2},\varepsilon)_{fin}\to\mathbb{C}:(f,g')\mapsto\int_K f(k)\overline{g'(k)}dk$$

which is invariant under action of G by(11.10.1.45). Now let $s_2=-\overline{s_1}$, then $s=\frac{1}{2}(s_1-s_2+1)$ is real and $\mu=s_1+s_2$ is purely imaginary. Then composing this pairing with $i^\varepsilon M(s): H(s_1,s_2,\varepsilon)_{fin}\to H(s_2,s_1,\varepsilon)_{fin}=H(-\overline{s_1},-\overline{s_2},\varepsilon)_{fin}$, then

$$(f,\overline{f}')=\int_K f(k)\overline{i^\varepsilon M(s)f'(k)}dk.$$

is G-invariant. We will show that it is positive definite if $\varepsilon = 0$ and $1/2 < s < 1$.

It can be seen from(18.9.4.19) that an orthogonal basis for $H(s_1, s_2, 0)_{fin}$ under this pairing is $f_{k,s}$ for k even. And by(18.9.4.19),

$$(f_{k,s}, f_{k,s}) = (-1)^{k/2}\sqrt{\pi}\frac{\Gamma(s)\Gamma(s-\frac{1}{2})}{\Gamma(s+\frac{k}{2})\gamma(s-\frac{k}{2})}$$

which is positive for $1/2 < s < 1$. Now we obtain a unitary representation of G on the Hilbert completion of this space(11.10.2.8).

Now we have constructed a unitary representation in the infinitesimal equivalence class $P_\mu(\lambda, 0)$ with $\lambda = s(1-s)$, $s = \frac{1}{2}(s_1 - \overline{s_1} + 1)$, so any $0 < \lambda < 1/4$ is possible. □

Lemma (18.9.4.21). For any integer k, there is a bijection between holomorphic functions φ on $\mathcal{H}$ and smooth functions Φ on $GL(2,\mathbb{R})^+$ that is invariant under $Z(R)^+$ and

$$\Phi(gk_\theta) = e^{ik\theta}\Phi(g), \quad L\Phi = 0.$$

┘

Proof: The bijection is given by

$$\varphi(z) = y^{-k/2}\Phi(\begin{bmatrix} y & x \\ & 1 \end{bmatrix}), \quad \Phi(g) = ((y^{k/2}\varphi)[g]_k)i.$$

and the proof is a combination of formal calculation in(20.1.2.9) and(20.1.1.19) forgetting Γ:

$$L_k(y^{k/2}f(z)) = -(z-\overline{z})\frac{\partial}{\partial\overline{z}} - \frac{k}{2}(y^{k/2}f(z)) = -2iy^{(k+2)/2}\frac{\partial}{\partial\overline{z}}f(z).$$

□

Lemma (18.9.4.22) [Discrete Series]. if $k > 1$, then there exists a unitary representation in the infinitesimal equivalence class $D^{\pm}(k)$, more precisely,

- Let $L^2(\mathcal{H}, \mu_k)$ be the L^2-space of holomorphic functions f on the upper plane $\mathcal{H}$ w.r.t the measure $\mu_k = y^k\frac{dxdy}{y^2}$(11.5.3.3). Then the left action

$$\pi_k(g)f = f[g^{-1}]_k.$$

  of G is unitary and this representation π_k is in the infinitesimal equivalence class $D^-(k)$.

- Consider the automorphic of $GL(2,\mathbb{R})^+$:

$$\iota(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = \begin{bmatrix} a & -b \\ -c & d \end{bmatrix}$$

  then the representation $\pi_k \circ \iota$ is in the infinitesimal equivalence class $D^+(k)$

┘

Proof: The second one follows from the first one, as ι interchanges the action of K thus the K-types.

For the first one, firstly it is a unitary representation: for $z' = g(z) = x' + iy'$, we have

$$y' = \frac{ad-bc}{|cz+d|^2}y$$

and $\mu_z = \mu_{z'}$, thus

$$||\pi(g^{-1})f||^2 = \int_{\mathcal{H}} |f(z')|^2 \frac{(ad-bc)^k}{|cz+d|^{2k}} y^k \mu_z = \int_{\mathcal{H}} |f(z')|^2 (y')^k \mu_{z'} = ||f||^2.$$

For the infinitesimal equivalence class, we consider the orthogonal basis $\varphi_n = (\frac{z-i}{z+i})^n \frac{(2i)^k}{(z+i)^k}$ and prove

$$\pi(k_\theta^{-1})\varphi_n = e^{2\pi i(k+2n)\theta}\varphi_n.$$

Then this will determine the K-type of π_k. This can be proven by direct calculation, Cf.[Ngo, P39]. □

Cor. (18.9.4.23). By(18.9.4.21) and the measure μ_k we choose, it is clear that there is an isometry between $L^2(\mathcal{H}, \mu_k)$ and a subspace of $L^2(G/Z)$ that is compatible with the left G action on $L^2(G)$, but the left and right action on $L^2(G/Z)$ is isomorphic, as $f(t) \mapsto f(t^{-1})$ intertwine them, because G/Z is unimodular. So this representation is **square integrable**, i.e. it can be embedded in $L^2(G/Z)$. ⌟

Lemma (18.9.4.24) [Limits of Discrete Series]. There exists a unitary representation in the infinitesimal equivalence class $D^{\pm}(1)$. ⌟

Proof: These two classes already appear in the unitary representation $H(0, 0, 1)$, by(18.9.3.32). □

Prop. (18.9.4.25) [List of Irreducible Unitary Representations of $GL(2, \mathbb{R})^+$]. Let μ be purely imaginary,

- The 1-dimensional representation $g \mapsto |\deg(g)|^\mu$.
- The unitary principal series $P_\mu(\lambda, \varepsilon)$, where $\varepsilon = 0, 1$ and $\lambda \geq 1/4$.
- The complementary series representations $P_\mu(\lambda, 0)$ where $0 < \lambda < 1/4$.
- The holomorphic discrete series $D^0_\mu(k)(k \geq 2)$ and limits of discrete series $(k = 1)$ $D^{\pm}_\mu(k)$.

Notice each of these infinitesimal equivalence classes of irreducible representations has a unique representative that is a unitary representation by(18.9.3.10). ⌟

Proof: By(18.9.3.25) and(18.9.3.10), the conclusion follows from the classification of $(\mathfrak{g}, K)$-modules(18.9.3.33) and determining which infinitesimal class has a unitary representative, which follows from(18.9.4.13)(18.9.4.16), (18.9.4.15)(18.9.4.17), (18.9.4.20)(18.9.4.22), (18.9.4.24). □

Cor. (18.9.4.26). Similar as in(18.9.3.34), by(18.9.3.25), we can classify all irreducible unitary representations of $GL(2, \mathbb{R})$. ⌟

18.10 Cuspidal Representations

1 GL(n)

References are [Local Langlands Correspondence for GL(2)], [Bushnell and P. Kutzko. The admissible dual of GL(N) via compact open subgroups].

Prop. (18.10.1.1) [Bushnell-Kutzko]. All cuspidal representations of $GL(n, F)$ can be constructed by induction from open subgroups. ⌟

Proof: Cf.[Bushnell, C. and P. Kutzko, The admissible dual of $GL(N)$ via compact open subgroups, Princeton University Press, Princeton (1993).] □

2 SL(n)

[Bushnell and P. Kutzko.The admissible dual of SL(N)]

18.11 Admissible Representations of GL(n) over p-Adic Number Fields

Main references are [Bum98], [Representation theory of GL(n) over non-Archimedean local fields, Prasad],[B-Z76], [C.J. Bushnell and P.C. Kutzko, The admissible dual of GL(N) via compact open subgroups, Princeton university press, Princeton, (1993).]

Notation (18.11.0.1).

- Use notations defined in Classical Representation Theory.
- Let K be a p-adic local field or a finite field.
- Use group-theoretic notations as in(20.5.0.3).
- Fix a non-trivial character ψ of K with conductor $\mathfrak{p}^{-n(\psi)}$.
- Choose the Haar measure dx on K that is self-dual w.r.t. ψ as in(11.10.3.33).
- For $\alpha \in \mathbb{A}^{n-1}(K)$, let $\psi_{N,\alpha}$ be a character of $N(K)$ given by $\psi_N(g) = \sum_i \psi(\alpha_i g_{i,i+1})$.

⌟

Def. (18.11.0.2) [p-adic Local Fields]. If K is a p-adic local field, let $\mathcal{O}_K$ the ring of integers in K, $\mathfrak{p}$ the maximal ideal in $\mathcal{O}_K$, and ϖ a fixed uniformizer of $\mathfrak{p}$.

Denote $\mathcal{K} = GL(n, \mathcal{O}_K)$, $G_n^0 = \det^{-1}(\mathcal{O}^*) \subset GL(n, K)$.

Define subgroups $\mathrm{Unip}_k(n, K)$ of $\mathrm{Unip}(n, K)$ as $\mathrm{Unip}_k(n, K)$ is the group of unipotent matrices that $v(e_{ij}) \geq k(i-j)$. Then $\cup_{k>0} \mathrm{Unip}_k(n, K) = \mathrm{Unip}(n, K)$. In particular, $\mathrm{Unip}(n, K)$ is exhausted by compact open subgroups.

For any character χ of $\mathcal{O}_K^*$, by continuity, there is a minimum v that $c(1 + \mathfrak{p}^v) = 1$, and $\mathfrak{p}^v$ is called the **conductor** of χ. ⌟

1 Basics

References are [Representations of p-adic Groups Bernstein]. [Bum98]Chap4.

Geometry

Prop. (18.11.1.1). $GL(n, K)$ is unimodular, and the modular function of $B(K)$ is $\Delta_B(\begin{bmatrix} x & y \\ & z \end{bmatrix}) = \frac{z}{x}$ by(11.10.1.20). Also denote $\delta = \Delta_B^{-1}$. ⌟

Def. (18.11.1.2) [Unramified Quasi-Characters]. A **unramified quasi-character** on F is a quasi-character χ that $\chi(\mathcal{O}_K^\times) = 0$.

Define $\alpha(\chi) = \chi(\varpi)$ if χ is unramified and 0 otherwise, called the **Satake parameter** of χ. ⌟

Prop. (18.11.1.3) [Diagonal Quasi-Characters]. Let $\chi_1, \ldots, \chi_n$ be quasi-characters of K^*, then define two quasi-characters χ, χ' on $T(K)$:

$$\chi(\mathrm{diag}(y_1, \ldots, y_n)) = \chi_1(y_1) \ldots \chi_n(y_n), \quad \chi(\mathrm{diag}(y_1, \ldots, y_n)) = \chi_n(y_1) \ldots \chi_1(y_n).$$

When $n = 2$, the quasi-character χ on $T(K)$ is called **regular** if $\chi_1 \neq \chi_2$, and **dominant** if $|\chi_1(\varpi)| < |\chi_2(\varpi)|$. ⌟

Prop. (18.11.1.4) [Iwasawa Decomposition]. $GL(n,K) = B(K)\mathcal{K}$, in particular, $B(K)\backslash G$ is compact. ⌟

Proof: Prove by induction on n. $n=1$ is clear. Given a $g \in GL(n,K)$, we consider its bottom row, as let x_{n_k} be the term of minimal multiplicative valuation, then we can right multiply by a permutation matrix $w \in K$ that x_{nn} is of minimal valuation. Now right multiply by a matrix k, which is 1 on the diagonal and $k_{ni} = -x_i x_n^{-1}$ on the bottom row, then $k \in K$, and gk has bottom row$= e_n$. Thus we can induct and find a $k_0 \in \mathcal{K}$ that $gk_0 \in B(K)$. □

Prop. (18.11.1.5) [p-adic Cartan Decomposition]. A complete set of double coset representatives for $\mathcal{K}\backslash GL(n,K)/\mathcal{K}$ consists of diagonal matrices $\{\begin{bmatrix}\varpi^a & \\ & \varpi^b\end{bmatrix}, a \leq b \in \mathbb{Z}\}$. ⌟

Proof: This follows directly from Smith normal form(12.11.5.7). □

Cor. (18.11.1.6). $GL(n,K)$ is σ-compact. ⌟

Def. (18.11.1.7) [Principal Congruence Subgroups]. There is a map $\pi : \mathcal{K} \to GL(n, \mathcal{O}_K/(\varpi^m))$, the kernel of which is called the **principal congruence subgroup** of level m, denoted by $\mathcal{K}_m$. ⌟

Def. (18.11.1.8) [Partition and Groups]. Let $\alpha = (n_1, \ldots, n_k)$ be a partition of n, define

$$\mathrm{GL}_\alpha = \mathrm{GL}(n_1) \times \ldots \times \mathrm{GL}(n_k), \quad \mathcal{K}_\alpha = \mathcal{K} \cap GL_\alpha(F), \quad B_\alpha = B \cap \mathrm{GL}_\alpha, \quad D_\alpha = D \cap \mathrm{GL}_\alpha$$

And for a principal congruence subgroup $\mathcal{K}_m$ of $GL(n,K)$, $\mathcal{K}_m \cap GL_\alpha(F)$ is called a principal congruence subgroup of $GL_\alpha(F)$.

Denote U_α the subgroup of U_n That $a_{ij} = 0$ for i,j in the same segment of α and $i \neq j$. Let $P_\alpha = \mathrm{GL}_\alpha \ltimes U_\alpha$ be the parabolic subgroup corresponding to .

For $\beta \prec \alpha$, denote

$$U_\beta(\alpha) = U_\beta \cap \mathrm{GL}_\alpha, \quad P_\beta(\alpha) = P_\beta \cap \mathrm{GL}_\alpha = \mathrm{GL}_\beta \ltimes U_\beta(\alpha).$$

Let $N = \mathcal{K}_m \cap G_\alpha$ be a principal congruence subgroup, denote

$$N_\beta^+(\alpha) = N \cap U_\beta(\alpha), \quad N_\beta^-(\alpha) = N \cap \overline{U}_\beta(\alpha), \quad N_\beta^0(\alpha) = N \cap GL_\beta(F).$$

Moreover, define $K_0(\mathfrak{a}) = \pi^{-1}(B(\mathcal{O}_F/\mathfrak{a})), K_1(\mathfrak{a}) = \pi^{-1}(N(\mathcal{O}_F/\mathfrak{a}))$. In particular, $K_0(\mathfrak{p})$ are called the **Iwahori subgroup**, a vector is called **Iwahori fixed** iff it is $K_0(\mathfrak{p})$-fixed. ⌟

Prop. (18.11.1.9) [Iwahori Factorizations]. If $\mathfrak{a} \neq \mathcal{O}$, there are **Iwahori factorizations**

$$K_0(\mathfrak{a}) = N_-(\mathfrak{a})T(\mathcal{O})N(\mathcal{O}), \quad K_1(\mathfrak{a}) = N_-(\mathfrak{a})T(\mathfrak{a})N(\mathcal{O})$$

$$N = N_\beta^-(\alpha)N_\beta^0(\alpha)N_\beta^+(\alpha) = N_\beta^+(\alpha)N_\beta^0(\alpha)N_\beta^-(\alpha)$$

⌟

Proof: This is by column and row reduction. Cf.[Bernstein-Zelevinsky 1, P32].**?** □

Cor. (18.11.1.10). Denote $K_0 = K_0(\mathfrak{a})$ or $K_1(\mathfrak{a})$, and $T_0 = T(\mathcal{O})$ or $T(\mathfrak{a})$ respectively, then we can decompose the Haar measure on K_0 as

$$\int_{K_0} \varphi(k)dk = \int_{N_-(\mathfrak{a})}\int_{T_0}\int_{N(\mathcal{O})} \varphi(n_- t_0 n) dn dt_0 dn_- = \int_{N_-(\mathfrak{a})}\int_{T_0}\int_{N(\mathcal{O})} \varphi(n t_0 n_-) dn dt_0 dn_-.$$

⌟

Proof: Use(11.10.1.39), noticing all groups here are compact. □

Cor. (18.11.1.11) [Iwahori-Bruhat Decomposition].

$$GL(2,K)=B(K)K_0(\mathfrak{p})\coprod B(K)w_0K_0(\mathfrak{p}).$$

? How about the general case? ⌟

Proof: By pulling back the Bruhat decomposition of $GL(2,\mathcal{O}/\mathfrak{p})$ to $\mathcal{K}=GL(2,\mathcal{O})$, we have

$$\mathcal{K}=K_0(\mathfrak{p})\cup K_0(\mathfrak{p})w_0K_0(\mathfrak{p}).$$

The Iwahori factorization shows $K_0(\mathfrak{p})=(K_0(\mathfrak{p})\cap B(K))N_-(\mathfrak{p})$. Then this implies

$$\mathcal{K}=K_0(\mathfrak{p})\cup(K_0(\mathfrak{p})\cap B(K))w_0K_0(\mathfrak{p}),$$

because $w_0^{-1}N_-(\mathfrak{p})w_0\in K_0(\mathfrak{p})$. Then Iwasawa decomposition $G=BK$ gives the desired result. Notice this decomposition is clearly disjoint. □

Prop. (18.11.1.12).

- Any open normal subgroup of $GL(2,K)$ must contain $SL(2,K)$.
- If a subgroup of $GL(2,K)$ contains $N(K)$ and an open subgroup, then it must contain $SL(2,K)$.

⌟

Proof: 1: this normal subgroup contains $\begin{bmatrix}1&a\\&1\end{bmatrix}$ for $|a|$ small enough, and it is also a group, but $\begin{bmatrix}t&\\&t^{-1}\end{bmatrix}^{-1}\begin{bmatrix}1&a\\&1\end{bmatrix}\begin{bmatrix}t&\\&t^{-1}\end{bmatrix}=\begin{bmatrix}1&at^{-1}\\&1\end{bmatrix}$, thus it contains all $N(K)$. and then by item2 it contains $SL(2,K)$. Now for any f.d. irreducible smooth representation of $GL(2,K)$, choose a basis $v_1,\ldots,v_n$, then there is an open normal subgroup fixing all v_i, thus $SL(n,F)$ acts trivially on V, and then it factors through $\det:GL(2,K)\to K^\times$, and any irreducible representation of $K^\times$ is of 1-dimensional by Schur's lemma, so V must be 1-dimensional.

2: It contains some matrix that is not upper-triangular, so it contains $SL(2,K)$ by(3.1.5.9). □

Hecke Algebras

Prop. (18.11.1.13) [Spherical Idempotents]. The Hecke algebra $\mathcal{H}_{GL(n,K)}$(18.1.5.12) has a spherical idempotent(3.6.4.10) $e_{\mathcal{K}}$, where the anti-involution is given by transposition.

Then via the correspondence(18.1.5.16), $(\pi,V)\in\mathrm{Irr}^{\mathrm{adm}}(GL(n,K))$ is called a **spherical representation** if its corresponding $\mathcal{H}_{GL(n,K)}$-module is spherical(3.6.4.11). Equivalently, it contains a $\mathcal{K}$-fixed vector. And the dimension of spherical vectors is≤ 1 by(3.6.4.11). ⌟

Proof: For the invariance of $\mathcal{H}[e_{\mathcal{K}}]$, notice that $\mathcal{H}[e_{\mathcal{K}}]=\mathcal{H}_{\mathcal{K}}$ is the subspace of $\mathcal{K}$-bi-invariant functions on G, but we have the p-adic Cartan decomposition(18.11.1.5), so the value of $\varphi\in H[e_{\mathcal{K}}]$ are determined by restriction on the diagonal matrices, but they are invariant under transposition. This shows $e_{\mathcal{K}}$ is spherical. □

Prop. (18.11.1.14) [Transpose Invariant Distribution]. If $\mathcal{D}$ is a distribution on $GL(n,K)$ that is invariant under conjugation, then it is also invariant under transpose. ⌟

Proof: This follows from(18.1.5.11), as we look at the conjugate action of G on itself, with σ being the transposition. Conjugate action is constructive, by(9.2.1.23), and $g^\sigma = g^{-t}$, and a matrix is conjugate to its traspose(3.5.4.18). □

Prop. (18.11.1.15) [Gelfand-Kazhdan]. If $(\pi, V) \in \mathrm{Irr}^{\mathrm{adm}}(\mathrm{GL}(n, K))$, then:

- If π_1 is defined by $\pi_1(g) = \pi(g^{-t})$, then $\pi^\vee \cong \pi_1$.
- suppose $n = 2$ and ω is the central character of π, then if $\pi_2 = \pi \otimes (\omega^{-1} \circ \deg)$, then $\pi^\vee \cong \pi_2$.

⌟

Proof: 1: It is clear that the character(18.1.5.27) of a representation is conjugation invariant, thus by(18.11.1.14) it is transpose invariant.

Now the character of π_1 is $\chi_1(\varphi) = \chi(\varphi'')$, where $\varphi''(g) = \varphi(g^{-t})$, and this equals $\chi(\varphi')$ where $\varphi'(g) = \varphi(g^{-1})$, because the character is transpose invariant. It is also clear that $\widehat{\varphi'} = \pi(\varphi)^t$ on a finite space V^K, then $\widehat{\chi}(\varphi) = \chi(\varphi') = \chi_1(\varphi)$, so by(18.1.5.32) $\pi \cong \pi_1$.

2: If $n = 2$, we use further the property that if $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, then

$$g^{-1} = (\deg g)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = (\deg g)^{-1} \begin{bmatrix} & 1 \\ -1 & \end{bmatrix} g^t \begin{bmatrix} & 1 \\ -1 & \end{bmatrix}^{-1}$$

then the assertion is clear using item1. □

Cor. (18.11.1.16). Let π be an admissible representation of $GL(n, K)$, then π is irreducible iff $\pi^\vee$ is irreducible. ⌟

Smooth Representations

Def. (18.11.1.17) [Twists]. Let $(\pi, V) \in \mathrm{Irr}^{\mathrm{adm}}(GL(n, K))$, for any quasi-character χ of $K^\times$, denote $\pi(\chi)$ the representation $\pi \otimes (\chi \circ \det)$. And for $s \in \mathbb{C}$, denote $\pi(s)$ the representation of π tensored by the 1-dimensional representation $g \mapsto |\det(g)|^s$ ⌟

Prop. (18.11.1.18) [Admissible Representation of $\mathbb{G}_m^N(K)$]. Any non-zero $(\pi, V) \in \mathrm{Rep}^{\mathrm{adm}}(\mathbb{G}_m^N(K))$ contains a 1-dimensional invariant subspace. ⌟

Proof: Consider the restriction on $\mathbb{G}_m^n(\mathcal{O}_K)$, by(18.1.5.25), $V = \oplus_{\chi \in \widehat{(\mathcal{O}_K^*)^k}} V_\chi$, and $\dim V_\chi < \infty$. As $(1, \ldots, \varpi, \ldots, 1)$ commutes with $\mathbb{G}_m^n(\mathcal{O}_F)$, it preserves V_χ for each χ. And these elements commute, so they have a common eigenvalue, which means V has a 1-dimensional invariant subspace. □

Lemma (18.11.1.19). Let $(\pi, V) \in \mathrm{Rep}^{\mathrm{alg}}(GL(n, K))$, then $\pi|_{G_n^0}$ splits into a finite direct sum of irreducible representations of G_n^0. ⌟

Proof: This follows from(18.1.2.11). □

Lemma (18.11.1.20). If $(\pi, V) \in \mathrm{Rep}^{\mathrm{alg}}(GL(n, K))$ satisfies V is generated by V^{K_m}, then for any submodule V', V' is generated by $V^N \cap V'$. ⌟

Proof: Cf.[B-Z76]P38. □

Prop. (18.11.1.21) [Irreducible Smooth Representation is Admissible]. For any connected reductive group G over a p-adic number field F, $\mathrm{Irr}^{\mathrm{alg}}(G(F)) = \mathrm{Irr}^{\mathrm{adm}}(G(F))$. ⌟

Proof: ? We only prove for $G = \mathrm{GL}(n)$.

By(18.11.2.9)(18.11.2.10) and(18.11.2.8), it suffices to prove for π quasi-cuspidal. But then this follows from(18.11.2.12)(18.11.1.19) and(18.1.5.48). □

Prop. (18.11.1.22)[Howe]. Let $(\pi, V) \in \mathrm{Rep}^{\mathrm{alg}}(GL(n,K))$, then π is of finite length iff it is admissible and f.g.. ⌟

Proof: A finite length representation is admissible by(18.11.1.21) and(18.1.5.24). For the converse, as V is f.g., take N compact open s.t. V is generated by V^N, and $\dim V^N < \infty$ as V is admissible. Then by(18.11.1.19): $V' \to V' \cap V^N$ is an injection from the set of subrepresentations of V to the set of subspaces of V^N, thus V is of finite length. □

Finite dimensional Representations

Prop. (18.11.1.23). Any $\pi \in \mathrm{Irr}^{\mathrm{adm}}(GL(2,K))$ has dimension 1. ⌟

Proof: By the no-small-subgroup argument, the kernel of this representation contains an open normal subgroup. But any open normal subgroup of $GL(2,V)$ contains $SL(2,V)$ by(18.11.1.12), thus this is a representation of $K^\times$, which must be of 1-dimensional by(18.11.1.18). □

Lemma (18.11.1.24) [2-Dimensional Smooth Representation of $K^\times$]. Any $\rho \in \mathrm{Rep}^{\mathrm{adm,dim}=2}(K^\times)$ is one of the following form:

- $\rho(t) = \mathrm{diag}(\xi(t), \xi'(t))$, where ξ, ξ' are two quasi-characters of $K^\times$.
- $\rho(t) = \xi(t)\begin{bmatrix} 1 & v(t) \\ & 1 \end{bmatrix}$, where ξ is a quasi-character of $K^\times$.

⌟

Proof: There exists a 1-dimensional invariant subspace spanned by x by(18.11.1.18), on which $K^\times$ acts by a quasi-character ξ, and consider the quotient space, on which $K^\times$ acts by a quasi-character ξ'. choose y that is linearly-independent of x, then $\rho(t)y = \xi'(t)y + \lambda(t)x$, and

$$\lambda(tu) = \xi'(u)\lambda(t) + \lambda(u)\xi(t)$$

which is symmetric in t, u.

If $\xi \neq \xi'$,

$$\lambda(t)(\xi(u) - \xi'(u)) = \lambda(u)(\xi(t) - \xi'(t))$$

therefore $\lambda(t) = C(\xi(t) - \xi'(t))$, so $z = y - Cx$ is fixed by $\rho(K^\times)$.

If $\xi - \xi'$, then λ/ξ is an additive character of $K^\times$, thus it is trivial on $\mathcal{O}^*$, so $\lambda(t) = cv(t)$. □

Zelevinsky Segments

Def. (18.11.1.25) [Zelevinsky Segments]. For $\pi \in \mathrm{Irr}^{\mathrm{adm}}(GL(n,K))$, a **Zelevinsky segment** $\Delta(\pi, m)$ is an ordered m-tuple $(\pi, \pi(1), \ldots, \pi(m-1))$ of cuspidal representations of $GL(n,K)$.

For two segments $\Delta(\pi_1, m)$ and $\Delta(\pi_2, n)$, $\Delta(\pi_1, m)$ **precedes** $\Delta(\pi_2, n)$ if $\Delta(\pi_1, m) \cap \Delta(\pi_2, n) = \varnothing$ and $(\Delta(\pi_1, m), \Delta(\pi_2, n))$ is another segment. They are called **linked segements** if one precedes another. ⌟

Def. (18.11.1.26) [Dual Segments]. For a segment $\Delta(\pi, m) = (\pi, \pi(1), \ldots, \pi(m-1))$, its **dual segment** $\Delta^\vee$ is the segment $(\pi^\vee(1-m), \pi^\vee(2-m), \ldots, \pi) = \Delta(\pi^\vee(1-m), m)$. ⌟

Def. (18.11.1.27) [$\pi(\Delta)$]. Let $\Delta = \Delta(\pi, m)$ be a Zelevinsky segment of length m and degree mn, we can define an admissible representation $\pi(\Delta)$ of $GL(mn, K)$ given by

$$\pi(\Delta) = \pi \times \pi(1) \times \ldots \times \pi(m-1) = I_{P(n,n,\ldots,n)}^{GL(mn,K)}(\otimes \pi_i)$$

⌟

Def. (18.11.1.28) [Zelevinsky Conditions]. A tuple of Zelevinsky segments $\Delta_1, \ldots, \Delta_r$ is said to satisfy the **Zelevinsky condition** if for each $i < j$, Δ_i doesn't precedes Δ_j. ⌟

2 Cuspidal Representations

Jacquet Functors

Def. (18.11.2.1) [Jacquet Functors]. Let $P = LU$ be a parabolic subgroup of G, if (π, V) be a representation of $G(F)$, then $V_U = V/(\text{span}\{\rho(u)v - v | u \in U\}) = V/V(U)$ is naturally a $L \cong P/U$ representation, so we can define the **Jacquet functor**:

$$J_P^G : \text{Rep}^{\text{alg}}(G(F)) \to \text{Rep}^{\text{alg}}(L(F)) : V \mapsto V_U.$$

Given a character ψ of $U(F)$, similarly $V_{U,\psi} = V/(\text{span}\{\rho(u)v - \psi(u)v | u \in U\}) = V/V(U,\psi)$ is a $Z(K)$-module, we can also define similarly the **twisted Jacquet functor**

$$J_{P,\psi}^G : \text{Rep}^{\text{alg}}(G(F)) \to \text{Rep}^{\text{alg}}(Z(K)) : V \mapsto V_{U,\psi}.$$

For convenience, define the **normalized Jacquet functor**: $r_P^G = \sqrt{\frac{\Delta_P}{\Delta_G}} \otimes J_P^G$.

$J_P^G, J_{P,\psi}^G, r_P^G$ are exact functors, by(18.1.2.4). ⌟

Prop. (18.11.2.2). For the the minimal parabolic subgroup $P = B(K)$, $J_{N,\psi_{a,N}}(V) \cong J_{N,\psi_U}(V)$ for $a \in \mathbb{G}_m^{n-1}(F) \times 1$. ⌟

Proof: This is because $\pi(a)$ maps $V(N, \psi_{a,N})$ isomorphically to $V(N, \psi_N)$, thus induces an isomorphism $J_{N(K),\psi_{a,N}}(V) \cong J_{N(K),\psi_N}(V)$. □

Prop. (18.11.2.3). $J_P^G, J_{P,\psi}^G, r_P^G$ map smooth representations of finite length to smooth representations of finite length(because it is f.g.). ⌟

Proof: If V is a f.g. G-module, then it is a f.g. P-module, because $G = PK$, and Kv_i is of f.d. for any $v \in V$. Thus the quotient V_U of V is also f.g..

For finite length**?**, Cf.[Bernstein-Zelevinsky2, P8]. □

Lemma (18.11.2.4) [Jacquet]. If (π, V) is a smooth representation of $GL(n, K)$, then using the notation as in(18.11.1.10), where $\mathfrak{a}$ is a proper ideal, V^{K_0} and $V^{N_-(\mathfrak{a})T_0}$ have the same image in the Jacquet module $J(V)$. ⌟

Proof: One inclusion is trivial, for the other, if $x \in V^{N_-(\mathfrak{a})T_0}$ then $x_1 = \int_{K_0} \pi(k)xdk$ lies in V^{K_0}, so it suffices to show x and x_1 have the same image in $J(V)$. But by(18.11.1.10)

$$x_1 = \int_{N_-(\mathfrak{a})} \int_{T_0} \int_{N(\mathcal{O})} \pi(nt_0n_-)xdndt_0dn_- = \int_{N(\mathcal{O})} \pi(n)xdn$$

and notice $p(\pi(n)x) = p(x)$. □

Prop. (18.11.2.5) [Jacquet Modules are Admissible]. Let (π, V) be a smooth representation of $GL(2,K)$, then

- Using the notation as in(18.11.1.10), if $\mathfrak{a}$ is a proper ideal, then the projection map $p : V \mapsto J(V)$ induces a surjection of $V^{K_0} \to J(V)^{T_0}$.
- If (π, V) is admissible, then $J(V)$ is also admissible representation of $T(F)$.

? For $GL(n,K)$ case, Cf.[Bernstein-Zelevinksy1, P33].? ⌟

Proof: 2 follows from 1 because we can choose $T_0 = T(\mathfrak{a})$ to be arbitrarily small, then it is of f.d., thus admissible.

For 1, notice fist that any $x \in J(V)^{T_0}$ is an image of a $x_1 \in V^{T_0}$, because $p(\pi(t)x) = \pi(t)p(x) = p(x)$, thus we can choose $x_1 = \frac{1}{V(T_0)}\int_{T_0} \pi(t)x dt$.

Thus for any f.d. subspace $\overline{U}$ of $J(V)^{T_0}$, we can find a f.d. $U \subset V^{T_0}$ that is mapped isomorphically onto $\overline{U}$. Now U is fixed by some $N_-(\mathfrak{p}^n)$ for n large, so U is fixed by $N_-(\mathfrak{p}^n)T_0$. Notice $\mathfrak{a} = \mathfrak{p}^m$ for some m, and

$$\pi(d)N_-(\mathfrak{p}^n)T_0\pi(d)^{-1} = N_-(\mathfrak{a})T_0, \quad d = \begin{bmatrix} \varpi^{n-m} & \\ & 1 \end{bmatrix},$$

so $\pi(d)U$ is stabilized by $N_-(\mathfrak{a})T_0$. Hence by lemma(18.11.2.4), $\pi(d)p(U) = p(\pi(d)U) \subset p(V^{K_0})$, so the dimension of $\overline{U}$ is bounded by dimension of V^{K_0}, so we can choose $\overline{U}$ just to be $J(V)^{T_0}$. Now $\pi(d)$ commutes with $T(F)$, so we have $\pi(d)J(V)^{T_0} = J(V)^{T_0} \subset p(V^{K_0})$. The reverse containment is clear. □

Parabolic Induction

Def. (18.11.2.6) [Parabolic Induction]. Let $P = LU$ be a parabolic subgroup of G, let $\mathrm{pr} : P \to P/U \cong L$, the **parabolic induction** functor I_P^G is the functor

$$I_P^G : \mathrm{Rep}^{\mathrm{alg}}(L) \to \mathrm{Rep}^{\mathrm{alg}}(G) : \rho \mapsto \mathrm{Ind}_P^G(\rho \circ \mathrm{pr})(18.1.5.34).$$

⌟

Prop. (18.11.2.7)[Parabolic Induction and Jacquet Functor]. For any parabolic subgroup P, I_P^G is right adjoint to the normalized Jacquet functor r_P^G. ⌟

Proof: For $\sigma \in \mathrm{Rep}^{\mathrm{alg}}(L), \rho \in \mathrm{Rep}^{\mathrm{alg}}(G)$,

$$\mathrm{Hom}_{P/U}(\sqrt{\frac{\Delta_P}{\Delta_G}} \otimes (\mathrm{res}_P^G(\sigma))_U, \rho) \cong \mathrm{Hom}_P(\mathrm{res}_P^G(\sigma), \sqrt{\frac{\Delta_G}{\Delta_P}} \otimes (\rho \circ \mathrm{pr})) = \mathrm{Hom}_G(\sigma, \mathrm{Ind}_P^G(\rho \circ \mathrm{pr})).$$

□

Prop. (18.11.2.8). I_P^G maps admissible representations to admissible representations and maps finite length representations to finite length representations. ⌟

Proof: By(18.1.5.44) and Iwasawa decomposition.

For finte length? □

Cuspidal Representation

Main references are [The Local Langlands Correspondence: The non-Archimedean case, 1994], [Induced Representations of Reductive p-Adic Groups, Berstein Zelevinsky].

Def. (18.11.2.9) [Cuspidal Representations]. $(\pi, V) \in \mathrm{Rep}^{\mathrm{alg}}(G(F))$ is called a **quasi-cuspidal representation** if for any proper parabolic subgroup $P = LU$ of G, $r_P^G(V) = 0$. A **cuspidal representation** is a representation that is both quasi-cuspidal and admissible. The category of cuspidal representations is denoted by $\mathrm{Rep}^{\mathrm{cusp}}(G(F))$. ⌟

Prop. (18.11.2.10) [Cuspidal Dichotomy]. If $\pi \in \mathrm{Irr}^{\mathrm{alg}}(G(F))$, then either π is (quasi-)cuspidal, or π is a subrepresentation of $I_P^G(\rho)$, where $P = LU$ is a proper parabolic subgroup of G, and $\rho \in \mathrm{Irr}^{\mathrm{alg}}(L(F))$ is (quasi-)cuspidal. ⌟

Proof: If π is not (quasi-)cuspidal, choose a minimal parabolic P that $r_P^G(\pi) \neq 0$. As $r_P^G(\pi)$ is f.g.(18.11.2.3), by(18.1.2.8), it has an irreducible subquotient σ. Then

$$0 \neq \mathrm{Hom}_M(r_P^G\pi, \sigma) = \mathrm{Hom}_G(\pi, I_P^G\sigma).$$

And by minimality, σ is (quasi-)cuspidal by(18.11.2.5). □

Prop. (18.11.2.11) [Representation from Finite Case]. Let (π_0, V_0) be an irreducible cuspidal representation of $GL(2, \mathbb{F}_q)$, then it is representation of $\mathscr{K}$ by the projection $\mathscr{K} \to GL(2, \mathbb{F}_q)$, with central character ω_0. Extend ω_0 to a character ω of $K^\times$, then extend π_0 to a representation of $\mathscr{K}Z(K)$ with central character ω. Finally let $(\pi, V) = \mathrm{ind}_{\mathscr{K}Z(K)}^{GL(2,K)} \pi_0$. Then π is a unitarizable cuspidal irreducible admissible representation of $GL(2, K)$. ⌟

Proof: To show it is admissible, we use Mackey's intertwining formula(18.1.5.43). By(18.1.5.25), it suffices to show for any $\rho\,\mathrm{ind}\,\mathrm{Irr}^{\mathrm{adm}}(\mathscr{K})$, $\dim \mathrm{Hom}_{\mathscr{K}}(\pi_0, \rho) < \infty$. By p-adic Cartan decomposition(18.1.5.43), a representative set for $\mathscr{K}\backslash G/\mathscr{K}Z(K)$ is $\{\begin{bmatrix} 1 & \\ & \varpi^n \end{bmatrix}, 0 \leq n \in \mathbb{Z}\}$. Notice π_0 is of f.d., thus it suffices to show that only f.m. $\mathrm{Hom}_{K_0(\mathfrak{p}^n)}(\pi_0, \rho^{\varpi^n}) \neq 0$. For this, notice that by continuity, for n large, $\rho^{\varpi^n}(\begin{bmatrix} 1 & b \\ & 1 \end{bmatrix}) = \mathrm{id}$ for any $b \in \mathcal{O}$, thus any $\varphi \in \mathrm{Hom}_{K_0(\mathfrak{p}^n)}(\pi_0, \rho^{\varpi^n}) \neq 0$ factors through the Jacquet module of π, which is 0 as π_0 is cuspidal.

By(18.1.5.45), π is unitarizable. And then by(18.1.5.46), it suffices to show that $\dim \mathrm{End}(\pi) = 1$. By Mackey theory again,

$$\mathrm{Hom}_G(\pi, \pi) \subset \mathrm{Hom}_G(\pi, \mathrm{Ind}_{\mathscr{K}Z(K)}^{GL(2,K)} \pi_0) = \prod_{n \geq 0} \mathrm{Hom}_{K_0(\mathfrak{p}^n)}(\pi_0, \rho^{\varpi^n})$$

by the same reason as above, for $n > 0$, this is 0, and for $n = 0$, this has dimension 1 because π_0 is an irreducible representation of K.

It remains to show π is cuspidal: Use Mackey theory again. By Iwasawa decomposition, a representative set for $\mathscr{K}\backslash G/\mathscr{K}Z(K)$ is $\{\begin{bmatrix} 1 & \\ & \varpi^n \end{bmatrix}, 0 \leq n \in \mathbb{Z}\}$. Now it suffices to show $\mathrm{Hom}_{\mathrm{Unip}(2,K)}(\pi_0, 1) = 0$. But this is because π_0 is cuspidal. □

Thm. (18.11.2.12) [Harish-Chandra]. then for $(\pi, V) \in \mathrm{Rep}^{\mathrm{alg}}(GL(n, K))$, the following are equivalent:

- π is quasi-cuspidal.
- For any principal congruence subgroup $\mathcal{K}_m$, the function $D_{\xi,K}: G \to V : g \mapsto \pi(e_K)\pi(g^{-1})\xi$ has compact support modulo $Z(K)$.
- Every matrix coefficient of π is compactly supported modulo $Z(K)$.
- The restriction of π to G_n^0 is compact.

⌟

Proof: 2 → 3 is verbatim as that of(18.1.5.48), 3 → 4 is easy. 4 → 2 follows from the definition of compact representations and the fact $GL(n,K)/G_n^0 Z(K)$ is finite.

1 $\iff$ 2: Cf.[Bernstein-Zelevinsky, P34].**?** □

Cor. (18.11.2.13) [Contragradient of Cuspidal Representations]. For $\pi \in \mathrm{Rep}^{\mathrm{cusp}}(GL(n,K))$, $\widehat{\pi} \in \mathrm{Rep}^{\mathrm{cusp}}(GL(n,K))$ too. ⌟

3 Whittaker Models

Def. (18.11.3.1) [Whittaker Functionals & Whittaker Models]. For $(\pi, V) \in \mathrm{Irr}^{\mathrm{alg}}(GL(n,K))$,

- a **Whittaker functional** on V is a $\mathrm{Unip}(n,K)$-map $\lambda : V \to \psi_N$.(Compare with(20.1.3.9).)
- a **Whittaker model** is a subrepresentation of $\mathrm{Ind}_{\mathrm{Unip}(n,K)}^{GL(n,K)}(\psi_N)$ that is isomorphic to π and consists of functions φ of moderate growth.

An irreducible smooth representation having a Whittaker functional is called a **generic representation**. ⌟

Remark (18.11.3.2). Generic representations are important because for any global number field F and $\pi \in \mathrm{Irr}^{\mathrm{auto}}(\mathrm{GL}(n)/F)$, all the local components π_v are generic, by(20.5.3.7).

Whittaker models are important because we can use it to attach local Euler factors for such representations. ⌟

Prop. (18.11.3.3).

- The definition of generic is independent of ψ, by(18.11.2.2).
- π is generic iff $\pi^\vee$ is generic.**?**
- For a quasi-character χ of $K^\times$, π is generic iff $\pi(\chi)$ is generic, as $J_{\mathrm{Unip}(n,K),\psi_N}(\pi) = J_{\mathrm{Unip}(n,K),\psi_N}(\pi(\chi))$.

⌟

Prop. (18.11.3.4) [Transpose Invariant Distribution]. If $\Delta \in \mathcal{D}(GL(n,K))$ is a distribution that satisfies

$$\lambda(u)\Delta = \psi_N(u)^{-1}\Delta, \quad \rho(u)\Delta = \psi_N(u)\Delta,$$

where ψ is defined in(20.1.3.9), then Δ is stable under involution $\iota : GL(n,K) \to GL(n,K) : \iota(g) = w^0 g^t w^0$(18.11.0.1). ⌟

Proof: Firstly notice that ι fixes $N(K)$, and $\psi_N(\iota(g)) = \psi_N(g)$, so $\iota(\Delta)$ also satisfies these equations, so we can replace Δ by $\Delta - \iota(\Delta)$, then assume $\iota(\Delta) = -\Delta$ and prove $\Delta = 0$.

Consider the group G that is a semi-direct product

$$1 \to N(K) \times N(K) \to G \to \mathbb{F}_2$$

and $\iota\in\mathbb{F}_2$ acts on $N(K)\times N(K)$ by $(u_1,u_2)\mapsto(\iota(u_2)^{-1},\iota(u_1)^{-1})$.

Define a character χ on G by $\chi((u_1,u_2))=\psi_N(u_1)^{-1}\psi_N(u_2),\chi(\iota)=-1$, then G acts on $GL(n,K)$ by

$$\sigma((u_1,u_2))=\lambda(u_1)\rho(u_2),\quad \sigma(\iota)=\iota$$

then the conditions are summarized into a single condition:

$$\sigma(g)\Delta=\chi(g)\Delta.$$

We only prove for $n=2$:**?**

Consider the action of $N(K)\times N(K)$ on $GL(2,K)$ by left-right action, then we can use(18.1.5.10) and(18.1.5.11), because the action is constructive, by(9.2.1.23), and $\iota N(K)\iota=N(K)$, and ι preserves orbits except for $\mathrm{diag}\{a,d\},a\neq d$.

But there are no desired distribution on this orbit: this orbit is homeomorphic to $N(K)$ via $u\mapsto u\mathrm{diag}(a,d)$, and the distribution is transferred to a left invariant distribution, thus by(18.1.5.4) it is just the Haar measure

$$\Delta(f)=c_1\int_{N(K)}f(u\begin{bmatrix}a&b\\&d\end{bmatrix})\psi_N(u)du.$$

We notice using a right-invariant version of(18.1.5.4) that

$$\Delta(f)=c_2\int_{N(K)}f(\begin{bmatrix}a&b\\&d\end{bmatrix}u)\psi_N(u)du=c_2\int_{N(K)}f(u\begin{bmatrix}a&b\\&d\end{bmatrix})\psi_N(\begin{bmatrix}a&b\\&d\end{bmatrix}^{-1}u\begin{bmatrix}a&b\\&d\end{bmatrix})du$$

as $N(K)$ is unimodular. Notice now $c_1\psi_N(u)=c_2\psi_N(\begin{bmatrix}a&b\\&d\end{bmatrix}^{-1}u\begin{bmatrix}a&b\\&d\end{bmatrix})$ cannot happen for all u, as this implies $c_1=c_2$ by choosing $u=I$, and then $\psi(x)=\psi(ax/d)$, which is impossible by(11.10.3.35). So if some u this is not equal, then we find a function supported at a nbhd of u, then this two distributions cannot be equal. □

Prop. (18.11.3.5)[Local Multiplicity One Theorem]. For $(\pi,V)\in\mathrm{Irr}^{\mathrm{adm}}(GL(n,K))$, the space of Whittaker functionals has dimension≤ 1. ⌟

Proof: Define another representation $\pi'(g)=\pi(\iota(g)^{-1})$, then this representation is isomorphic to π_1 defined in(18.11.1.15)($\pi(w^0)$ is an isomorphism), which is isomorphic to the contragradient of π, so there is a pairing on V that

$$(\pi(g)\xi,\eta)=(\xi,\pi(\iota(g))\eta).$$

Now for any smooth functional Λ, there is an element $[\Lambda]$ that $(\xi,[\Lambda])=\Lambda(\xi)$.

Now for any linear functional Λ on V and $\varphi\in\mathcal{H}_G$, we can define another smooth linear function $(\Lambda*\varphi)(\xi)=\Lambda(\pi(\varphi)\xi)$. Then clearly $\varphi*(\varphi_1*\varphi_2)=(\Lambda*\varphi_1)*\varphi_2$. We need the following lemma:

Lemma (18.11.3.6).

- $\pi(g)[\Lambda*\varphi]=[\Lambda*\rho(\iota(g)^{-1})\varphi]$.
- If L is a smooth functional, $[L*\varphi]=\pi(\iota(\varphi))[L]$.
- If L is a Whittaker functional, $[\Lambda*\lambda(u)\varphi]=\psi_N(u)[\Lambda*\varphi]$.

⌟

Proof: 1:

$$(\xi,\pi(g)[\Lambda*\varphi])=(\pi(\iota(g))\xi,[\Lambda*\varphi])=(\Lambda*\varphi)(\pi(\iota(g))\xi)$$
$$=\int_G\Lambda(\pi(h)\pi(\iota(g))\xi)\varphi(h)dh=\int_G\Lambda(\pi(h)\xi)\varphi(h\iota(g)^{-1})dh=(\xi,[\Lambda*\rho(\iota(g)^{-1})\varphi]).$$

2: $(\xi,[L*\varphi])=(L*\varphi)(\xi)=L(\pi(\varphi)\xi)=(\pi(\varphi)\xi,[L])=(\xi,\pi(\iota(\varphi))[L])$.

3:

$$(\xi,[\Lambda*\lambda(u)\varphi])=(\Lambda*\lambda(u)\varphi)(\xi)=\int_G\Lambda(\pi(g)\xi)\varphi(u^{-1}g)dg$$
$$=\int_G\Lambda(\pi(u)\pi(g)\xi)\varphi(g)dg$$
$$=\psi_N(u)(\Lambda*g)(\xi)=\psi_N(u)(\xi,[\Lambda*\varphi])$$

□

Now if Λ_1,Λ_2 are two Whittaker functionals, we will show they are propositional: we define a distribution Δ on G that $\Delta(\varphi)=\Lambda_1([\Lambda_1*\varphi])$, then by the lemma above, (18.11.3.4) can be applied to $\overline{\Delta}$ so we have $\Delta=\iota(\Delta)$.

Next we show for any linear functional Λ, $V=\{[\Lambda*\varphi]|\varphi\in\mathcal{H}\}$: Notice the RHS is G-invariant by(18.11.3.6), and it is not empty by smoothness technique. To go further, need another lemma:

Lemma (18.11.3.7). If $\varphi\in\mathcal{H}$ satisfies $\Lambda_1*\varphi=0$, then $\Lambda_2*\varphi=0$. ⌟

Proof: Firstly, all $\Lambda_1*\pi(g)\varphi=0$, which follows from(18.11.3.6) item1. Hence,

$$\Lambda_2([\Lambda_1*\lambda(g)\iota(\varphi)])=\Delta(\iota(\rho(\iota(g)^{-1})\varphi)\varphi)=\Delta(\rho(\iota(g)^{-1})\varphi)=\Lambda_2([\Lambda_1*\rho(\iota(g)^{-1})\varphi])=0.$$

hence by linearity, for any $\sigma\in\mathcal{H}$, $\Lambda_2([\Lambda_1*\sigma*\iota(\varphi)])=0$, which by(18.11.3.6) item2 is equivalent to $\Lambda_2(\pi(\varphi)[\Lambda_1*\varphi])=0=(\Lambda_2*\varphi)[\Lambda_1*\varphi]$, because $\Lambda_1*\sigma$ is smooth. But we know $[\Lambda*\varphi]$ can be any $v\in V$, thus $\Lambda_2*\varphi=0$. □

By the lemma, we can define a map $T:V\to V:T([\Lambda_1*\varphi])=[\Lambda_2*\varphi]$, which is a G-homomorphism by(18.11.3.6), and it is defined on all of V, so $T\xi=c\xi$ for some c, then we see $\Lambda_2=c\Lambda_1$, by a smoothness technique. □

Cor. (18.11.3.8) [Local Multiplicity One]. For $(\pi,V)\in\mathrm{Irr}^{\mathrm{alg}}(GL(n,K))$, there exists at most one Whittaker model for π. ⌟

Proof: A Whittaker model is equivalent to a $GL(n,K)$-homomorphism $V\to\mathrm{Ind}_{\mathrm{Unip}(n,K)}^{GL(n,K)}(\mathbb{C}_{\psi_N})$, which by smooth Frobenius reciprocity(18.1.5.37) is equivalent to a $N(K)$-homomorphism $V\to\mathbb{C}_{\psi_N}$, which is just a Whittaker functional. So this proposition is equivalent to(18.11.3.5). □

Prop. (18.11.3.9). A Whittaker functional for (π,V) is the same as a linear functional on $J_{\mathrm{Unip}(n,K),\psi_N}(V)$. ⌟

Cor. (18.11.3.10). For $(\pi,V)\in\mathrm{Irr}^{\mathrm{adm}}(GL(n,K))$, $\dim J_{\mathrm{Unip}(n,K),\psi_N}(V)\le 1$, by(18.11.3.5). ⌟

Existence of Whittaker Models

Def. (18.11.3.11) [Sheaf on F associated to V]. As $\mathrm{Unip}(2) \cong \mathbb{A}^1$, any smooth representation V of $\mathrm{Unip}(2, K)$ corresponds to a smooth $\mathcal{H}(F)$-module by(18.1.5.16), thus we can view it as a $C_c^\infty(F)$-module by

$$\varphi(v) = \int_{\mathrm{Unip}(2,K)} \widehat{\varphi}(x)\pi(u)v dx.$$

Then this module is smooth thus non-degenerate by(18.1.5.16), then we can define $\mathcal{S}(V)$ the sheaf associated to V, as in(4.4.4.14). ⌟

Cor. (18.11.3.12). Let V be a smooth $B(K)$-sheaf and let $a \in K$, then the stalk

$$\mathcal{S}(V)_a \cong \begin{cases} J(V) & a = 0 \\ J_{\psi_a}(V) \cong J_\psi(V) & a \neq 0 \end{cases}.$$

⌟

Proof: By definition(4.4.4.14), the stalk is V modulo the subgroup consisting of elements v that $\chi_U \cdot v = 0$, where $U = a + \mathfrak{p}^k$ for some large k. Back the definition of $\mathcal{S}(V)$, consider the Fourier transform

$$\widehat{\chi_{a+\mathfrak{p}^k}}(x) = \overline{\psi(ax)} V(\mathfrak{p}^k)\chi_{\mathfrak{p}^{n-k}}(x)$$

where $\mathfrak{p}^n$ is the conductor of ψ. Thus

$$\chi_{a+\mathfrak{p}^k} v = C \int_{\mathfrak{p}^{n-k}} \overline{\psi(ax)}\pi(\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix})v dx = 0$$

for large k, which is equivalent to $v \in V_{N,\psi_a}$ by(18.1.2.6). Finally, $J_{\psi_a}(V) \cong J_\psi(V)$ by(18.11.2.2). □

Cor. (18.11.3.13) [Existence of Whittaker Functional]. $(\pi, V) \in \mathrm{Rep}^{\mathrm{adm}}(\mathrm{GL}(2, K))$ has a Whittaker functional unless it factors through the determinant map. In particular, if π is irreducible, then $\dim J_\psi(V) = 1$ iff it is not 1-dimensional, or to say, it is ∞-dimensional. ⌟

Proof: The existence of a Whittaker functional is equivalent to the fact $J_\psi(V) \neq 0$, which is the stalk of the sheaf $\mathcal{S}(V)$. If it vanishes, then $\mathcal{S}(V)$ is a skyscraper sheaf by(18.11.3.12), and by the correspondence of $\mathcal{S}(V)$ and V(4.4.4.14), V equals $\Gamma(F, \mathcal{S}(V)) = J(V)$, thus $\mathrm{Unip}(2, K)$ acts trivially on V.

So also all the conjugates of $\mathrm{Unip}(2, K)$ acts trivially, so $SL(2, K)$ acts trivially, by5, thus the representation factors through the quotient $K^\times$, the rest is clear.

Finally, if it is irreducible, then it factors through the determinant map iff $V \cong \mathbb{C}$ and $\pi(g) = \chi(\det(g))$, by(18.11.1.18). So $J_\psi(V) = 0$ as ψ is non-trivial. □

Prop. (18.11.3.14) [GL(n) Case]. In fact, $\pi = Q(\Delta_1, \ldots, \Delta_k) \in \mathrm{Irr}^{\mathrm{adm}}(GL(n, K))$ is generic iff no two of Δ_i are linked, in which case

$$\pi = Q(\Delta_1) \times \ldots \times Q(\Delta_k).$$

In particular, π is generic iff its Gelfand-Kirillov dimension is maximal among those irreducible admissible representations with the same cuspidal supports. ⌟

Proof: Cf.[Induced Representations of Reductive p-Adic Groups, Zelevinsky(1980)].? □

Kirillov Model

Def. (18.11.3.15) [Kirillov Model]. For $(\pi, V) \in \mathrm{Irr}^{\mathrm{alg}}(GL(n,K))$, a **Kirillov model** $\mathcal{K}(\pi)$ is a subrepresentation of $\mathrm{Ind}_{\mathrm{Unip}(n,K)}^{P_{n-1,1}(F)}(\psi)$ that is isomorphic to $\pi|_{B_1(F)}$, and consist of functions on $B_1(F)$ that φ is compactly supported on T_1(Notice this condition is automatic by(18.11.3.19)).

When $n = 2$, it is equivalently a subspace of $C^\infty(K^\times)$ with an action of $B_1(F)$ that satisfies

$$[\pi(\begin{bmatrix} a & b \\ & 1 \end{bmatrix})\varphi](x) = \psi(bx)\varphi(ax)$$

and isomorphic to (π, V) via the isomorphism $v \mapsto \varphi_v$. ⌟

Proof: The last assertion is because $B_1(F) = \mathrm{Unip}(2,K)T_1(F)$, thus the value of a function in $\mathrm{Ind}_{N(K)}^{B_1(F)}(\psi)$ is determined by its restriction on $T_1(F) \cong K^\times$. □

Prop. (18.11.3.16). The action of $B_1(F)$ on $C_c^\infty(K^\times)$ as defined in(18.11.3.15) is irreducible. ⌟

Proof: Let U be a non-zero invariant subspace of $C_c^\infty(K^\times)$, we will show that for any $a \in K^\times$, U contains χ_U for any sufficiently small nbhd U of a. Let $\varphi \in U$ and $\varphi(b) \neq 0$, then by action of $\begin{bmatrix} b/a & \\ & 1 \end{bmatrix}$, we may assume $\varphi(a) \neq 0$.

If $f \in C_c^\infty(F)$, f acts on φ via

$$\pi(f)\varphi = \int_F f(x)\pi(\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix})\varphi dx,$$

which in fact a finite sum of elements in $N(K)v$. Then $\pi(f)\varphi(y) = \int_F f(x)\psi(xy)\varphi(y)dx = \widehat{f}(y)\varphi(y)$. By the isomorphism $\mathcal{H}_{\mathcal{F}} \cong C_c^\infty(F)$(18.1.5.19), we can choose f that $\widehat{f} = \varphi(a)^{-1}\chi_U$ for a small nbhd U of a that φ is constant on U, then $\pi(f)\varphi = \chi_U$. □

Lemma (18.11.3.17). For $(\pi, V) \in \mathrm{Irr}^{\mathrm{adm}}(GL(2,K))$, if $\dim V = \infty$, then $V^{\mathrm{Unip}(2,F)} = 0$. ⌟

Proof: Cf.[Bump, P464]**?**

The stabilizer of v is open, thus by(18.11.1.12) it is fixed by all $SL(2,K)$. Also it is fixed by the center $Z(K)$. Now $GL(2,K)/SL(2,K)Z(K) \cong K^\times/(K^\times)^2$ which is finite by(14.2.3.6), thus the invariant subspace generated by v is of f.d., contradiction. □

Lemma (18.11.3.18). If $(\pi, V) \in \mathrm{Irr}^{\mathrm{adm}}(GL(2,K))$, and Λ is a Whittaker functional on V, then for $v \neq 0 \in V$, there exists some $a \in K^\times$ that $\Lambda(\pi(\begin{bmatrix} a & \\ & 1 \end{bmatrix})v) \neq 0$. ⌟

Proof: For any $a \in K^\times$, it is clear that the kernel of the map $v \mapsto \Lambda(\pi(\begin{bmatrix} a & \\ & 1 \end{bmatrix})v)$ contains V_{N,ψ_a}**??** but by local multiplicity one(18.11.3.5), $\dim J_{\psi_a}(V) \leq 1$, and this map is non-trivial because Λ is non-trivial, thus the kernel is exactly V_{N,ψ_a}.

Thus if $\Lambda(\pi(\begin{bmatrix} a & \\ & 1 \end{bmatrix})v) = 0$, then v is the section of $\mathcal{S}(V)$ that vanishes at all $a \neq 0$, thus for any $x \in F$, $v' = v - \pi(\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix})v$ vanishes at every $a \in F$, thus $v' = 0$. Then $v = 0$ by(18.11.3.17). □

Prop. (18.11.3.19) [Kirillov Model and Whittaker Model]. For $(\pi, V) \in \mathrm{Irr}^{\mathrm{adm}}(GL(2,K))$, if it has a Whittaker functional Λ, then it has a Whittaker model $\mathcal{W}$ consisting of functions $W_v(g) = \Lambda(\pi(g)v)$, and we can define functions on $K^\times$ by

$$\varphi_v(a) = W_v(\begin{bmatrix} a & \\ & 1 \end{bmatrix}).$$

Then G acts on $\mathcal{K}(\pi)$ by acting on the subscript. Then it is a Kirillov model for V, and consists of functions that is compactly supported on F.

Conversely, if $\{\varphi_v | v \in V\}$ is a Kirillov model for (π, V), then we can construct functions on $GL(2,K)$ by $W_v(g) = \varphi_{\pi(g)v}(1)$. Then this is a Whittaker model for V. ⌟

Proof: The equations can be checked by hand. To given an action $\pi(\varphi_v) = \varphi_{\pi(g)v}$ on $\{\varphi_v | v \in V\}$, we need to show that $W_v \mapsto \varphi_v$ is injective, which is true by(18.11.3.18). Then $v \mapsto \pi_v$ is an isomorphism.

It remains to show that $\varphi_v \in C_c^\infty(K^\times)$. As π is a smooth representation, for any v, W_v is stable under $N(\mathfrak{p}^k)$ for some k, thus by equation above, $\varphi_v(a) = \psi_a(n)\varphi_v(a)$ for all a and $n \in N(\mathfrak{p}^k)$. Then if $|a|$ is sufficiently large, $\psi_a(n) \neq 0$ for some $n \in N(\mathfrak{p}^k)$, implying $\varphi_v(y) = 0$. □

Prop. (18.11.3.20) [Kirillov Model and Jacquet Functor]. Let V be a generic irreducible admissible representation of $GL(2,K)$, thus having a Kirillov model by(18.11.3.19), thus we can identify V with a space of functions on $K^\times$, and there is an exact sequence of vector spaces

$$0 \to C_c^\infty(K^\times) \to \mathcal{K}(\pi) \to J_{\mathrm{Unip}(2,K)}(\pi) \to 0.$$

⌟

Proof: V_N is generated by elements of the form $v' = \pi(\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix})v - v$. Notice $\varphi_{v'}(y) = (\psi(xy) - 1)\varphi_v(y)$, as ψ is continuous, when $|y|$ is small, $\varphi_{v'}(y) = 0$.

To show that if $C_c^\infty(K^\times) \subset V_N$, notice V_N is non-zero, because $\dim V = \infty$ but $\dim J(V)$ is finite(18.11.4.20). Notice V_N is stable under $B(K)$ action, thus it must be $C_c^\infty(K^\times)$ by(18.11.3.16). □

Prop. (18.11.3.21). If (π, V) is an irreducible generic admissible representation of $GL(2,K)$ thus having a Kirillov model. If χ is a quasi-character of $T(F)$ that $\pi(t)\overline{\varphi}_v = (\delta^{1/2}\chi)(t)\overline{\varphi}_v \in J(V)$, then for $|t|$ small, $\varphi_v(t)$ is a constant multiple of $|t|^{1/2}\chi_1(t)$. ⌟

Proof: Let $t_0 \in \mathfrak{p}\backslash\mathfrak{p}^2$, then

$$\pi(\begin{bmatrix} t_0 & \\ & 1 \end{bmatrix})\varphi - |t_0|^{1/2}\chi_1(t_0)\varphi \in V_N,$$

thus by(18.11.3.20), there exists some $\varepsilon(t_0) > 0$ that

$$\varphi(tu) - |t|^{1/2}\chi_1(t)\varphi(u) = 0$$

for $t = t_0$ and $|u| \le \varepsilon(t_0)$. Because both sides are locally constant on t, by the compactness of $\mathfrak{p}\backslash\mathfrak{p}^2$, there exists some $\varepsilon > 0$ that for the equation is true for all $t \in \mathfrak{p}\backslash\mathfrak{p}^2$ and $|u| \le \varepsilon$.

Now any element $t \in \mathfrak{p}$ can be factored into product of elements in $\mathfrak{p}\backslash\mathfrak{p}^2$, so by induction this is true for any $t \in \mathfrak{p}$. Thus we are done. □

Lemma (18.11.3.22) [Gelfand Uniqueness Principle]. Let $(\pi, V) \in \mathrm{Irr}^{\mathrm{adm}}(GL(2,K))$, and let χ be a quasi-character of $K^\times$, then there are at most two essentially different values of s that there are at least two linear functionals $L : V \to \mathbb{C}$ that satisfies

$$L(\pi(\begin{bmatrix} y & \\ & 1 \end{bmatrix})v) = \chi(y)|y|^s L(v).$$

⌟

Remark (18.11.3.23). In fact, for any s, there exists at most one such linear functional**?**. ⌟

Proof: If $\dim V = 1$, this is trivial. Otherwise $\dim V = \infty$ and (π, V) has a Kirillov model. Identify V with its Kirillov model. Suppose L_1, L_2 are two linear functionals that satisfies the equation, consider their restriction to $V_N = C_c^\infty(K^\times)$, on which $B_1(F)$ acts, thus L_1, L_2 are linearly dependent when restricted to V_N by(18.1.5.5). Thus there exists constants c_1, c_2 that $c_1L_1 + c_2L_2$ factors through $J(V)$. $\dim J(V) \leq 2$ by(18.11.4.20). So by(18.11.1.24) for all but two possible choices of s, $c_1L_1 + c_2L_2 = 0$, thus there are two linear functionals only for possibly two choices of s. □

4 Bernstein-Zelevinsky Classification

Thm. (18.11.4.1) [Bernstein-Zelevinsky].

1. For any Zelevinsky segment Δ of length m, the representation $\pi(\Delta)$ has length 2^{m-1}.
2. Let Δ be a Zelevinsky segment, then $\pi(\Delta)$ has a unique irreducible subrepresentation $Z(\Delta)$ and a unique irreducible quotient representation $Q(\Delta)$.
3. Let $(\Delta_1, \ldots, \Delta_r)$ be a tuple of Zelevinsky segments satisfying the Zelevinsky condition(18.11.1.28), then $Q(\Delta_1) \times \ldots \times Q(\Delta_r) \in \mathrm{Rep}^{adm}(GL(\sum n_i m_i, F))$ admits a unique irreducible quotient $Q(\Delta_1, \ldots, \Delta_r)$. Moreover, $Q(\Delta_1, \ldots, \Delta_r)$ is independent of the order of $\Delta_1, \ldots, \Delta_r$(also need to satisfy the Zelevinsky condition).
4. Any irreducible representation (π, V) of $GL(n, K)$ is isomorphic to one of the form $\pi \cong Q(\Delta_1, \ldots, \Delta_r)$ where $\Delta_i = \Delta(\pi_i, m_i)$ and $\sum n_i m_i = n$. for a unique tuple of segments $(\Delta_1, \ldots, \Delta_r)$ satisfying Zelevinsky condition up to permutation.
5. Let $(\Delta_1, \ldots, \Delta_r)$ be a tuple of segments satisfying the Zelevinsky condition, then $Q(\Delta_1, \ldots, \Delta_r)$ is irreducible iff no two elements are linked.
6. $Q(\Delta_1, \ldots, \Delta_r)^\vee = Z(\Delta_1^\vee, \ldots, \Delta_r^\vee)$.
7. Dual statement of item$3-6$ holds for $Z(\Delta_1) \times \ldots \times Z(\Delta_r)$, which admits a unique irreducible subrepresentation $Z(\Delta_1, \ldots, \Delta_r)$.

⌟

Proof: □

Cor. (18.11.4.2) [Principal Series]. $\mathcal{B}(\chi_1, \chi_2)$ is irreducible except the following two cases:

- If $\chi_2 = \chi_1(1)$, then $\mathcal{B}(\chi_1, \chi_2)$ has a 1-dimensional invariant subspace and the quotient representation is irreducible.
- If $\chi_2 = \chi_1(-1)$, then $\mathcal{B}(\chi_1, \chi_2)$ has an irreducible invariant subspace of codimension 1.

In these cases, the infinity-dimensional irreducible representations are called the **Steinberg representations** $\sigma(\chi_1, \chi_2)$, and the one-dimensional representation is denoted by $Z(\chi_1, \chi_2)$. ⌟

Proof: Firstly we prove if $\mathcal{B}(\chi_1,\chi_2)$ has a non-trivial subspace, then it has a non-trivial subspace of dimension 1 or codimension 1: Let V' be the invariant subspace and V'' the quotient space, by the exactness of Jacquet functor(18.11.2.1) and(18.11.3.10), at least one of $J_\psi(V'), J_\psi(V'')$ vanishes. If $J_\psi(V')=0$, then by(18.11.3.13) it factors through the determinant map, thus it has a 1-dimensional invariant space. If $J_\psi(V'')=0$, then we can use(18.11.4.9) and(18.1.5.21) to dualize.

Next, if $\mathcal{B}(\chi_1,\chi_2)$ has a 1-dimensional subspace $V=\{f\}$, then $\pi(g)f=\rho(\det(g))f$ for some quasi-character ρ of $K^\times$. Now consider the fact $f\in\mathcal{B}(\chi_1,\chi_2)$, take $b=\mathrm{diag}(y,y^{-1})$, then $(\delta^{1/2}\chi)(b)=1$, showing $\chi_1\chi_2^{-1}=|\cdot|^{-1}$. The codimension1 case is dual by(18.1.5.21) and(18.11.4.9), so $\mathcal{B}(\chi_1,\chi_2)$ is irreducible except when $\chi_1\chi_2^{-1}=|\cdot|^{\pm 1}$.

Finally, if $\chi_1\chi_2^{-1}=|\cdot|^{-1}$, let $\chi_1=\chi|\cdot|^{-1/2}$, then $f(g)=\chi(\det(g))$ is an invariant 1-dimensional subspace, and this is the only 1-dimensional invariant subspace that factors through the determinant map, because if $f(g)=\chi'(\det(g))\in\mathcal{B}(\chi_1,\chi_2)$, then $\chi'=\chi_1|\cdot|^{1/2}=\chi_2|\cdot|^{-1/2}=\chi$.

Also the quotient representation is irreducible because the same argument by Jacquet module shows if it is non-irreducible, then it has an invariant subspace of dimension 1 that G action factors through the determinant map or of codimension 1, which means there are two invariant 1-dimensional subspace that the G-action factors through the determinant map, or a invariant subspace of codimension1 of $\mathcal{B}(\chi_1,\chi_2)$, the latter case contradicting the argument above. For the former case, we get a 2-dimensional subrepresentation of $\mathcal{B}(\chi_1,\chi_2)$ that factors through the determinant map. The argument above shows it is generated by $\chi(\det())$ and some function f, but f must satisfy $f(g)=\chi(\det(g))f(1)+a$, which is possible only if $a=0$, so $f=\chi\circ\det$, contradiction.

The codimension 1 case is dual by(18.1.5.21) and(18.11.4.9). □

Cor. (18.11.4.3) [Steinberg Representation]. Consider the segment $\Delta(|\cdot|^{\frac{1-n}{2}},n)$ of length n and degree n, then $(\pi(\Delta),V)$ is the space of functions $B\backslash G\to\mathbb{C}$. Thus $Z(\Delta)$ is the trivial representation, and $Q(\Delta)$ is called the (standard)**Steinberg representation**, denoted by St_n. It is self-dual.

If $n=2$, then $\pi(\Delta)$ has length 2, thus there are an exact sequences,

$$0\to 1\to|\cdot|^{-1/2}\times|\cdot|^{1/2}\to\mathrm{St}_2\to 0,\quad 0\to\mathrm{St}_2\to|\cdot|^{1/2}\times|\cdot|^{-1/2}\to 1\to 0$$

⌟

Cor. (18.11.4.4) [Classification of $\mathrm{Irr}^{\mathrm{adm}}(GL(2,K))$]. The $n=2$ case is particularly clear: any $\pi\in\mathrm{Irr}^{\mathrm{adm}}(GL(2,K))$ has the following possibilities:

1. π is cuspidal.
2. $\pi=Q(\chi|\cdot|^{-1/2},\chi|\cdot|^{1/2})$, which equals $\mathrm{St}_2(\chi)$.
3. $\pi=\chi_1\times\chi_2$, where χ_1,χ_2 are not linked, which is the principal series.
4. $\pi=Q(\chi|\cdot|^{1/2},\chi|\cdot|^{-1/2})$, which equals $\mathbb{1}(\chi)$.

⌟

Def. (18.11.4.5) [Cuspidal Supports]. For a $\pi=Q(\Delta_1,\ldots,\Delta_r)\in\mathrm{Irr}^{\mathrm{adm}}(GL(n,K))$, where $\Delta_i=(\pi_i,m_i)$, define the **cuspidal supports** of π as the set

$$\mathrm{Supp}(\pi)=\{\pi_i(j)\}_{1\le i\le r,1\le j\le m_i-1}.$$

⌟

Principal Series Representations

Def. (18.11.4.6) [Principal Series Representations]. Given a diagonal quasi-character χ of $T(F)$, define the **principal series representation** of G as

$$\mathcal{B}(\chi_1,\ldots,\chi_n)=I_{B(K)}^{G(F)}(\chi)(18.1.5.34)=\{f\in C^\infty(G)|f(\begin{bmatrix}y_1 & & *\\ & \ldots & \\ & & y_n\end{bmatrix}g)=\chi_1(y_1)\ldots\chi_n(y_n)|y_1^{n-1}y_2^{n-3}\ldots y_n^{-n+1}|^{1/2}f$$

It is admissible of finite length by(18.11.2.8). If it is irreducible, its isomorphism class is denoted by $\pi(\chi_1,\chi_2)$. ⌟

Lemma (18.11.4.7). By(18.1.5.41), we have a map $P:C_c^\infty(G(F))\to\mathcal{B}(\chi_1,\ldots,\chi_n)$:

$$(P\varphi)(g)=\int_{B(K)}\varphi(b^{-1}g)(\delta^{1/2}\chi)(b)db$$

Then this map is intertwining and surjective. Moreover, we have

$$P(\lambda(b)^{-1}\varphi)=(\delta^{-1/2}\chi)(b)P(\varphi),\quad b\in B(K)$$

⌟

Prop. (18.11.4.8). The representation $B(\chi_1,\ldots,\chi_n)$ admits at most one Whittaker functional. In other words, $\dim J_\psi(B(\chi_1,\ldots,\chi_n))\leq 1$. in fact, it is exactly one, as will be shown by(18.11.4.2) and(18.11.3.13). ⌟

Proof: Let $\Lambda:V\to\mathbb{C}$ be a Whittaker functional, then we define a distribution Δ on $GL(2,K)$ as $\Delta(\varphi)=\Lambda(P\varphi)$. Then

$$\lambda(b)\Delta=(\delta^{-1/2}\chi)(b)\Delta, b\in B(K),\quad \rho(n)\Delta=\psi_N(n)^{-1}\Delta, n\in N(K)$$

by(18.11.4.7). Because P is surjective(18.11.4.7), it suffices to show that these Δ are unique up to scalar.

Consider the left-right action of $B(K)\times N(K)$ on $G(F)$, then there are $n!$ orbits $B(K)WN(K)$ by Bruhat decomposition(12.11.5.6). For $w\neq 1$, the orbit $B(K)wN(K)$ is isomorphic to $B(K)\times N(K)$ via $(b,n)\mapsto bwn^{-1}$, thus the restriction of Δ on $B(K)wN(K)$ must be of the form

$$\Delta_1(\varphi)=C\int_{B(K)}\int_{N(K)}\varphi(bwn^{-1})\psi_N(n)(\delta^{1/2}\chi^{-1})(b)dbdn$$

by(18.1.5.4). This is the unique map that satisfies the condition.

As for the distribution on $B(K)$, the same reasoning shows the restriction of Δ on $B(K)$ must be of the form

$$\Delta_2(\varphi)=C\int_{B(K)}\varphi(b)(\delta^{1/2}\chi^{-1})(b)db,$$

but it satisfies $\rho(n)\Delta_2=\Delta_2$, so there are no distribution on $B(K)$. Finally, (4.4.4.11) gives us the result. □

Cor. (18.11.4.9). The contragradient of $\chi_1\times\ldots\times\chi_n$ is $\chi_1^{-1}\times\ldots\times\chi_n^{-1}$. ⌟

Proof: If $f \in \mathcal{B}(\chi_1, \chi_2)$, $f' \in \mathcal{B}(\chi_1^{-1}, \chi_2^{-1})$, then the pairing $(f, f') = \int_K f(k)f'(k)dk$ is G-invariant by(11.10.1.45), so this defines a smooth functional $l_{f'}$, and it is non-degenerate, the mapping $f' \mapsto l_{f'}$ is injective(by letting $f = 1/f'$ on a $B(K)$-orbit that f' is non-zero) from $\mathcal{B}(\chi_1^{-1}, \chi_2^{-1})$ to $\mathcal{B}(\chi_1, \chi_2)^\vee$. Now by symmetry the other side is also injective, and we are done because $(V^\vee)^\vee =\cong V$(18.1.5.23). □

Cor. (18.11.4.10). $\mathrm{Hom}(\mathcal{B}(\chi_1, \ldots, \chi_n), \mathcal{B}(\mu_1, \ldots, \mu_n)) \neq 0$ only if $\{\chi_1, \ldots, \chi_n\} = \{\mu_1, \ldots, \mu_n\}$. ⌟

Proof: By smooth Frobenius reciprocity(18.1.5.37),

$$\mathrm{Hom}_G(\mathcal{B}(\chi_1, \chi_2), \mathcal{B}(\mu_1, \mu_2)) \cong \mathrm{Hom}_{B(K)}(\mathcal{B}(\chi_1, \chi_2), \delta^{1/2}\mu).$$

The proof below is similar to that of(18.11.4.8): For such a map Λ, we define a distribution $\Delta(\varphi) = \Lambda(P(\varphi))$, then

$$\lambda(b)\Delta = (\delta^{-1/2}\chi)(b)\Delta, \quad \rho(b)\Delta = (\delta^{-1/2}\mu^{-1})(b)\Delta, \quad b \in B(K).$$

So by the exact sequence(4.4.4.11), such distribution exists on one of the orbits $B(K)wN(K)$.

If such a distribution exists on $B(K)wN(K)$ for $w \neq 1$, then noticing $\rho(n)\Delta = \Delta$ for $n \in N(K)$, by(18.1.5.4)

$$\Delta(\varphi) = \int_{B(K)} \int_{N(K)} \varphi(bwn^{-1})(\delta^{1/2}\chi^{-1})(b)dbdn,$$

then we apply $\rho(t)$ with t diagonal, then

$$\begin{aligned}(\delta^{-1/2}\mu^{-1})(t)\Delta(\varphi) = (\rho(t)\Delta)(\varphi) &= \int_{N(K)} \int_{B(K)} \varphi((bwt^{-1}w^{-1})w(tnt^{-1})^{-1})(\delta^{1/2}\chi^{-1})(b)dbdn \\ &= \delta(t)^{-1}(\delta^{-1/2}\chi^{-1})(wtw^{-1})\Delta(\varphi)\end{aligned}$$

via change of variables(11.10.1.16). Notice that $\delta(t) = \delta(wtw^{-1})^{-1}$, thus $\mu(t) = \chi(wtw^{-1})$, which means $\chi_i = \mu_{w(i)}$.

Similarly, if such a distribution exists on $B(K)$, then

$$\Delta(\varphi) = \int_{B(K)} \varphi(b)(\delta^{1/2}\chi^{-1})(b)db.$$

Apply $\rho(b)$, then $\delta^{-1/2}\chi(b) = (\delta^{-1/2}\mu)(b)$, so $\chi_i = \mu_i$. □

Intertwining Integrals and Whittaker Functional

Prop. (18.11.4.11)[Intertwining Integral]. Let ξ_i be two characters of $K^\times$, and $\chi_i = |\cdot|^{s_i}\xi_i$, $(\pi, V) = \mathcal{B}(\chi_1, \chi_2)$, $(\pi', V') = \mathcal{B}(\chi_2, \chi_1)$. Define for $f \in V$,

$$Mf : GL(2, K) \to \mathbb{C} : Mf(g) = \int_{N(K)} f(w_0 ug)du$$

then if $\mathrm{Re}(s_1 - s_2) > 0$, the integral is absolutely convergent, $Mf \in V'$, and M is a nonzero intertwining, so $V \cong V'$ if they are both irreducible. ⌟

Proof: Should compare this proof with(18.9.4.18).

For the convergence, it suffices to check for $\begin{bmatrix}1 & x\\ & 1\end{bmatrix}$, $|x|$ large, but then

$$f(\begin{bmatrix} & -1\\ 1 & \end{bmatrix}\begin{bmatrix}1 & x\\ & 1\end{bmatrix}g)=f(\begin{bmatrix}x^{-1} & -1\\ & x\end{bmatrix}\begin{bmatrix}1 & \\ x^{-1} & 1\end{bmatrix}g)=|x|^{-1}(\chi_1^{-1}\chi_2)(x)f(\begin{bmatrix}1 & \\ x^{-1} & 1\end{bmatrix}g)$$

and because f is locally constant, when $|x|$ is large, $f(\begin{bmatrix}1 & \\ x^{-1} & 1\end{bmatrix}g)=f(g)$, thus the convergence on the unbounded region is dominated by

$$\int_{|x|>q^N}|x|^{-1}|(\chi_1^{-1}\chi_2)(x)|dx=\int_{|x|>q^N}|x|^{-s_1+s_2-1}dx,$$

which converges for $\mathrm{Re}(s_1-s_2)>0$.

To show $Mf\in V'$, we need to check

$$Mf(\begin{bmatrix}1 & x\\ & 1\end{bmatrix}g)=Mf(g),\quad Mf(\begin{bmatrix}y_1 & \\ & y_2\end{bmatrix}g)=|y_1/y_2|^{1/2}\chi_2(y_1)\chi_1(y_2)Mf(g).$$

The first is trivial and for the second:

$$Mf(\begin{bmatrix}y_1 & \\ & y_2\end{bmatrix}g)=\int_F f(\begin{bmatrix}y_2 & \\ & y_1\end{bmatrix}\begin{bmatrix} & -1\\ 1 & \end{bmatrix}\begin{bmatrix}1 & y_2y_1^{-1}x\\ & 1\end{bmatrix}g)dx$$

so it is clear.

Finally M is clearly intertwining, and it is not trivial by looking at the function f:

$$f=|y_1/y_2|^{1/2}\chi_1(y_1)\chi_2(y_2)\chi_{\mathcal{O}_F}(x),\text{ where }g=\begin{bmatrix}y_1 & z\\ & y_2\end{bmatrix}\begin{bmatrix} & -1\\ 1 & \end{bmatrix}\begin{bmatrix}1 & x\\ & 1\end{bmatrix}$$

and vanish if $g\in B(K)$. Notice the representation of g is unique by Bruhat decomposition. Then $Mf(1)=1$. □

Prop. (18.11.4.12) [Analytic Continuation of Intertwining Integral]. Let ξ_i be two characters of $K^\times$, $\chi_i=|\cdot|^{s_i}\xi_i$, $(\pi_{s_1,s_2},V_{s_1,s_2})=\mathcal{B}(\chi_1,\chi_2),(\pi'_{s_2,s_1},V'_{s_2,s_1})=\mathcal{B}(\chi_2,\chi_1)$.

Notice that by Iwasawa decomposition(18.11.1.4), an arbitrary $f\in\mathcal{B}(\chi_1,\chi_2)$ is determined by its restriction on K, and if a function f_0 on K satisfies

$$f_0(\begin{bmatrix}y_1 & x\\ & y_2\end{bmatrix}k)=\xi_1(y_1)\xi_2(y_2)f_0(k),y_1,y_2\in\mathcal{O}^*,$$

then f_0 can extends uniquely to an element $f_{s_1,s_2}\in V_{s_1,s_2}$ for any s_1,s_2, called the **flat sections** of f_0.

Then the intertwining integral Mf_{s_1,s_2} defined in(18.11.4.11) is analytic for the dominant χ in the flat family, and has an analytic continuation to all s_1,s_2 that $\chi_1\neq\chi_2$, and defines a nonzero operator $V_{s_1,s_2}\to V'_{s_2,s_1}$. ⌟

Proof: The proof is parallel to that of(18.11.4.11).

$$Mf_{s_1,s_2}(g)=\int_{|x|\leq q^N} f_{s_1,s_2}(\begin{bmatrix} & -1\\ 1 & \end{bmatrix}\begin{bmatrix}1 & x\\ & 1\end{bmatrix}g)dx+\int_{x\geq q^{N+1}}|x|^{-s_1+s_2-1}(\xi_1^{-1}\xi_2)(x)dxf_{s_1,s_2}(g)$$

the first term can easily be extended, and the second term vanishes if $\xi_1^{-1}\xi_2$ ramifies, and equals something like a multiple of $\frac{(\chi_1^{-1}\chi_2(\varpi))^{N+1}}{1-\chi_1^{-1}\chi_2(\varpi)}$, which extends unless $\chi_1=\chi_2$.

For the intertwining property, it is because equalities maintain along analytic continuation, in particular, it is non-trivial as $Mf_{s_1,s_2}(1)=1$. □

Cor. (18.11.4.13). $Z(\chi_1,\chi_2)\cong Z(\chi_2,\chi_1)$, $\sigma(\chi_1,\chi_2)\cong\sigma(\chi_2,\chi_1)$. If $\mathcal{B}(\chi_1,\chi_2)$ is irreducible, then $\pi(\chi_1,\chi_2)\cong\pi(\chi_2,\chi_1)$. Moreover, there are no other isomorphisms between these representations. ⌟

Proof: It suffices to show there are no other isomorphisms, and this is by(18.11.4.10). □

Prop. (18.11.4.14) [Whittaker functional of $\mathcal{B}(\chi_1,\chi_2)$]. There is a Whittaker functional on $\mathcal{B}(\chi_1,\chi_2)$ defined by

$$\Lambda(f)=\int_F f(w_0\begin{bmatrix}1 & x\\ & 1\end{bmatrix})\psi(-x)dx.$$

This integral is absolutely convergent if χ is dominant and is analytic for the flat family of χ, by method the same as in the proof of(18.11.4.11). And this can also be extended to all χ(as flat section(18.11.4.12)) by defining

$$\Lambda(f)=\lim_{k\to\infty}\int_{\mathfrak{p}^{-k}} f(w_0\begin{bmatrix}1 & x\\ & 1\end{bmatrix})\psi(-x)dx.$$

⌟

Remark (18.11.4.15). Compare with(20.5.3.3). ⌟

Proof: This makes sense because it stabilize as $k\to\infty$: when k is large,

$$\int_{\mathfrak{p}^{-k-1}\backslash\mathfrak{p}^{-k}} f(w_0\begin{bmatrix}1 & x\\ & 1\end{bmatrix})\psi(-x)dx=q^{-k-1}f(1)\int_{\mathfrak{p}^{-k-1}\backslash\mathfrak{p}^{-k}}\psi(-x)(\chi_1^{-1}\chi_2)(x)dx$$

By continuity(See the proof of(18.11.4.11)). If $\psi(t)\neq 0$, choose k large that $\chi_1^{-1}\chi_2(x)=\chi_1^{-1}\chi_2(x+t)$ for any $x\in\mathfrak{p}^{-k-1}\backslash\mathfrak{p}^{-k}$, thus this integral vanishes. □

Remark (18.11.4.16). For general n, this method won't work, and another method is used in**??**Bernstein, J., Letter to Piatetski-Shapiro (1985). To appear in Cogdell and Piatetski-Shapiro (book in preparation).] to extend analytically. ⌟

Prop. (18.11.4.17). If $\mathcal{B}(\chi_1,\chi_2)$ is irreducible, with the notations in(18.11.4.11), the intertwining integral $M:\mathcal{B}(\chi_1,\chi_2)\to\mathcal{B}(\chi_2,\chi_1)$ satisfies

$$\Lambda'\circ M=\xi_1\xi_2^{-1}(-1)\gamma(1-s_1+s_2,\xi_1^{-1}\xi_2,\psi)\Lambda,$$

where Λ is the Whittaker functional defined in(18.11.4.14), and $\gamma(s,\chi,\psi)$ is the local constant defined in(21.3.2.8). ⌟

Proof: Cf.[Bump, P485].**?** □

Cor. (18.11.4.18) [Composition of Intertwining Integrals]. If $\mathcal{B}(\chi_1,\chi_2)$ is irreducible, $M:\mathcal{B}(\chi_1,\chi_2)\to\mathcal{B}(\chi_2,\chi_1), M':\mathcal{B}(\chi_2,\chi_1)\to\mathcal{B}(\chi_1,\chi_2)$ are intertwining integrals, then $M'\circ M$ is the scalar $\gamma(1-s_1+s_2,\xi_1^{-1}\xi_2,\psi)\gamma(1+s_1-s_2,\xi_1\xi_2^{-1},\psi)$.

If $\mathcal{B}(\chi_1,\chi_2)$ is reducible, $M'\circ M=0$. ⌟

Proof: The irreducible case follows from the proposition. For the reducible case, let $\chi_1\chi_2^{-1}=|\cdot|$, the intertwining integral $\mathcal{B}(\chi_2,\chi_1)\to\mathcal{B}(\chi_1,\chi_2)$ is non-zero, so the image is ether $\mathcal{B}(\chi_1,\chi_2)$ or $\pi(\chi_1,\chi_2)$. In the first case, $\mathcal{B}(\chi_2,\chi_1)$ has a infinite dimensional proper quotient, contradiction. The intertwining integral $\mathcal{B}(\chi_1,\chi_2)\to\mathcal{B}(\chi_2,\chi_1)$ is non-zero, so the image is either $\mathcal{B}(\chi_2,\chi_1)$ or $\sigma(\chi_1,\chi_2)$. In the first case, $\mathcal{B}(\chi_1,\chi_2)$ has a 1-dimensional quotient, contradiction. □

Jacquet Module

Prop. (18.11.4.19) [Jacquet Module of $\mathcal{B}(\chi_1,\ldots,\chi_n)$]. Let χ_i be quasi-characters of $K^\times$, then the Jacquet module of $\chi_1\times\ldots\times\chi_n$ has dimension $n!$.

And if $n=2$, the representation of $T(F)$ on the Jacquet module is isomorphic to the representation

$$t\mapsto\begin{cases}\begin{bmatrix}(\delta^{1/2}\chi)(t) & \\ & (\delta^{1/2}\chi')(t)\end{bmatrix}, & \chi_1\neq\chi_2\\ (\delta^{1/2}\chi)(t)\begin{bmatrix}1 & v(t_1/t_2)\\ & 1\end{bmatrix}, & \chi_1=\chi_2=\chi\end{cases}.$$

⌟

Proof: Firstly we show $\dim J(\mathcal{B}(\chi_1,\chi_2))=2$: Let $\Lambda:V\to\mathbb{C}$ be a functional that $\Lambda(\rho(n)v)=\Lambda(v)$ for $n\in N(K)$, then we define a distribution Δ on $GL(2,K)$ as $\Delta(\varphi)=\Lambda(P\varphi)$. Then

$$\lambda(b)\Delta=(\delta^{-1/2}\chi)(b)\Delta, b\in B(K),\quad \rho(n)\Delta=\Delta, n\in N(K)$$

by(18.11.4.7). Because P is surjective(18.11.4.7), it suffices to show that there are exactly two linearly independent such Δ.

Consider the left-right action of $B(K)\times N(K)$ on $GL(2,K)$, then there are $n!$ orbits $B(K)WN(K)$ by Bruhat decomposition(12.11.5.6). For $w\neq 1$, the orbit $B(K)wN(K)$ is isomorphic to $B(K)\times N(K)$ via $(b,n)\mapsto bwn^{-1}$, thus the restriction of Δ on it must be of the form

$$\Delta_1(\varphi)=C\int_{B(K)}\int_{N(K)}\varphi(bwn^{-1})(\delta^{1/2}\chi^{-1})(b)dbdn$$

by(18.1.5.4).

As for the distribution on $B(K)$, the same reasoning shows the restriction of Δ on $B(K)$ must be of the form

$$\Delta_2(\varphi)=C\int_{B(K)}\varphi(b)(\delta^{1/2}\chi^{-1})(b)db,$$

and it truly satisfies $\rho(n)\Delta_2=\Delta_2$. Finally, (4.4.4.11) gives us the result.

Next we consider $J(V)$ as a 2-dimensional $T(F)$-representation must be of the two forms in(18.11.1.24), it suffices to distinguish these two cases.

Denote $V=\mathcal{B}(\chi_1,\chi_2)$. Consider for any quasi-character μ of $T(F)$,

$$\mathrm{Hom}_{T(F)}(J(V),\delta^{1/2}\mu)\cong\mathrm{Hom}_{B(K)}(V,\delta^{1/2}\mu)\cong\mathrm{Hom}_{GL(2,K)}(V,\mathcal{B}(\mu_1,\mu_2))$$

So(18.11.4.10)(18.11.4.13) can be used, so if $\chi_1\neq\chi_2$, there are two μ that can make the Hom group non-vanish, so it is the first case. If $\chi_1=\chi_2$, then V is irreducible, and there is only one μ that makes this Hom group non-vanish, and the Hom group is of dimension1 by Schur's lemma, so it is the second case. □

Prop. (18.11.4.20) [Jacquet Module is Finite Dimensional]. For $(\pi,V)\in\mathrm{Irr}^{\mathrm{adm}}(GL(n,K))$, $\dim J_{\mathrm{Unip}(n,K)}(V)\leq n!$, and if it is nonzero, then π is a subrepresentation of some $\mathcal{B}(\chi_1,\ldots,\chi_n)$. ⌟

Proof: By(18.11.2.10), π is isomorphic to a subrepresentation of some $\mathcal{B}(\chi_1,\ldots,\chi_n)$. Then by exactness of Jacquet functor(18.11.2.1), $J(V)$ is a subspace of $J(\mathcal{B}(\chi_1,\ldots,\chi_n))$, which has dimension $n!$(18.11.4.19). □

Prop. (18.11.4.21) [Jacquet Functor of $\sigma(\chi_1,\chi_2)$]. Suppose χ_1,χ_2 are characters of $K^\times$ that $\chi_1\chi_2^{-1}=|\cdot|^{-1}$, then $\mathcal{B}(\chi_1,\chi_2)$ is reducible, then the Jacquet modules of $\pi(\chi_1,\chi_2)$ and $\sigma(\chi_1,\chi_2)$ are 1-dimensional, and the characters of $T(F)$ they afford are $\delta^{1/2}\chi$ and $\delta^{1/2}\chi'$. ⌟

Proof: Clearly the Jacquet module of a representation $\mathbb{1}(\chi)$ is of dimension 1, so by the exactness of Jacquet functor(18.11.2.1) and(18.11.4.19), the Jacquet functor for $\sigma(\chi_1,\chi_2)$ is also of dimension 1.

For the determination of the Jacquet module, notice for any representation (π,V) of $GL(2,K)$,

$$\mathrm{Hom}_{T(F)}(J(V),\delta^{1/2}\mu)\cong\mathrm{Hom}_{B(K)}(V,\delta^{1/2}\mu)\cong\mathrm{Hom}_{GL(2,K)}(V,\mathcal{B}(\mu_1,\mu_2)).$$

So for $\pi=\pi(\chi_1,\chi_2)$, $\mathrm{Hom}_{T(F)}(J(V),\delta^{1/2}\mu)=\mathbb{C}$ for $\mu=\chi$, so $J(\pi(\chi_1,\chi_2))$ is $\delta^{1/2}\chi$. For $\pi=\sigma(\chi_1,\chi_2)$, then $\mathrm{Hom}_{T(F)}(J(V),\delta^{1/2}\mu)=\mathbb{C}$ for $\mu=\chi'$ by(18.11.4.13), so $J(\sigma(\chi_1,\chi_2))$ is $\delta^{1/2}\chi'$. □

Kirillov Modules of Principal Series

Prop. (18.11.4.22)[Kirillov Model of Principal Series]. Let $\pi(\chi_1,\chi_2)$ be an irreducible principal series,

- If $\chi_1\neq\chi_2$, then the Kirillov model of $\pi(\chi_1,\chi_2)$ consists of smooth functions φ on $K^\times$ that is compactly supported on F and $\varphi(t)$ is a linear combination of the function $|t|^{1/2}\chi_1(t)$ and $|t|^{1/2}\chi_2(t)$ when $|t|$ is small.
- If $\chi_1=\chi_2$, then the Kirillov model of $\pi(\chi_1,\chi_1)$ consists of smooth functions φ on $K^\times$ that is compactly supported on F and $\varphi(t)$ is a linear combination of the function $|t|^{1/2}\chi_1(t)$ and $v(t)|t|^{1/2}\chi_1(t)$ when $|t|$ is small.

⌟

Proof: First assume that $\chi_1=\chi_2$, then by(18.11.4.19), there are two functions φ_1,φ_2 that satisfies

$$\pi(t)\overline{\varphi}_1=(\delta^{1/2}\chi)(t)\overline{\varphi}_1,\quad \pi(t)\overline{\varphi}_2=(\delta^{1/2}\chi)(t)\overline{\varphi}_2+v(t_1/t_2)(\delta^{1/2}\chi)(t)\overline{\varphi}_1.$$

Then by(18.11.3.21), $\varphi_1(u)=C|u|^{1/2}\chi_1(u)$ for $|u|$ small, and because $\overline{\varphi}_1\neq 0\in J(V)$, $C\neq 1$ by(18.11.3.20), and we can assume that $C=1$. Then for any $t_0\in\mathfrak{p}\backslash\mathfrak{p}^2$,

$$\pi(\begin{bmatrix}t_0&\\&1\end{bmatrix})\varphi_2-|t_0|^{1/2}\chi_1(t_0)[\varphi_1+\varphi_2]\in V_N.$$

Thus by(18.11.3.20), there exists some constant $\varepsilon(t_0)$ that

$$\varphi_2(tu) = |t|^{1/2}\chi_1(t)\varphi_2(u) + |tu|^{1/2}\chi_1(tu).$$

is true for $t = t_0$ and $|u| \leq \varepsilon(t_0)$. Notice both sides are locally constant on t, so this is true for t near t_0. Because $\mathfrak{p}\backslash\mathfrak{p}^2$ is compact, there is a ε that this is true for any $t \in \mathfrak{p}\backslash\mathfrak{p}^2$ and $|u| \leq ve$.

Now any element $t \in \mathfrak{p}$ can be factored into product of elements in $\mathfrak{p}\backslash\mathfrak{p}^2$, so by induction

$$\varphi_2(tu) = |t|^{1/2}\chi_1(t)\varphi_2(u) + v(t)|tu|^{1/2}\chi_1(tu).$$

for any $t \in \mathfrak{p}$ and $|u| \leq \varepsilon$. So the theorem is true for φ_1 and φ_2, thus true for any other function because they differs from a linear combination of these two by an element in V_N, which vanishes for $|t|$ small, by(18.11.3.20).

Case1 is similar and easier. □

Prop. (18.11.4.23) [Kirillov Model of Steinberg Representations]. Let $\sigma(\chi_1, \chi_2)$ be a Steinberg representation of $GL(2, K)$, where $\chi_1\chi_2^{-1} = |\cdot|^{-1}$, then the Kirillov model of $\sigma(\chi_1, \chi_2)$ consists of smooth functions φ on $K^\times$ that is compactly supported on F and $\varphi(t)$ is a constant multiple of $|t|^{1/2}\chi_2(t)$ when $|t|$ is small. ⌟

Proof: The proof is the same as that of(18.11.4.22), with(18.11.4.21) used instead of(18.11.4.19). □

5 Spherical Representations

Def. (18.11.5.1) [Normalized Spherical Vector]. Let $\chi_1, \ldots, \chi_n$ be nonramified quasi-characters of $K^\times$, then $\mathcal{B}(\chi_1, \ldots, \chi_n)$ contains a K-fixed vector φ_K that is defined to be

$$\varphi_{\mathcal{K}}(bk) = (\delta^{1/2}\chi)(b), b \in B(K), k \in \mathcal{K}$$

Notice this is well-defined, because for $u \in B(K) \cap \mathcal{K}$, $(\delta^{1/2}\chi)(u) = 1$. $\varphi_{\mathcal{K}}$ is $\mathcal{K}$-spherical, and we refer to it the **normalized spherical vector** in V. Such a $\mathcal{B}(\chi_1, \ldots, \chi_n)$ is called a **unramified principal series** if it is irreducible.

Notice when $n = 2$ and $\chi_2 = \chi_1|\cdot|$, this spherical vector just spans the 1-dimensional invariant subspace in(18.11.4.2). ⌟

Prop. (18.11.5.2) [Satake Isomorphism]. There is an isomorphism

$$S : \mathcal{H}_K \cong \mathbb{C}[t_1, t_1^{-1}, \ldots, t_n, t_n^{-1}]^W.$$

s.t. if $\varphi \in \mathcal{H}_K$, for any spherical principal series $\pi(\chi_1, \ldots, \chi_n)$ and a spherical vector v, $\pi(\varphi)v = S(\varphi)(\alpha_1, \ldots, \alpha_n)$, where $\alpha_i = \chi(\chi_i)$ are the Satake parameters of χ_i. ⌟

Remark (18.11.5.3). For general Satake isomorphism, Cf.(18.12.0.3). ⌟

Proof: Cf.[Spherical representations and the Satake isomorphism]? □

Cor. (18.11.5.4). When $n = 2$, under the Satake isomorphism, the Hecke operators $T(\mathfrak{p}) = \begin{bmatrix} \varpi & \\ & 1 \end{bmatrix}$ and $R_p = \varpi I$ are mapped to

$$q^{1/2}(t_1 + t_2), \quad t_1 t_2,$$

resp. ⌟

Proof: For any unramified spherical representation with Satake parameters α_1, α_2, using the representative of $\mathscr{K}\begin{bmatrix}\varpi & \\ & 1\end{bmatrix}\mathscr{K}$ over $\mathscr{K}$ as in(20.2.2.9),

$$(T(\mathfrak{p})\varphi_{\mathscr{K}})(1) = \int_{\mathscr{K}\begin{bmatrix}\varpi & \\ & 1\end{bmatrix}\mathscr{K}} \varphi_K(g)dg = \sum_{\gamma\in K\begin{bmatrix}\varpi & \\ & 1\end{bmatrix}K/K} \varphi_K(\gamma)$$

$$= (\Delta^{1/2}\chi)(\begin{bmatrix}1 & \\ & \varpi\end{bmatrix}) + q(\Delta^{1/2}\chi)(\begin{bmatrix}\varpi & \\ & 1\end{bmatrix}) = q^{1/2}(\alpha_1+\alpha_2)$$

and similarly for $R(\mathfrak{p})$. □

Cor. (18.11.5.5) [Spherical Representation of $GL(n,K)$]. Every irreducible admissible spherical representation (π, V) of $GL(n,K)$ is of the form $Q(\Delta_1,\Delta_2,\ldots,\Delta_n)$ where $\Delta_i = (\chi_i, 1)$, χ_i are unramified quasi-characters. ⌟

Proof: Use the Satake isomorphic to find Satake parameters of unramified quasi-characters χ_i that makes the representation of $\mathcal{H}_K \cong \mathbb{C}[t_1, t_1^{-1},\ldots,t_n,t_n^{-1}]^W$ isomorphic to that of π, then by(3.6.4.3), $\chi_1\times\chi_2\times\ldots\times\chi_n$ has a unique irreducible subquotient that has the came spherical character as π, then by(3.6.4.12), this subquotient is isomorphic to π. Now use the fact we can change the order of χ_i s.t. it is just $Q(\Delta_1,\Delta_2,\ldots,\Delta_n)$. □

Prop. (18.11.5.6) [Intertwining Operator on Spherical Vector]. For χ_1,χ_2 unramified with Satake parameter α_i, consider $M:\mathcal{B}(\chi_1,\chi_2)\to\mathcal{B}(\chi_2,\chi_1)$, then

$$M\varphi_{K,\chi} = \frac{1-q^{-1}\alpha_1\alpha_2^{-1}}{1-\alpha_1\alpha_2^{-1}}\varphi_{K,\chi'}.$$

⌟

Proof: Clearly this equation is true up to scalar because M is intertwining, so it suffices to calculate $(M\varphi_K)(1)$. For this, we assume χ is dominant(18.11.5.2) because we can use analytic continuation. Then

$$(M\varphi_K)(1) = \int_F \varphi_K(w_0\begin{bmatrix}1 & x\\ & 1\end{bmatrix})dx.$$

The integral is 1 on $\mathcal{O}$, and for $m>0$, on $\mathfrak{p}^{-m}\backslash\mathfrak{p}^{-m+1}$, by(18.11.4.11), it equals $q^{-m}\alpha_1^m\alpha_2^{-m}q^m(1-q^{-1})$, so the total sum is $1+(1-q^{-1})\alpha_1\alpha_2^{-1}/(1-\alpha_1\alpha_2^{-1})$. □

Prop. (18.11.5.7). If χ_1,χ_2 are nonramified, $V=\mathcal{B}(\chi_1,\chi_2)$, $K_0(\mathfrak{p})$ is the Iwahori subgroup(18.11.1.8), then the composition

$$V^{K_0(\mathfrak{p})}\hookrightarrow V\to J(V)$$

is an isomorphism. In particular, it is of dimension 2. ⌟

Proof: Firstly notice $V^{K_0(\mathfrak{p})}$ has dimension≤ 2, because of the decomposition(18.11.1.11) and definition, and $J(V)$ has dimension2 by(18.11.4.19), so it suffices to show the map is surjective. The image is just $J(V)^{T(\mathcal{O})}$ by(18.11.2.5). But by(18.11.4.19) and the fact χ_i are nonramified, all of $J(V)$ are $T(\mathcal{O})$-fixed, thus $J(V)^{T(\mathcal{O})}=J(V)$. □

Cor. (18.11.5.8) [Casselman Basis]. When $\chi_1 \neq \chi_2$, we can easily find a basis of $V^{K_0(\mathfrak{p})}$, that is

$$L_1(\varphi) = \varphi(1), \quad L_0(\varphi) = (M\varphi)(1)$$

where M is intertwining integral defined in(18.11.4.12). These are $N(K)$-invariant, thus define functionals on $J(V) \cong V^{K_0(\mathfrak{p})}$. They are linearly independent checked on $T(F)$.

Then the dual basis $\varphi_0, \varphi_1 \in V^{K_0(\mathfrak{p})}$ are called the **Casselman basis**.

φ_0 has a simple form: using Iwahori-Bruhat decomposition(18.11.1.11),

$$\varphi_0(g) = \begin{cases} (\Delta^{1/2}\chi)(b) & g = bw_0k \in B(K)wK_0(\mathfrak{p}) \\ 0 & \text{otherwise} \end{cases}.$$

⌟

Proof: It is easily verified that this formula is well-defined and defines a Iwahori-fixed vector, so it suffices to valuate it by L_i. Clearly $L_1(\varphi_0) = 0$, and for $L_0(\varphi_0)$, notice that

$$w_0 \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} \in B(K)w_0K_0(\mathfrak{p})$$

iff $x \in \mathcal{O}$, so $L_0(\varphi_0) = 1$. □

Lemma (18.11.5.9). When $\chi_1 \neq \chi_2$ nonramified and $m \geq 0$, the function

$$F_m(g) = \int_{\mathcal{O}} \varphi_K(g \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} a_m)dx, \quad a_m = \begin{bmatrix} \varpi^m & \\ & 1 \end{bmatrix}$$

is an Iwahori-fixed vector, and

$$F_m = q^{-m/2}\alpha_2^m M(\varphi_K)(1)\varphi_0 + q^{-m/2}\alpha_1^m\varphi_1$$

⌟

Proof:

$$\int_{K_0(\mathfrak{p})} \pi(ka_m)\varphi_K dk = \int_{N_-(\mathfrak{p})}\int_{T(\mathcal{O})}\int_{N(\mathcal{O})} \varphi_K(gn_-t_0na_m)dndt_0dn_-\text{(18.11.1.9)}$$

noticing that $a_m^{-1}t_0n_-a_m \in K$ as $m \geq 0$, so the integrand is independent of t_0, n_- and equals F_m, and it is clearly Iwahori-fixed. And

$$c_1 = L_1(F_m) = F_m(1) = \varphi_K(a_m) = (\Delta^{1/2}\chi)(a_m) = q^{-m/2}\alpha_1^m.$$

Similarly, for χ dominant,

$$c_0 = L_0(F_m) = \int_{N(K)} F_m(w_0n)dn = \int_{N(K)}\int_{N(\mathcal{O})} \varphi_K(w_0nn'a_m)dn'dn.$$

By Fubini, the n' can be omitted, thus it equals $(M\varphi_K)(a_m) = (\Delta^{1/2}\chi')(a_m)$. □

Spherical Whittaker Function and Spherical Functions

See [Casselman, W., The unramified principal series of p-adic groups I: the spherical function, Compositio Math. 40 (1980), 387-406.] and [Casselman, W. and J. Shalika, The unramified principal series of p-adic groups II: the Whittaker function, Compositio Math. 40 (1980), 207-231.] for more general calculations.

Def. (18.11.5.10) [Spherical Whittaker Function]. The **spherical Whittaker function** of a generic spherical representation is the spherical vector W^0 in the Whittaker model normalized that $W_0(1) = 1$**?**.

For $n = 2$, we can define another normalization $W_0(g) = \Lambda(\pi(g)\varphi_K)$, where Λ is the Whittaker functional defined in(18.11.4.14) and φ_K is the normalized spherical vector defined in(18.11.5.1). ⌟

Prop. (18.11.5.11). We may assume that the conductor of ψ is $\mathcal{O}$, because any other character is of the form $x \mapsto \psi(ax)$, thus

$$W_0(g, \psi_a) = \int_F \varphi_K(w_0 \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} g)\psi(-ax)dx = |a|^{-1/2}\chi_2(a)W_0(\begin{bmatrix} a & \\ & 1 \end{bmatrix} g, \psi),$$

(and also by analytic continuity). In particular, $\mu(\mathcal{O}) = 1$(14.4.5.6).

Notice that

$$W_0(\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}\begin{bmatrix} z & \\ & z \end{bmatrix} gk) = \psi(x)\omega(z)W_0(g), z \in K^\times, k \in K,$$

where $\omega = \chi_1\chi_2$, so to calculate W_0, it suffices to compute $W_0(\begin{bmatrix} \varpi^m & \\ & 1 \end{bmatrix} = a_m)$. ⌟

Remark (18.11.5.12). We want to calculate the spherical Whittaker function W_0 explicitly because it is used to evaluate the local part of the global L-function(21.3.6.3). ⌟

Lemma (18.11.5.13) [Calculating W_0]. For $\mathcal{B}(\chi_1, \chi_2)$ with Satake parameters α_1, α_2, the spherical Whittaker function satisfies

$$W_0(1) = 1 - q^{-1}\alpha_1\alpha_2^{-1}, \quad W_0(a_m) = 0$$

for $m < 0$. ⌟

Proof: As in the proof of(18.11.4.11), because φ_K is K-invariant, we have

$$\int_{\mathcal{O}} \varphi_K(w_0 \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix})\psi(-x)dx = 1,$$

$$\int_{\mathfrak{p}^{-1}\setminus\mathcal{O}} \varphi_K(w_0 \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix})\psi(-x)dx = q^{-1}\alpha_1\alpha_2^{-1}\int_{\mathfrak{p}^{-1}\setminus\mathcal{O}} \psi(-x)dx = -q^{-1}\alpha_1\alpha_2^{-1},$$

$$\int_{\mathfrak{p}^{-k-1}\setminus p^{-k}} \varphi_K(w_0 \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix})\psi(-x)dx = q^{-k-1}\alpha_1^{k+1}\alpha_2^{-k-1}\int_{\mathfrak{p}^{-k-1}\setminus\mathfrak{p}^{-k}} \psi(-x)dx = 0, \quad k \geq 1$$

For $W_0(a_m)$, choose $x \in \mathcal{O}$ that $\psi(\varpi^m x) \neq 1$, then

$$W_0(a_m) = W_0(a_m \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}) = W_0(\begin{bmatrix} 1 & \varpi^m \\ & 1 \end{bmatrix} a_m) = \psi(\varpi^m x)W_0(a_m)$$

so $W_0(a_m) = 0$. □

Lemma (18.11.5.14) [Functional Equation]. For fixed g, $W_0(g)$ is an analytic function of α_1, α_2, and $(1 - q^{-1}\alpha_1\alpha_2^{-1})^{-1}W_0(g)$ is symmetric in α_1, α_2. ⌟

Proof: The Whittaker functional is defined by calculated by continuation(18.11.4.14), and for χ dominant, W_0 is analytic(18.11.4.14), thus by calculation in(18.11.5.13), its value at 1 is identically 1, thus so does its analytic continuation. Then to check after switching α_1, α_2 it is the same meromorphic function, it suffices to show for all irreducible principal series $\mathcal{B}(\chi_1, \chi_2)$. But in this case, $\mathcal{B}(\chi_1, \chi_2) \cong \mathcal{B}(\chi_2, \chi_1)$, so their Whittaker model thus spherical Whittaker function differ only by a scalar, thus the same. □

Prop. (18.11.5.15) [Calculating W_0].

$$(1 - q^{-1}\alpha_1\alpha_2^{-1})^{-1}W_0(a_m) = \begin{cases} q^{-m/2}\frac{\alpha_1^{m+1}-\alpha_2^{m+1}}{\alpha_1-\alpha_2} & m \geq 0 \\ 0 & m < 0 \end{cases}$$

⌟

Proof: By?? we can assume χ is dominant and use analytic continuation.

$$W_0(a_m) = \int_F F_m(w_0 \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix})\psi(-x)dx,$$

by(18.11.4.14)(18.11.5.9) and a change of variable. Then use(18.11.5.9), we see that

$$W_0(a_m) = C_1 q^{-m/2}\alpha_1^m + C_0 q^{-m/2}\alpha_2^m$$

where

$$C_0 = (M\varphi_K)(1)\int_F \varphi_0(w_0 \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix})\psi(-x)dx$$

And $\int_F \varphi_0(w_0 \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix})\psi(-x)dx = 1$, by the same consideration as in the proof of(18.11.5.8).

Finally, $(M\varphi_K)(1)$ can be calculated by(18.11.5.6), and the requirement of(18.11.5.14) will determine C_1. □

Prop. (18.11.5.16) [Spherical Function]. For a spherical irreducible admissible representation (π, V) of $GL(2, K)$, its contragradient $\widehat{V}$ is also spherical(3.6.4.11). Then we define the **spherical function**

$$\sigma(g) = (\pi(g)v, \widehat{v})$$

where $v, \widehat{v}$ are spherical and normalized that $\langle v, \widehat{v}\rangle = 1$. This is bi-invariant under K-action By(18.11.5.5).

By(18.11.5.5), (π, V) is of the form $\chi(\det(g))$ or $\pi(\chi_1, \chi_2)$ for π_i nonramified. In the former case the spherical function is just $\chi \circ \det$. Now we only consider the latter interesting case, for which there is a spherical functional $\widehat{v} : \varphi \mapsto \int_K \varphi(k)dk$, and it is 1 on the normalized spherical vector v(18.11.5.1), and

$$\sigma(g) = \int_K (\pi(g)\varphi_K)(k)dk = \int_K \varphi_K(kg)dk$$

⌟

Prop. (18.11.5.17) [Macdonald Formula]. The spherical function for unramified principal series behave well under $Z(K)$-action and is K-binvariant, so in order to compute it, it suffices to compute its value on a_m. We have:

$$\sigma(a_m) = \frac{q^{-m/2}}{1+q^{-1}}[\alpha_1^m \frac{1-q^{-1}\alpha_2\alpha_1^{-1}}{1-\alpha_2\alpha_1^{-1}} + \alpha_2^m \frac{1-q^{-1}\alpha_1\alpha_2^{-1}}{1-\alpha_1\alpha_2^{-1}}]$$

⌟

Proof: First notice that

$$\int_K F_m(k)dk = \int_K \int_{\mathcal{O}} \varphi_K(k \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} a_m) dx dk = \int_K \varphi_K(ka_m)dk$$

by a change of variable. Then by(18.11.5.9), this equals

$$[\int_K \varphi_0(k)dk] q^{-m/2}\alpha_2^m \frac{1-q^{-1}\alpha_1\alpha_2^{-1}}{1-\alpha_1\alpha_2^{-1}} + [\int_K \varphi_1(k)dk] q^{-m/2}\alpha_1^m.$$

Next we calculate $\int_K \varphi_0(k)dk$ directly: By(18.11.5.8), this equals the volume of $K \cap (K_0(\mathfrak{p})w_0K_0(\mathfrak{p})) = K_0(\mathfrak{p})w_0K_0(\mathfrak{p})$. $K/K_0(\mathfrak{p}) \cong GL(2,\mathbb{F}_q)/B(\mathbb{F}_q)$ has cardinality $q+1$, and by pulling back the Bruhat decomposition of $GL(2,\mathbb{F}_q)$, $K_0(\mathfrak{p})w_0K_0(\mathfrak{p})$ consists of q left cosets of $K_0(\mathfrak{p})$. So

$$\int_K \varphi_0(k)dk = \frac{q}{1+q}.$$

Finally the expression is symmetric in α_1, α_2, because the spherical vectors in $V, \widehat{V}$ are unique(3.6.4.11), and $\widehat{\mathcal{B}(\chi_1,\chi_2)} = \mathcal{B}(\chi_2,\chi_1)$. Also, the expression is a combination of α_i^m and the coefficient is independent of m, so it can be determined as above. □

6 Unitarizable, Tempered & L^2 Representations

Def. (18.11.6.1) [L^2-Representations]. An admissible irreducible representation (π, V) of G is called **essentially square-integrable** if for any $v \in V$ and $\lambda \in V^\vee$, the matrix coefficients $c_{v,\lambda}$ is L^2 on K.

It is called **square-integrable** if moreover the central character ω_π is unitary. ⌟

Remark (18.11.6.2) [Casselman]. For any smooth representation of $GL(n,K)$, there exists a unique real-valued quasi-character χ that the central character of $\pi \otimes (\chi \circ \det)$ is unitary. ⌟

Def. (18.11.6.3) [Tempered Representations]. Let G be a reductive group over F and π an admissible representation of $G(F)$, then π is called an **essentially tempered representation** if the matrix coefficients of π are all contained in $L^{2+\varepsilon}(K)$ for any $\varepsilon > 0$.

It is called a **tempered representation** if moreover the central character ω_π is unitary. ⌟

Prop. (18.11.6.4) [Jacquet, Zelevinsky].

- $\pi \in \mathrm{Irr}^{\mathrm{adm}}(GL(n,K))$ is essentially square-integrable iff it is of the form $Q(\Delta)$ for a single Zelevinsky segment Δ.
- $\pi \in \mathrm{Irr}^{\mathrm{adm}}(GL(n,K))$ is square-integrable iff it is of the form $Q(\Delta)$ for a single Zelevinsky segment, and the central character of $\sigma(\frac{m-1}{2})$ is unitary, where $\Delta = \Delta(\sigma, m)$.

- $\pi \in \text{Irr}^{\text{adm}}(GL(n,K))$ is tempered iff $\pi = Q(\Delta_1,\ldots,\Delta_r)$, where each $Q(\Delta_i)$ is square-integrable.

⌟

Proof: Cf.[Generic Representations, Jacquet(1977)]. □

Cor. (18.11.6.5)[Classification of Irreducible tempered representations of $GL(2)$]. Irreducible tempered representations of $GL(2,K)$ are one of the following form:

- Cuspidal representation with unitary central characters.
- Steinberg representations with unitary central characters.
- Principal representations $\mathcal{B}(\chi_1,\chi_2)$ with χ_1,χ_2 unitary.

⌟

Proof: Cf.[G-H11]P365. □

Cor. (18.11.6.6)[Tempered Representation is Generic]. Irreducible tempered representations are precisely generic ones $Q(\Delta_1)\times\ldots\times Q(\Delta_r)$ s.t. each $Q(\Delta_i)$ has a unitary central character. ⌟

Proof: It suffices to show that no two Δ_i,Δ_j are linked. But notice if $\Delta_i=(\sigma_i,m_i)$, then $\sigma(i)(\frac{m_i-1}{2})$ is the central character, so there are no chance that they are linked. □

Unitarizable Representations

Lemma (18.11.6.7) [Possibility of Unitarization of Principal Series]. If $\mathcal{B}(\chi_1,\chi_2)$ admits an invariant non-degenerate Hermitian pairing, then either χ_1,χ_2 are all characters or $\chi_1=\overline{\chi_2}^{-1}$. ⌟

Proof: There is an anti-linear $GL(2,K)$-map $\mathcal{B}(\chi_1,\chi_2)\to\mathcal{B}(\overline{\chi_1},\overline{\chi_2})$ which is conjugation, so if there is a $GL(2,K)$-invariant Hermitian pairing on $\mathcal{B}(\chi_1,\chi_2)$, $(f_1,f_2)\mapsto(f_1,\overline{f_2})$ will be a non-degenerate $GL(2,K)$-invariant bilinear pairing

$$\mathcal{B}(\chi_1,\chi_2)\times\mathcal{B}(\overline{\chi_1},\overline{\chi_2})\to\mathbb{C}.$$

So $\mathcal{B}(\chi_1,\chi_2)\cong\mathcal{B}(\overline{\chi_1}^{-1},\overline{\chi_2}^{-1})$, so χ_i are characters or $\chi_1=\overline{\chi_2}^{-1}$ by(18.11.4.10). □

Lemma (18.11.6.8). If χ_1,χ_2 are characters, then $\mathcal{B}(\chi_1,\chi_2)$ is unitarizable, by(18.1.5.45). ⌟

Lemma (18.11.6.9). Let $\chi_s=\chi_0|\cdot|^s$, where χ_0 is a character of F. If $s\neq 0,1/2$ is a real number (so that $\mathcal{B}(\chi_s,\chi_{-s})$ is irreducible), then $\mathcal{B}(\chi_s,\chi_{-s})$ is unitarizable iff $-1/2<s<1/2$. ⌟

Proof: Because $\mathcal{B}(\chi_s,\chi_{-s})=\chi_0\otimes\mathcal{B}(|\cdot|^s,|\cdot|^{-s})$, we can assume $\chi_0=1$. Let $M_s:\mathcal{B}(\chi_s,\chi_{-s})\to\mathcal{B}(\chi_{-s},\chi_s)$ be the intertwining integral(18.11.4.12), then we see the sesquilinear pairing

$$(f_1,f_2)=\int_K(M_sf_1)(k)\overline{f_2(k)}dk$$

is G-invariant and non-degenerate by the proof of(18.11.4.9). For an irreducible representation, such a pairing must be unique, so we are reduced to checking this representation is positive/negative definite.

Consider the Iwahori-fixed vector $f_0=\Delta^{s+1/2}(b)$ for $g=bk$ as defined in(18.11.5.8), then as s varies, f_0 forms a flat section. We calculate (f_0,f_0) for $s>0$ and then use continuation:

In this case,

$$(f_0, f_0) = V(K_0(\mathfrak{p}))\int_F f_0(w_0\begin{bmatrix}1 & x\\ & 1\end{bmatrix})dx$$

and

$$\begin{bmatrix} & -1\\ 1 & \end{bmatrix}\begin{bmatrix}1 & x\\ & 1\end{bmatrix} \in B(K)K_0(\mathfrak{p})$$

iff $x \notin \mathcal{O}$, in which case

$$\begin{bmatrix} & -1\\ 1 & \end{bmatrix}\begin{bmatrix}1 & x\\ & 1\end{bmatrix} = \begin{bmatrix}x^{-1} & -1\\ & x\end{bmatrix}\begin{bmatrix}1 & \\ x^{-1} & 1\end{bmatrix}.$$

So

$$(f_0, f_0) = \frac{1}{q+1}\int_{|x|>1} |x|^{-1-2s}dx = \frac{1-q^{-1}}{1+q}\frac{q^{-2s}}{1-q^{-2s}}.$$

We then consider the spherical vector φ_K(18.11.5.1), then(18.11.5.6) shows

$$(\varphi_K, \varphi_K) = \frac{1-q^{-1-2s}}{1-q^{-2s}}.$$

which is positive if $|s| > 1/2$. So if $\mathcal{B}(\chi_s, \chi_{-s})$ is unitarizable, $|s| < 1/2$.

Now for $|s| < 1/2$, we show $\mathcal{B}(\chi_s, \chi_{-s})$ is unitary: Modify the intertwining operator $M_s^* = (1-q^{-2s})M_s$, then it is definable for $s = 0$, by calculation in(18.11.4.12), so the modified Hermitian product

$$(\cdot,\cdot)^* = (1-q^{-2s})(-,-)$$

is defined at $s = 0$, and is positive/negative definite, because in this case it is irreducible and unitarizable(18.11.6.8). The eigenvalue of this Hermitian form deforms continuously, and it is never zero because it is non-degenerate as said above(only when $s \neq 1/2$ because we need M_s to be isomorphism), so it is always definite and $\mathcal{B}(\chi_s, .\chi_{-s})$ is unitarizable. □

Prop. (18.11.6.10)[Unitarizable Principal Series]. An irreducible principal series $\mathcal{B}(\chi_1, \chi_2)$ is unitary iff either χ_1, χ_2 are all characters, or there is a unitary character χ_0 and $-1/2 < s < 1/2$ that $\chi_1 = \chi_0|\cdot|^s, \chi_1 = \chi_0|\cdot|^{-s}$, called **complementary series representations**. ⌟

Proof: Follows immediately from the lemmas above(18.11.6.8)(18.11.6.7)(18.11.6.9). □

18.12 Local Langlands for GL(n) over p-Adic Fields

Main references are [B-K93], [Bus19] and [The Local Langlands correspondence, the Non-Archimedean Case, Kudla(1994)].

Notation (18.12.0.1).

- Let $K \in p$-LField.

⌟

Prop. (18.12.0.2). If G/K is a split almost simple algebraic group, then it is isogenous to one of the following groups: $\mathrm{SL}(n), \mathrm{SO}(n), \mathrm{Sp}(n), G_2, F_4, E_6, E_7, E_8$.

It is false in general that maximal compact subgroups of G are conjugate. However, there are **special maximal compact subgroups**, and an irreducible admissible representation of $G(F)$ is called **spherical** if it is fixed by the special maximal compact subgroup. ⌟

Proof: ? □

Prop. (18.12.0.3) [Langland's Formation of the Satake Isomorphism]. If G is split, then $\mathcal{H}_K$ is isomorphic to ring generated by the characters of irreducible analytic f.d. representations of ${}^L G$, and the spherical representations of $G(K)$ are parametrized by the semisimple conjugacy classes in ${}^L G^0$.

If G is non-split but splits over an unramified Galois extension Ω/K, let Φ be the Frobenius element in $G(\Omega/F)$, and consider the cosets $\widehat{G} \subset {}^L G$, then $\mathcal{H}_K$ is isomorphic to the ring of functions on the this coset that are generated by the restrictions of characters of irreducible representations of ${}^L G$, and the spherical representations of $G(F)$ are parametrized by the semisimple conjugacy classes in ${}^L G$ in this coset. ⌟

1 Local Langlands for p-adic GL(n)

References are [M. Harris, R. Taylor: The geometry and cohomology of some simple Shimura varieties], [The Local Langlands Correspondence for GL(n) over p-adic Fields, Wedhorn], [Yao17].

Cor. (18.12.1.1) [LLC for GL(1)].

Local class field theory told us that W_K^{ab} is isometric to $K^\times$, And notice by Schur's lemma, any smooth representation of $K^\times$ is 1-dimensional and factors through some U_K.

And a Weil-Deligne representation is now a continuous $W_K^{\mathrm{ab}} \to \mathbb{C}^*$. but it must factor through some U_K, so these two are equivalent. ⌟

Lemma (18.12.1.2) [Jacquet-Langlands]. Let E/K be a quadratic extension and χ a quasi-character of W_E, $\rho : W_F \to GL(2, \mathbb{C})$ the induced representation of W_F, then $\pi(\rho)$ in(20.6.1.5) exists. ⌟

Proof: Cf.[Bump, P556].? □

Thm. (18.12.1.3) [LLC for GL(n)]. There exists a unique collection of bijections rec_n between sets:

$$\mathrm{rec}_n : \mathrm{Irr}^{\mathrm{adm}}(GL(n,F)) \cong \mathfrak{wd}^{\varphi-ss}_{\dim -n}(W_F).$$

satisfying the following properties:

- For a quasi-character χ of K^*, $\mathrm{rec}_1(\chi) = \chi \circ \mathrm{Art}$.
- For every pair $\pi_1, \pi_2 \in \mathrm{Irr}^{\mathrm{adm}}(GL(n,F))$,

$$L(\pi_1 \times \pi_2, s) = L(\mathrm{rec}_{n_1}(\pi_1) \otimes \mathrm{rec}_{n_2}(\pi_2), s), \quad \varepsilon(\pi_1 \times \pi_2, s) = \varepsilon(\mathrm{rec}_{n_1}(\pi_1) \otimes \mathrm{rec}_{n_2}(\pi_2), s).$$

- For a quasi-character χ of K^* and $\pi \in \mathrm{Irr}^{\mathrm{adm}}(GL(n,K))$, $\mathrm{rec}_n((\chi\circ\det)\otimes\pi) = \mathrm{rec}_n(\pi)\otimes\mathrm{rec}_1(\chi)$.
- For any $\pi \in \mathrm{Irr}^{\mathrm{adm}}(GL(n,F))$ with central character ω, $\det\circ\mathrm{rec}_n(\pi) = \mathrm{rec}_1(\omega)$.
- For any $\pi \in \mathrm{Irr}^{\mathrm{adm}}(GL(n,F))$, $\mathrm{rec}_n(\pi^\vee) = \mathrm{rec}_n(\pi)^*$.

Moreover, these bijections also preserves two more invariants:

- Conductor: $c(\pi) = c(\mathrm{rec}_n(\pi))$.
- Depth: $d(\pi) = d(\mathrm{rec}_n(\pi))$.

⌟

Proof: Cf.[Harris-Taylor] and [Laumon, G., M. Rapoport and U. Stuhler, $\mathcal{D}$-elliptic sheaves and the Langlands correspondence, Invent. Math. 113 (1993), 217-338.] □

Lemma (18.12.1.4) [Plan of Proof]. By Bernstein-Zelevinsky classification(18.11.4.1), it suffices to construct rec_n for irreducible cuspidal representations, then for any $\pi = Q(\Delta_1,\ldots,\Delta_r) \in \mathrm{Irr}^{\mathrm{adm}}(GL(n,F))$, where $\Delta_i = \Delta_i(\pi_i, m_i)$, $\sum n_i m_i = n$, we can define

$$\mathrm{rec}_n(\pi) = \oplus_{i=1}^r \mathrm{Sp}_{m_i}(\mathrm{rec}_{n_i}(\pi_i)).$$

By work of Henniart, it suffices to prove there exist maps rec_n on irreducible cuspidal representations that satisfies these properties, because it will be automatically bijective and unique. His method is to use the numerical local Langlands correspondence. ⌟

Remark (18.12.1.5). it seems Scholze's approach bypasses Henniart numerical local Langlands correspondence. ⌟

Prop. (18.12.1.6). Under the local langlands correspondence(18.12.1.3), $\pi \in \mathrm{Irr}^{\mathrm{adm}}(GL(n,F))$ is

- supercuspidal iff $\mathrm{rec}_n(\pi)$ is irreducible.
- essentially square integrable iff $\mathrm{rec}_n(\pi)$ is indecomposable.
- generic iff $L(\mathrm{ad}\circ\mathrm{rec}_n(\pi), s)$ has no pole at $s = 1$.

⌟

Proof: □

Prop. (18.12.1.7) [Inertia Correspondence]. Under the local langlands correspondence(18.12.1.3), for $\pi, \pi' \in \mathrm{Irr}^{\mathrm{adm}}(GL(n,F))$,

- $\pi|_K \cong \pi'|_K$ iff $\mathrm{rec}_n(\pi)|_{I_F} \cong \mathrm{rec}_n(\pi')|_{I_K}$.
- (Paskunas)Let τ be a Weil-Deligne inertia type of I_K that extends to an n-dimensional irreducible F-semisimple representation of W_K, then there exists a unique irreducible smooth representation σ_τ of K s.t. for any irreducible infinite-dimensional representation π of $GL(n,F)$, $\pi|_K$ contains σ_τ iff $\mathrm{rec}_n(\pi)|_{I_F} \cong \sigma$.

⌟

Proof: □

Prop. (18.12.1.8) [LLC for GL(2)]. Under the classification of $\mathrm{Irr}^{\mathrm{adm}}(GL(2,F))$ given in(18.11.4.4), the corresponding Weil-Deligne representations are

1. For π supercuspidal, $\mathrm{rec}_2(\pi) = (\rho, 0)$, ρ irreducible, by(18.12.1.6).
2. For principal series $\chi_1 \times \chi_2$, $\mathrm{rec}_2(\pi) = (\chi_1 \otimes \chi_2, 0)$.

3. For $1(\chi)$, $\mathrm{rec}_2(\pi) = (\chi \oplus \chi(1), 0)$.
4. For $\pi = \mathrm{St}_2(\chi)$, $\mathrm{rec}_2(\chi) = \mathrm{Sp}_2(\chi) = (\chi \oplus \chi(1), N)$, where N sends χ to $\chi(1)$.

┘

Proof: □

2 Cuspidal Representations

3 Simple Characters

4 Tame Lifting

5 Description of the Langlands Correspondence

19 Shimura Varieties

19.1 Shimura Varieties(Deligne)

Main references are [Lan20], [Mil17b], [Mil11], http://virtualmath1.stanford.edu/~conrad/shimsem/, [Canonical Models of Mixed Shimura Varieties and Automorphic Vector Bundles, Milne].

1 Connected Shimura Varieties

Def. (19.1.1.1)[Connected Shimura Data]. A **connected Shimura datum** is a pair (G, D) where $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/\mathbb{Q}$ is a semisimple algebraic group and D a $G^{\mathrm{ad}}(\mathbb{R})^0$-conjugacy classes of homomorphisms $u : \mathrm{U}(1) \to G^{\mathrm{ad}}_{\mathbb{R}}$ satisfying

SU1: Only $z, 1, z^{-1}$ appear in the character of the complex representation $\mathrm{Ad} \circ u : \mathrm{U}(1) \to \mathrm{Lie}(G^{\mathrm{ad}})_{\mathbb{C}}$.

SU2: $\mathrm{ad}(u(-1))$ is a Cartan involution on $G^{\mathrm{ad}}_{\mathbb{R}}$.?

SU3: G^{ad} has no $\mathbb{Q}$-factor H s.t. $H(\mathbb{R})$ is compact.

⌟

Prop. (19.1.1.2). Let H be an adjoint real Lie group and $u : U(1) \to H$ a homomorphism satisfying SU1, SU2, then the following are equivalent:

- $u(-1) = 1$.
- u is trivial.
- H is compact.

⌟

Proof: 1 $\iff$ 2: If $u(-1) = 1$, then u factors through $\mathrm{U}(1) \xrightarrow{2} \mathrm{U}(1)$, so the characters z, z^{-1} cannot occur in $\mathrm{Ad} \circ u$. The converse is trivial.

1 $\to$ 3: by(9.3.6.19), H is compact iff $\mathrm{ad}(u(-1)) = 1$, which is equivalent to $u(-1) = 1$ as H is adjoint. □

Prop. (19.1.1.3) [Shimura Varieties a la Shimura]. A connected Shimura datum is equivalent to the following data:

- $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/\mathbb{Q}$ semisimple of non-compact type.
- D a Hermitian symmetric domain.
- an action of $G(\mathbb{R})^0$ on D via a surjective homomorphism $G^{\mathrm{ad}}(\mathbb{R})^0 \to \mathrm{Hol}(D)^0$ with compact kernel.

⌟

Proof: Cf.[Mil17b]P45.? □

Prop. (19.1.1.4). Let (G,D) be a connected Shimura datum and X be the $G^{\mathrm{ad}}(\mathbb{R})$-conjugacy class of homomorphisms $\mathbb{S}^1 \to \mathbb{G}_{\mathbb{R}}$ containing D, and D is a connected component of X, with stabilizer $G^{\mathrm{ad}}(\mathbb{R})^0 \subset G^{\mathrm{ad}}(\mathbb{R})$. ⌟

Proof: Cf.[Mil17b]P45. □

Def. (19.1.1.5) [Connected Shimura Varieties]. Let (G,D) be a connected Shimura datum(19.1.1.1), then the map $G^{\mathrm{ad}}(\mathbb{R})^0 \to \mathrm{Hol}(D)^0$ as in(19.1.1.3) has compact kernel, so for any arithmetic subgroup $\Gamma \subset G^{\mathrm{ad}}(\mathbb{R})^0 \cap G^{\mathrm{ad}}(\mathbb{Q})$(15.5.1.1), the image $\overline{\Gamma}$ is an arithmetic subgroup of $\mathrm{Hol}(D)^0$(15.5.2.1), thus we can apply Baley-Borel compactification(12.13.7.4) to get an algebraic structure on $D(\Gamma) = \Gamma\backslash D = \overline{\Gamma}\backslash D$. Moreover, if $\Gamma' \subset \Gamma \subset G^{\mathrm{ad}}(\mathbb{R})^0 \cap G^{\mathrm{ad}}(\mathbb{Q})$ and $\overline{\Gamma'}, \overline{\Gamma}$ are both torsion-free, then by Borel(12.13.7.5), there is a morphism $D(\Gamma') \to D(\Gamma)$.

So for any $\Gamma \in G^{\mathrm{ad}}(\mathbb{R})^0 \cap G^{\mathrm{ad}}(\mathbb{Q})$ s.t. $\overline{\Gamma}$ is torsion-free, $D(\Gamma)$ is called a **connected Shimura variety relative to** (G,D). And the inverse images of these Shimura varieties are called the **connected Shimura variety attached to** (G,D), denoted by $\mathrm{Sh}^0(G,D)$. ⌟

Prop. (19.1.1.6) [Galois Action on Shimura Varieties]. ⌟

2 Shimura Varieties

Def. (19.1.2.1) [Shimura Varieties according to Deligne]. Let $K \subset G(\mathbf{A}^f)$ be a compact open subset, and

$$S_K(\mathbb{C}) = G(\mathbb{Q})\backslash X \times G(\mathbf{A}^f)/K.$$

Then when K is neat**?**(which is true when K is small enough), $S_K(\mathbb{C})$ has the structure of an algebraic variety over $\mathbb{C}$ by Baily-Borel**?**, and has a model $\mathcal{S}_K$ over the reflex field E, by[Milne]. ⌟

Proof: **?** □

3 Siegel Moduler Varieties

Prop. (19.1.3.1) [Abelian Varieties with Polarizations and Level Structures]. For $n, N \in \mathbb{Z}_+, d_1|d_2|\ldots|d_n \in \mathbb{Z}_+$ s.t. $(d_n, N) = 1$, consider the functor

$$\mathcal{A} : \mathcal{S}\mathrm{ch}\,/\mathbb{Z}[\frac{1}{Nd_n}] \to \mathcal{S}\mathrm{et}$$

s.t. for any $S \in \mathcal{S}\mathrm{ch}\,/\mathbb{Z}[\frac{1}{Nd_n}]$, $\mathcal{A}(S)$ is the set of isomorphism classes of triples (A,λ,η) where

- $A \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}^n\,/S$,
- $\lambda : A \to A^\vee$ is a polarization of type $D = \mathrm{diag}(d_1,\ldots,d_n)$.
- $\eta : ((\mathbb{Z}/(N))^{2g}, \mathrm{Std}) \cong (A[N], e_N^\lambda)$ is a symplectic similitude.

⌟

Thm. (19.1.3.2) [$\mathcal{A}$ is Representable]. Situation as in(19.1.3.1), if N is large enough w.r.t. D(when $d_n = 1$, it suffices to have $N \geq 3$), then $\mathcal{A}$ is representable by a smooth quasi-projective scheme over $\mathbb{Z}[\frac{1}{Nd_n}]$. ⌟

Proof: For $S \in \mathcal{S}\mathrm{ch}$, $(A,\lambda) \in \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}^{g,D}/S$, let $\mathcal{L}^\Delta(\lambda) = (\mathrm{id}_A,\lambda)^* p_A$. Then locally on étale nbhd, if $\lambda = \lambda_\mathcal{L}$ for an relative ample line bundle $\mathcal{L}$, then

$$\mathcal{L}^\Delta(\lambda) = [-1]^*\mathcal{L} \otimes \mathcal{L}(15.7.4.6)$$

is also relatively ample(6.5.4.19), and

$$\lambda_{\mathcal{L}^\Delta(\lambda)} = 2\lambda_\mathcal{L}(15.7.4.13).$$

Thus $\mathcal{L}^\Delta(\lambda)^{\otimes 3}$ is relatively very ample(15.7.5.8), and $R^i\,\mathrm{pr}_*\,\mathcal{L}^{\otimes 3} = 0$ for $i \geq 1$. Let $\mathcal{M} = \mathrm{pr}_*\,\mathcal{L}^{\otimes 3} \in \mathcal{Q}\mathcal{C}\mathrm{oh}^{\mathrm{free},6^n d}/S$, where $d = \prod d_i$.

Define a new functor $\mathcal{H}$ that is the same as $\mathcal{A}$ except for that we require a projective trivialization of $\mathcal{M}$. Then $\mathcal{H} \to \mathcal{A}$ is a $\mathrm{PGL}(6^n d - 1)$-torsor. For $X \in \mathcal{H}(S)$, $\mathrm{pr}_*\,\mathcal{L}^{\otimes 3}$ provides a projective embedding $X \subset \mathbb{P}_S^{6^n d-1}$, and for any $r \in \mathbb{Z}_+$, $\mathrm{rank}\,\mathrm{pr}_*\,\mathcal{L}^{\otimes 3r} = 6^n d r^n$, so there is a natural transformation

$$\mathcal{H} \to \underline{\mathrm{Hilb}}^{Q(t),1}_{\mathbb{P}^{6^n d-1}} : X \mapsto (X,e), \quad Q(t) = 6^n d t^n.$$

Then this is an open subfunctor whose image are contained in the moduli of pointed smooth subschemes of $\mathbb{P}^{6^n d-1}$: It is injective because any pointed smooth subscheme has at most one Abelian variety structure(15.7.1.5), and its image is a union of components of the smooth locus of $\underline{\mathrm{Hilb}}^{Q(t),1}_{\mathbb{P}^{6^n d-1}}$: This is because of(15.7.12.12).

Then $\mathcal{H}$ is a smooth quasi-projective variety. For the rest, it needs to use GIT quotient of $\mathcal{H}$ by $\mathrm{PGL}(6^d)$, using the level structure to show stability properties, which I will not cover here. Cf.[Ngo, Shimura Variaties]P15**?**. □

Prop. (19.1.3.3) [Siegel Modular Varieties]. For $k \in \texttt{Field}$, the étale shifification $\mathcal{M}^{g,d}_{\text{ét}}$ of the functor

$$\mathcal{M}^{g,d} : \mathcal{S}\mathrm{ch}/k \to \mathcal{S}\mathrm{et} : X \mapsto \mathcal{A}\mathrm{b}\,\mathcal{V}\mathrm{ar}^{g,\mathrm{polar}=d}/X$$

is representable by a variety $\mathcal{M}^{g,d} \in \mathcal{V}\mathrm{ar}/k$. ⌟

Proof: **?** □

Prop. (19.1.3.4) [Canonical Ample Divisor on $\mathcal{M}^{g,d}$]. There exists a canonical ample divisor on $\mathcal{M}^{g,d}$ given by the determinant of the sheaf of invariant differentials on the universal Abelian variety $\mathcal{A}$. ⌟

Proof: □

Prop. (19.1.3.5). The j-invariant of elliptic schemes define an isomorphism $\mathcal{M}^{1,1}_{\mathbb{Q}} \to \mathbb{A}^1_{\mathbb{Q}}$. ⌟

Proof: **?** □

Prop. (19.1.3.6). Let

$$(V,\psi) = (\mathbb{Q}^{2g}, \langle (a_i),(b_i)\rangle = \sum_{i=1}^{g}(a_i b_{g+i} - a_{g+i}b_i)),$$

and $\widetilde{G} = \mathrm{GSp}(V)$, then the Hermitian symmetric domain $\widetilde{X}$ is the Siegel double space, and for any neat compact open subgroup $\widetilde{K} \subset \widetilde{G}(\mathbf{A}^f)$, the corresponding Shimura variety $\widetilde{S}_{\widetilde{K}}$ is the moduli space of principally polarized g-dimensional Abelian varieties with level-$\widetilde{K}$-structure, which has a model over the reflex field $\mathbb{Q}$. ⌟

4 Hodge Type Shimura Varieties

A Shimura datum (G, X) is called of **Hodge Type** if it admits a closed embedding into some Siegel variety datum $(\widetilde{G}, \widetilde{X})$. Thus it carries a universal Abelian variety.

Prop. (19.1.4.1). If (G, X) is a Shimura datum of Hodge type with an embedding $(G, X) \hookrightarrow (\widetilde{G}, \widetilde{X})$, then there exists a neat subgroup $\widetilde{K} \subset \widetilde{G}(\mathbf{A}^f)$, $K = \widetilde{K} \cap G(\mathbf{A}^f)$ s.t. there is a closed embedding of Shimura varieties

$$S_K \hookrightarrow \widetilde{S}_K \otimes_{\mathbb{Q}} E.$$

⌟

Proof: [Deligne71, Prop1.15]. □

5 PEL Type Shimura Varieties

6 Complex Multiplication

7 Canonical Models

Remark (19.1.7.1) [Miyake-Shih-Shimura/Deligne/Milne-Borovoi]. Delete this?. For a Shimura datum (G, X), attached to each compact open subgroup $K \subset G(\mathbf{A}^f)$, there is a map

$$f_K : \mathrm{Sh}_k(G, X) \to \pi_K$$

where π_K is a the theory of canonical model defines

- a reflex field $E = E(G, X)$, which is a number field.
- A canonical model $(f_K)_0 : \mathrm{Sh}_K(E, G)_0 \to (\pi_K)_0$ of f_K over E, which is uniquely characterized by the reciprocity law at the special points.

and also describes the action of $\mathrm{Aut}(\mathbb{C}/E)$ on π_K. ⌟

Remark (19.1.7.2). Delete this?. The method of constructing the canonical model is the following: When our Shimura variety arises naturally as a moduli space over $\mathbb{C}$, then we can use the action of $\mathrm{Gal}(\mathbb{C}/E)$ on the $\mathbb{C}$-points to define a model of the variety over a specific number field.

The theory of complex multiplication will give us an explicit description of the action on certain special points, called the **reciprocity law** at these points, which will determine the model uniquely. ⌟

Remark (19.1.7.3). Delete this?. A heuristic reason that a Shimura variety has a canonical model is that if it is defined only on a transcendental field, then it can be spread out to give a flat family of varieties. But there are only countably many arithmetic locally symmetric varieties up to isomorphism, so there cannot be a ⌟

8 Automorphic Vector Bundles

9 Shimura Curves

André-Oort Conjecture

Def. (19.1.9.1) [Special Subvarieties]. ⌟

Conj. (19.1.9.2) [André-Oort]. Let S be a Shimura variety. Let $V \subset S$ be a subvariety, then there are only f.m. maximal special subvarieties contained in V. ⌟

Proof: □

19.2 Compactification of Shimura Varieties

1 Baily-Borel Compactifications

2 Smooth Compactifications

19.3 Modular Curves and Isogenies of Elliptic Curves

References are [K-M85] and [Kat73].

1 Moduli Problems

Def. (19.3.1.1) [$\Gamma(N)$-Structure]. Let $S \in \mathcal{S}\mathrm{ch}$ and $E \in \mathcal{E}\mathrm{ll}/S$, a

- **$\Gamma(N)$-structure** on E/S is a homomorphism $\varphi : (\mathbb{Z}/(N))^2 \to \ker([N])(S)$ s.t. there is an equality of effective Cartier divisors
$$E[N] = \sum_{(a,b)\in(\mathbb{Z}/(N))^2} [\varphi((a,b))].$$
- **$\Gamma_1(N)$-structure** on E/S is a homomorphism $\varphi : \mathbb{Z}/(N) \to \ker([N])(S)$ s.t. the effective Cartier divisor
$$\sum_{a\in\mathbb{Z}/(N)} [\varphi(a)].$$
is a subgroup scheme of E.
- **balanced $\Gamma_1(N)$-structure** on E/S is an exact sequence
$$0 \to K \to E[N] \to K' \to 0$$
of group schemes over S s.t. K, K' both has rank N over S.
- **$\Gamma_0(N)$-structure** on E/S is a finite subgroup scheme $K \subset E[N]$ over S that is cyclic of rank n.

⌟

Prop. (19.3.1.2) [Functors]. ⌟

Prop. (19.3.1.3) [Weil-Pairing]. Let $S \in \mathcal{S}\mathrm{ch}$ and $E \in \mathcal{E}\mathrm{ll}/S$ with a $\Gamma(N)$-structure, ⌟

Prop. (19.3.1.4) [Moduli Interpretation of Modular Curves]. The functor $\mathcal{S}\mathrm{ch}/\mathbb{Q} \to \mathcal{S}\mathrm{et}$ that maps S to the isomorphism classes of elliptic curves over S with a $\Gamma(N)$-structure is representable by ⌟

Def. (19.3.1.5) [Atkin-Lehner Involutions]. ⌟

Representability

Prop. (19.3.1.6)[Level Structure Schemes]. For any $S \in \mathcal{S}\mathrm{ch}$, $E \in \mathcal{E}\mathrm{ll}/S$, and $M, N \in \mathbb{Z}_+$ invertible on S, there exists a moduli scheme $S(M,N)$ that is finite étale over S, which represents the moduli problem:
$$S(M,N)(T) = \{\text{monomorphism}\alpha : (\mathbb{Z}/(M) \times \mathbb{Z}/(N))_T \hookrightarrow E_T\}.$$
And denote $S(N) = S(N,N), S_1(N) = S(N,1), S_1'(N) = S(1,N)$.

And also denote the $S_0(N)$ parametrizing $\Gamma_0(N)$-structure. Then it is a quotient of $S_1(N)$. ⌟

Proof: ? □

Prop. (19.3.1.7) [$\mathcal{E}_{0,N}$]. If $k \in \texttt{Field}$ and $(N, \operatorname{char} k) = 1$, then the moduli problem $\mathcal{E}_{0,N}$ of the set of elliptic curves with a cyclic N-subgroup has a coarse moduli scheme M over k. And if $\operatorname{char} k = 0$, M is canonically isomorphic to $Y_0(N)_{\mathbb{Q}} \otimes k$, and the map

$$\mathcal{E}_{0,N}(k) \to M(k) \cong Y_0(N)_{\mathbb{Q}}(k) \xrightarrow{(j, j_N)} \operatorname{Spec} k[X,Y]/\Phi_m(X,Y).$$

is given by $(E, S) \mapsto (j(E), j(E/S))$. ⌟

Proof: ? □

Prop. (19.3.1.8) [$\mathcal{E}_N$]. If $k \in \texttt{Field}$ and $\mathbb{Q}(\zeta) \subset k$, then the moduli problem $\mathcal{E}_N$ of the set of elliptic curves with a a $\Gamma(N)$-structure with Weil pairing ζ_N has a coarse moduli scheme M over k. And if $k = \mathbb{C}$, M is canonically isomorphic to $Y(N)$.

And for $k = \mathbb{Q}(\zeta_N)$, M has good reduction over places away from N. ⌟

Proof: ? □

Cor. (19.3.1.9) [$\mathcal{E}_2$]. The moduli problem $\mathcal{E}_2$ in fact has $\mathbb{A}^1$ as the fine moduli scheme over $\mathbb{Q}$: There is an elliptic curve $E \in \mathcal{E}\mathrm{ll}/\mathbb{A}^1$ given by

$$W_\lambda : y^2 = x(x-1)(x-\lambda), \quad \lambda \in \mathbb{A}^1.$$

And it has a $\Gamma(2)$-structure given by the points $((0,0),(1,0))$. And it can be checked that this is a fine moduli problem.? ⌟

Proof: □

2 Modular Curves

Prop. (19.3.2.1) [Shimura Curves]. For any compact open subgroup $K \subset \mathrm{GL}(2, \mathbf{A}_f)$, there exists a modular curve M_K defined over $\mathbb{Q}$ s.t.

$$M_K(\mathbb{C}) = GL(2,\mathbb{Q})\backslash\mathscr{H}^\pm \times \mathrm{GL}(2, \mathbf{A}_f)/K.$$

And there is a compactification $M_K \hookrightarrow \overline{M}_K$. where $\overline{M}_K$ is a smooth projective curve over $\mathbb{Q}$.

In particular, we can define $X(N), X_1(N)$ and $X_0(N)$. ⌟

Proof: □

Prop. (19.3.2.2) [Integral Modular Curves $Y(N)$ and $X(N)$]. For $N \geq 3$, the functor "isomorphism classes of elliptic curves with a level N structure" is representable by a scheme $Y(N)$ and a universal elliptic curve $E^{\mathrm{uni}}/Y(N)$ with a level N structure α_N.

$Y(N)$ is an affine smooth precurve over $\mathbb{Z}[\frac{1}{N}]$, finite flat of degree $\#\,\mathrm{GL}(2,\mathbb{Z}/(N))/\{\pm 1\}$ over the affine j-line $\mathbb{Z}[\frac{1}{N}, j]$, and étale away from from 0 and 1728.

The normalization $X(N)$ of the projective j-line $\mathbb{P}^1_{\mathbb{Z}[\frac{1}{N}]}$ in $Y(N)$ is a proper smooth precurve over $\mathbb{Z}[\frac{1}{N}]$.

$\Gamma(X(N() = \mathbb{Z}[\frac{1}{N}, \zeta_N]$, and $X(N) \otimes_{\mathbb{Z}[\frac{1}{N}]} \mathbb{Z}[\frac{1}{N}, \zeta_N]$(resp. $Y(N) \otimes_{\mathbb{Z}[\frac{1}{N}]} \mathbb{Z}[\frac{1}{N}, \zeta_N]$) is a disjoint union of $\varphi(n)$ affine(resp. proper) smooth curve over $\mathbb{Z}[\frac{1}{N}, \zeta_N]$.

Let $X(N)^\infty = X(N)\setminus Y(N)$, then $(X(N)^\infty)_{\mathbb{Z}[\frac{1}{N},\zeta_N]}$ is a disjoint union of points, called the **cusps** of $X(N)$. And they naturally correspond to the set of isomorphism classes of level N structures on $\mathrm{Tate}(q)_{\mathbb{Z}((q))\otimes\mathbb{Z}[\frac{1}{N},\zeta_N]}$.

The completion of $X(N)$ along any of the cusp is isomorphic to $\mathrm{Spec}\,\mathbb{Z}[\frac{1}{N},\zeta_N][[q]]$. The completion of the j-line along ∞ is also isomorphic to $\mathrm{Spec}\,\mathbb{Z}[\frac{1}{N},\zeta_N][[q]]$ via $j\mapsto q^{-1}+744+\ldots$. And the projection of these two completions along $X(N)\to\mathbb{P}^1_{\mathbb{Z}[\frac{1}{N}]}$ is just $q\mapsto q^N$.

There is a unique invertible sheave $\omega_{\overline{E^{\mathrm{uni}}}/X(N)}$ on $X(N)$ whose restriction on $Y(N)$ is $\omega_{E^{uni}/Y(N)}$, and at each cusp, it is $\mathbb{Z}[\frac{1}{N},\mu_N]$ multiples of the canonical differential of $\mathrm{Tate}(q^N)$ via the identification as above. ⌟

Proof: ? □

Prop. (19.3.2.3) [Cusps]. Let $M_K^\infty = \overline{M_K}\setminus M_K$ be the cusps, then

$$M_K^\infty(\mathbb{C}) = (\pm\,\mathrm{Unip}(\widehat{\mathbb{Z}}))\setminus \mathrm{GL}(2,\widehat{\mathbb{Z}})/K,$$

and $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$ acts on the cusps by

$$[k]^\tau = [\mathrm{diag}(\chi_{\mathrm{cycl}}(\tau),1)k],\quad k\in\mathrm{GL}(2,\widehat{\mathbb{Z}}).$$

⌟

Proof: ? □

Prop. (19.3.2.4). If $M,N\in\mathbb{Z}_+, M+N\geq 5$, the functor "isomorphism classes of elliptic curves with an injection of $\mathbb{Z}/(M)\times\mathbb{Z}/(N)$" is represented by a scheme $Y(M,N)$ and a universal elliptic curve $E^{\mathrm{uni}}/Y(M,N)$ with a level structure $\alpha:\mathbb{Z}/(M)\times\mathbb{Z}/(N)\hookrightarrow Y(M,N)$. ⌟

Proof: □

Prop. (19.3.2.5). The restriction map

$$H^2_{\mathrm{Mot}}(\overline{M},\mathbb{Q}(2))\to H^2_{\mathrm{Mot}}(M,\mathbb{Q}(2))$$

is injective. ⌟

Proof: Cf.[Scholl, Beilinson's theorem on Modular Curves]P276. □

Def. (19.3.2.6) [Ordinary Locus]. Let $Y(N)^{\mathrm{ord}}$ be the complement of $Y(N)_{\mathbb{Z}}$ of the finite set of supersingular points in characteristic dividing N. Then $Y(N)^{\mathrm{ord}}$ is smooth over $\mathbb{Z}[\mu_N]$. ⌟

Proof: Cf.[Katz-Mazur]Cor10.9.2.? □

Manin-Drinfeld Theorem

Thm. (19.3.2.7) [Manin-Drinfeld Theorem]. Let $\mathcal{C}\in\mathrm{Pic}^0(M_K^c\otimes\mathbb{C})$ be the subgroup of classes of divisors supported on the cusps of $M_K^c(\mathbb{C})$, then $\mathcal{C}$ is finite. ⌟

Proof: □

3 Complex Modular Curves and Jacobians

Prop. (19.3.3.1) [Local Picture]. Let D be the unit disk and Δ be a finite group acting on D and fixing 0, then by Schwarz lemma, Δ is a finite subgroup of $\mathrm{Aut}(D,0)\cong\mathbb{R}/\mathbb{Z}$, so it is a finite cyclic group. If $|\Delta|=m$, then z^m is invariant under Δ and defines a function on $\Delta\backslash D$. It is a homeomorphism from $\Delta\backslash D$ to D, thus defines a complex structure on $\Delta\backslash D$.

Let $X=\{z\in\mathbb{C}|\,\mathrm{Im}(z)>c\}$ and h an integer. Let $\mathbb{Z}$ acts on X by $nz=z+nh$. This action can extend to $X^*=X\cup\{\infty\}$, and we can consider the quotient space $\mathbb{Z}\backslash X^*$. The function $q(z)=e^{2\pi iz/h}$ is a homeomorphism from $\mathbb{Z}\backslash X^*$ onto the open disk of radius $e^{-2\pi c/h}$ and center 0, which defines a complex structure on $\mathbb{Z}\backslash X^*$. ⌟

Lemma (19.3.3.2) [Modular Curves for $\Gamma(1)$]. Let $\mathscr{H}^*=\mathscr{H}\cup\{\infty\}$, the Riemann surface $\Gamma(1)\backslash\mathscr{H}^*$ is compact and of genus 0, so isomorphic to the Riemann surface. ⌟

Proof: We first define a complex structure on $\Gamma(1)\backslash\mathscr{H}$: Let $p:\mathscr{H}\to\Gamma(1)\backslash\mathscr{H}$ be the quotient map, and let Q be a point of $\mathscr{H}$ mapping to P. If Q is not an elliptic point, then we can choose a nbhd of Q that maps isomorphically to a nbhd of P, so we can define the complex structure near P.

If $Q=i$, then the map $z\mapsto\frac{z-i}{z+i}$ maps some open nbhd of i to an open disk D' with center 0, and the action of S is transformed to the action $z\mapsto -z$. By the local picture, $f(z)=(\frac{z-i}{z+i})^2$ is invariant under action of S and defines a complex structure near $p(i)$. Similarly, if $Q=\rho$, then $g(z)=(\frac{z-\rho}{z-\overline{\rho}})^3$ is invariant under the action of ST, and defines a complex structure near $p(\rho)$.

The space $\Gamma\backslash\mathscr{H}$ we get is not compact, and it can be compactified by adding a point ∞, the resulting space is compact because it is a quotient space of $\overline{D}\cup\{\infty\}$, which is compact. And we give a complex structure on the resulting space: The function $q=e^{2\pi iz}$ is a function mapping a nbhd of ∞ in the fundamental domain to an open disk with center 0, and thus giving a complex structure near ∞.

It can be seen directly that $\Gamma(1)\backslash\mathscr{H}^*$ is homeomorphic to a sphere, and then use the fact any Riemann surface of genus 0 is isomorphic to S^1(6.12.8.2). □

Prop. (19.3.3.3) [Modular Curves for Γ]. For a congruence group Γ, the quotient space $\Gamma\backslash\mathscr{H}$ can be compactified to a Riemann surface $X(\Gamma)$ by adjoining n points, where n is the number of cusps of Γ. ⌟

Proof: The quotient space $\Gamma\backslash\mathscr{H}$ can be given a complex structure exactly the same way as $\Gamma(1)\backslash\mathscr{H}$, and it can be compactified by adding $\mathbb{P}^1(\mathbb{Q})$, which has only f.m. orbits under action of Γ, by(20.2.1.13) and the fact Γ has finite index in $\Gamma(1)$. For the complex structure: if h is the smallest positive integer that $T^h\in\Gamma$, then $q=e^{2\pi iz/h}$ is a homeomorphism of a nbhd of ∞ in $\Gamma\backslash\mathscr{H}$ to some open disk of 0, thus defines a complex structure near ∞. For any other cusps α, let $\gamma\in\Gamma(1)$ satisfies $\alpha=\gamma(\infty)$, then $z\mapsto q(\gamma^{-1}(z))$ defines a complex structure near α. □

Def. (19.3.3.4) [Notations]. Let Γ be a congruence subgroup, then we denote

$$Y(\Gamma)=\Gamma\backslash\mathscr{H},\quad X(\Gamma)=\Gamma\backslash\mathscr{H}^*.$$

Also abbreviate $Y(\Gamma(N))$ to $Y(N)$, $X(\Gamma(N))$ to $X(N)$, and $Y(\Gamma_0(N))$ to $Y_0(N)$, and $X(\Gamma_0(N))$ to $X_0(N)$. ⌟

Prop. (19.3.3.5) [Modular Form as Differential Forms]. A holomorphic modular form of degree k in $M_k(\Gamma)$ is just a holomorphic differential form on $X(\Gamma)$ of degree k, and its dimension can be calculated, see Dimension Formulae.

Similarly, an automorphic function for Γ is the same as a function on $X(\Gamma)$(19.3.3.3). In particular, if it is holomorphic and vanishes at cusps, then it is constant. ⌟

Proof: ? □

Cor. (19.3.3.6) [Hauptmodul]. Let Γ be a congruence subgroup with only 1 cusp, a **Haptmodul** is the unique meromorphic modular form that has only a simple pole at the cusp with residue 1. ⌟

Over $\mathbb{C}$

Prop. (19.3.3.7). Let $\mathcal{E}_{0,N}$ be the functor of elliptic curves with a cyclic subgroup of order N, then there is a bijection

$$Y_0(N) = \Gamma_0(N)\backslash\mathscr{H} \cong \mathcal{E}_{0,N}(\mathbb{C}) : z \mapsto (\mathbb{C}/\Gamma(z,1), \Gamma(z,1/N)/\Gamma(z,1)).$$

⌟

Proof: Cf.[Diamond or Milne]. □

Prop. (19.3.3.8). Let $\mathcal{E}_N$ be the functor of elliptic curves with a $\Gamma(N)$ structure of Weil pairing ζ_N, then there is a bijection

$$Y(N) = \Gamma(N)\backslash\mathscr{H} \cong \mathcal{E}_{0,N}(\mathbb{C}) : z \mapsto (\mathbb{C}/\Gamma(z,1); z/N, 1/N).$$

⌟

Proof: Cf.[Diamond]. □

Modular Equations

Prop. (19.3.3.9) [$X_0(N)$, Modular Equations]. The field $C(X_0(N))$ of modular functions for $\Gamma_0(N)$ is generated by $j(z)$ and $j(Nz)$ over $\mathbb{C}$, and the minimal polynomial $F(j,Y)$ of $j(Nz)$ over $\mathbb{C}(j)$ has degree $d = [\mathrm{PSL}(2,\mathbb{Z}) : \overline{\Gamma}_0(N)]$(20.2.3.1), and $F(j,Y) \in \mathbb{Z}[j,Y]$.

When $N > 1$, $F(X,Y)$ is symmetric in X, Y, and when $N = p$ is a prime,

$$F(X,Y) \equiv X^{p+1} + Y^{p+1} - X^pY^p - XY \mod p.$$

⌟

Proof: Cf.[Milne, Modular Forms]P88. □

Cor. (19.3.3.10). The field of functions on $X(1)$ is $\mathbb{C}(j)$. ⌟

Thm. (19.3.3.11). For $E, E' \in \mathcal{E}\mathrm{ll}/\mathbb{C}$, there exists a cyclic isogeny $\alpha : E \to E'$ of degree m iff $\Phi_m(j(E), j(E')) = 0$. ⌟

Proof: Cf.[Cox, P213]. □

Action of Hecke Algebras

Prop. (19.3.3.12) [Double Coset Operators]. There is an action of $\mathcal{R}$ on $X_1(\Gamma)$ ⌟

Modular Jacobians

Def. (19.3.3.13) [Modular Jacobians]. Define $J_1(N) = \mathrm{Jac}(X_1(N))$, $J_0(N) = \mathrm{Jac}(X_0(N))$, which is defined over the same field as the defining field of $X_1(N)$ or $X_0(N)$. ⌟

Eichler-Shimura Relations

4 $X(p)$

[Maz78]Intro contains a lot numerical data for the geometry of $X_0(p)$ and its minimal quotients.

Minimal Quotients of $X(p)$

Prop. (19.3.4.1) [Minimal Quotients of $X(p)$]. Let $p \in \mathbf{P}_{\geq 5}$, then any proper subgroup of $\mathrm{GL}(2,\mathbb{Z}/(p))$ is conjugate to a subgroup of the following:

- $H = B(\mathbb{Z}/(p))$, and $X_H(p) = X_0(p)$, with field of definition $\mathbb{Q}$.
- H is the normalizer of a split Cartan subgroup $\mathrm{diag}(*,*) \coprod \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \mathrm{diag}(*,*)$, and $X_H(p) = X_{\mathrm{split}}(p)$, with field of definition $\mathbb{Q}$. Moreover,
$$g_{\mathrm{split}}(p) = \frac{11 + (p-8)p - 4\left(\frac{-3}{p}\right)}{24}.$$
- H is the normalizer of a non-split Cartan subgroup $\mathbb{F}_{p^2}^\times \subset \mathrm{GL}(2,\mathbb{Z}/(p))$, and $X_H(p) = X_{\mathrm{nonsplit}}(p)$, with field of definition $\mathbb{Q}$. Moreover,
$$g_{\mathrm{nonsplit}}(p) = \frac{23 + (p-10)p + 6\left(\frac{-1}{p}\right) + 4\left(\frac{-3}{p}\right)}{24}.$$
- H is the inverse image of $S_4 \subset \mathrm{PGL}(2,\mathbb{Z}/(p))$, and $X_H(p) = X_{S_4}(p)$, with field of definition $\begin{cases} \mathbb{Q} & , p \equiv \pm 3 \pmod 8 \\ \mathbb{Q}(\chi_p) & , p \equiv \pm 1 \pmod 8 \end{cases}$.
- H is the inverse image of $A_5 \subset \mathrm{PGL}(2,\mathbb{Z}/(p))$ if $p \equiv \pm 1 \pmod 5$, and $X_H(p) = X_{A_5}(p)$, with field of definition $\mathbb{Q}(\chi_p)$.
- H is the inverse image of $A_4 \subset \mathrm{PGL}(2,\mathbb{Z}/(p))$, and $X_H(p) = X_{A_4}(p)$, with field of definition $\mathbb{Q}(\chi_p)$.

The last 4 cases are called **exceptional groups**. ⌟

Proof: □

Cor. (19.3.4.2). $X_{\mathrm{split}}(p)$ corresponds to the problem of classifying elliptic curves with an unordered pair of p-isogenies. And $X_{\mathrm{nonsplit}}(p)$ corresponds to the problem of classifying elliptic curves with a chosen subfield $\mathbb{F}_{p^2}$ in $\mathrm{GL}(2, E[p])$(But the inclusion may be up to conjugacy). ⌟

5 Isogenies of Elliptic Curves

Conj. (19.3.5.1) [Mazur]. is it true that for any $F \in$ `NField`, the j-invariants of an elliptic curve over F with an F-rational cyclic group of order N s.t. $g(X_0(N)) \geq 2$(equivalently, $N > 21$ and $N \neq 24, 25, 27, 32, 36, 49$) ⌟

Proof: □

19.4 Shimura-Taniyama-Weil Conjecture

References are [Ring-theoretic properties of certain Hecke algebras, Taylor-Wiles], [Henri Darmon, Fred Diamond, and Richard Taylor, Fermat's last theorem, Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), Int. Press, Cambridge, MA, 1997, pp. 2 – 140.], http://virtualmath1.stanford.edu/~conrad/modseminar/.

1 Weil Parametrizations

Def. (19.4.1.1) [Weil Parametrizations]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ with conductor $N = N_E$ and Néron differential α, a **Weil parametrization** is a minimal map**?** $\pi : X_0(N) \to E$ over $\mathbb{Q}$ s.t. $\varphi^*\alpha = 2\pi\,\mathrm{i}\, c_E f_E(z)\mathrm{d}z$ for some newform $f \in \mathrm{SF}_2^{\mathrm{new}}(\Gamma_0(N))$. This $c_E \in \mathbb{Q}^\times$ is called the **Manin constant** of E. ⌟

Conj. (19.4.1.2) [Manin]. For any $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$, $c_E = \pm 1$. ⌟

Proof: □

Thm& Conj.Cor. (19.4.1.3) [Manin-S.D]. If $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ is semistable, then $|c_E| \in 2^{\mathbb{Z}_+}$. ⌟

Proof: [Arithmetic of Weil Curves]. □

Thm& Conj.Cor. (19.4.1.4) [Raynaud]. If $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ is semistable, then $\log|c_E|$ is bounded. ⌟

Prop. (19.4.1.5) [Heights and Weil Parametrization]. Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ with a Weil parametrization $\varphi_E : X_0(N) \to E$ and corresponding normalized modular form f_E and Manin constant c_E,then

$$\frac{1}{2}\log\Big(\frac{\deg(\varphi_E)}{[\mathrm{SL}(2,\mathbb{Z}) : \Gamma_0(N)]}\Big) = h_{\mathrm{Fal}}(E/\mathbb{Q}) + \log(4\pi^2||f_E||_{\mathrm{Pet}}) + \log|c_E|.$$

⌟

Proof: let α_E be a Néron differential of E, then $\varphi_E^*\alpha_E = 2\pi\,\mathrm{i}\, c_E f_E(z)\mathrm{d}z$, so

$$\begin{aligned} 4\pi^2|c_E|^2||f_E||_{\mathrm{Pet}}^2 &= \frac{1}{[\mathrm{SL}(2,\mathbb{Z}) : \Gamma_0(N)]}\frac{i}{2}\int_{X_0(N)} \varphi_E^*\alpha_E \wedge \overline{\varphi_E^*\alpha_E} \\ &= \frac{\deg(\varphi_E)}{[\mathrm{SL}(2,\mathbb{Z}) : \Gamma_0(N)]}\frac{i}{2}\int_{E^{\mathrm{an}}} \alpha_E \wedge \overline{\alpha_E} \\ &= \frac{\deg(\varphi_E)}{[\mathrm{SL}(2,\mathbb{Z}) : \Gamma_0(N)] H_{\mathrm{Fal}}^2(E)} (15.13.3.1) \end{aligned}$$

□

Cor. (19.4.1.6) [Lower Bounded for $\deg(\varphi_E)$]. For any $\varepsilon \in \mathbb{R}_+$, there exists $C_\varepsilon \in \mathbb{R}_+$ such that: Suppose $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ with a Weil parametrization $\varphi_E : X_0(N) \to E$ and associated normalized cusp form f_E and Manin constant $c_E = 1$, then

$$\deg(\varphi_E) \ge C_\varepsilon \max(|c_4(E)|^{1/4}, |c_6(E)|^{1/6})^{2-\varepsilon}.$$

⌟

Proof: Use(19.4.1.5). Firstly, by(15.13.3.13), $h_{\mathrm{Fal}}(E/\mathbb{Q}) \ge (1-\varepsilon)\log\max(|c_4(E)|^{1/4}, |c_6(E)|^{1/6}) + O_\varepsilon(1)$. Next, $||f_E|| \ge e^{-4\pi}/(4\pi)$ by(20.2.1.22) and the fact f_E is normalized. Then the assertion follows. □

2 Modularity

Thm. (19.4.2.1)[Eichler-Shimura]. If $f \in S_2(\Gamma_0(N))$ be a Hecke eigenform with integral coefficients, then there exists an elliptic curve $E/\mathbb{Q}$ s.t. $L(E,s) = L(f,s)$(21.2.6.2)(21.3.6.17). ⌟

Proof: □

Prop. (19.4.2.2) [Modular Elliptic Curves]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$, the following are equivalent:

- there exists a normalized Hecke eigenform $f \in S_2(\Gamma_0(N_E))$ with integral coefficients s.t. $L(E;s) = L(f,s)$.
- For some(every) $p \in \mathbf{P}$, $\rho_{E,p}$ is modular.
- There is a non-constant map $X_0(N) \to E$ over $\mathbb{Q}$ for some $N \in \mathbb{Z}_+$.
- E is isogenous to the modular Abelian variety A_f associated to some newform $f \in S_2(\Gamma_0(N_E))$.

And E is called a **modular elliptic curve** if these hold. ⌟

Proof: □

Lemma (19.4.2.3). For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ and $N \in \mathbb{Z}_+$, there is a surjection $X_0(N_E) \to E$ iff there is a surjection $J_0(N) \to E$. ⌟

Proof: If $\varphi : X_0(N) \to E$ is non-zero, then $\varphi_* : J_0(N) \to \mathrm{Jac}(E) \cong E$ is nonzero, by(15.7.10.9). If $\Phi : J_0(N) \to E$ is surjective, then $X_0(N) \xrightarrow{\text{Abel}} J_0(N) \to E$ is also surjective, by looking at the Tate module**?**. □

Lemma (19.4.2.4) [Langland-Tunnell]. If $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ is semistable and $E[\ell]$ is irreducible for some odd prime ℓ, then $E[\ell]$ is modular. ⌟

Lemma (19.4.2.5) [Taylor-Wiles]. If $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ is semistable and ℓ is an odd prime s.t. $E[\ell]$ is irreducible and modular, then T_ℓ is modular. ⌟

Proof: □

Thm. (19.4.2.6) [Modularity Theorem(Shimura-Taniyama1955), Taylor-Wiles/Breuil-Conrad-Diamond-Taylor]. Any $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ is modular(19.4.2.2). ⌟

Proof: Cf.[On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, C. Breuil, B. Conrad, F. Diamond, and R. Taylor]. □

Thm. (19.4.2.7) [Wiles]. The modular deformation ring T is isomorphic to the Galois deformation ring $R_{\overline{\rho}}$. ⌟

Proof: □

Prop. (19.4.2.8) [Elliptic Curves and Modular Forms]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ with conductor N and sign of functional equation w_E, and has L-function $L(E,s) = \sum c_n n^{-s}$. Let $f_E(\tau) = \sum c_n e^{2\pi i \tau}$ be the Mellin transform of $L(E,s)$, then

- f_E is a cuspidal modular form on $S_2(\Gamma_0(N))$.
- f_E is a normalized Hecke eigenfunction, and satisfies $f[w_N]_2 = -w_E f(\tau)$, where w_E is the sign of functional equation of E(21.2.6.4).

- Let ω be an invariant differential form on E, then there exists a finite morphism $\varphi : X_0(N) \to E$ over $\mathbb{Q}$ s.t. $\varphi^*(\omega)$ is a multiple of the differential form on $X_0(N)$ represented by $f(\tau)d\tau$.

⌟

Proof: □

Def. (19.4.2.9) [Manin Constant]. Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ and $\omega \in \mathcal{K}_{E/\mathbb{Q}}$, the **Manin constant** is defined to be the constant $c \in \mathbb{C}$ s.t. $f^*\omega = c \cdot 2\pi\,\mathrm{i}\, f_E dz$. ⌟

19.5 André-Oort Conjecture

References are [Canonical Heights on Shimura Varieties and the André-Oort Conjecture].

19.6 Cohomology of Unitary Shimura Varieties

References are [On the Generic Part of the Cohomology of Compact Unitary Shimura Varieties, Caraiani-Scholze], [On the Generic Part of the Cohomology of Non-Compact Unitary Shimura Varieties, Caraiani-Scholze].

1 Perfectoid Siegel Spaces

Cf.[Torsion in the Cohomology of Locally Symmetric Varieties, Scholze].

Geometric points of $\mathcal{F}l$ are in bijection with principally polarized p-divisible groups $G/\mathcal{O}_C$ with a trivialization of their Tate module.

On geometric points, the Hodge-Tate map is the map sending an Abelian variety over $\mathcal{O}_C$ to its associated p-divisible group.

2 Hodge-Tate Period Map

Given a (G, X) be a Shimura datum?, there is a flag variety we can define an **Borel embedding**

$$\beta : X \to \mathrm{Flag}_{G,\mu}(\mathbb{C}) : [\mu] \in X \mapsto \mathrm{Fil}^\bullet(\mu).$$

where μ is the X is defined over a number field E, called the reflex field of X, where $\mathrm{Fil}^p(\mu)$ for any representation is the direct sum of all subspaces of the type (p', q') with $p' \geq p$.

Choose a Hodge cocharacter $\mathbb{G}_m \to G_{\mathbb{C}}$.

Then P_μ^{std} can be defined to be the subgroup of G stabilizing $\mathrm{Fil}^\bullet(\mu)$, which is a parabolic subgroup.? And dually, we can define $\mathrm{Fil}_\bullet(\mu)$ and P_μ the stabilizer of $\mathrm{Fil}_\bullet(\mu)$.

$M_\mu = C_G(\mu)$ is the Levi component of both parabolics.

Let $Fl_{G,\mu}^{std}(\mathbb{C}) = G(\mathbb{C})/P_\mu^{std}(\mathbb{C})$, then there is a Borel embedding $X \hookrightarrow Fl_{G,\mu}^{std}(\mathbb{C})$.

Example (19.6.2.1) [Siegel Varieties]. A Shimura variety of Hodge Type can be regarded as a moduli space for Abelian varieties with certain Hodge-tensors?. ⌟

For the Siegel variety V, the flag variety $Fl_{\widetilde{G},\widetilde{\mu}}$ parametrizes totally isotropic subspaces $W \subset V$.? [Ana-Scholze]P11.

For $p \in \mathbf{P}$, consider compact open subgroups of the form $K = K^p \times K_p \subset G(\mathbf{A}^{p\infty}) \times G(\mathbb{Q}_p)$.

Fix a place $\mathfrak{p} \in \Sigma_E^p$, let $\mathscr{F}\mathscr{L}_{G,\mu}$ be the adic space associated with $\mathcal{F}l_{G,\mu} \times_E E_{\mathfrak{p}}$?.

Prop. (19.6.2.2) [Hodge-Tate Period Map]. For a Shimura datum of Hodge type (G, X) and any sufficiently small tame lever $K^p \subset G(\mathbf{A}^{p\infty})$, there exists a perfectoid space $\mathcal{S}_{K^p}$ s.t.

$$\mathcal{S}_{K^p} \sim \lim_{K_p} (S_{K^p K_p} \otimes_E E_{\mathfrak{p}})^{\mathrm{ad}},$$

and there is a $G(\mathbb{Q}_p)$-equivariant **Hodge-Tate period map**

$$\pi_{\text{H-T}} : \mathcal{S}_{K^p} \to \mathscr{F}\mathscr{L}_{\widetilde{G},\widetilde{\mu}}$$

which is equivariant w.r.t the natural Hecke action? of $G(\mathbf{A}^{p\infty})$ on the inverse system $\mathcal{S}_{K^p}$ and the trivial action of $G(\mathbf{A}^{p\infty})$ on $\mathscr{F}\mathscr{L}_{\widetilde{G},\widetilde{\mu}}$. ⌟

Proof: Cf.[Scholze, coh of symmetric spaces] or [S-Weinstein] □

Remark (19.6.2.3). This Hodge-Tate map is a p-adic analogue of the Borel embedding, and on closed points it maps an Abelian variety to its Hodge-Tate filtration of its Tate module**?**. ⌟

Prop. (19.6.2.4) [Hodge-Tate Period Map].

- The Hodge-Tate period map(19.6.2.2) factors through $\mathscr{GL}_{G,\mu}$ and the resulting map
$$\pi_{\text{H-T}}: \mathcal{S}_{K^p} \to \mathscr{GL}_{G,\mu}$$
is independent of the choice of the embedding of Shimura data.
- For any μ in the given conjugacy class defined over a finite extension of E, the tensor functor
$$f_p: \mathrm{Rep}(M_\mu) \xrightarrow{\mathrm{pr}^*} \mathrm{Rep}(P_\mu) \to \{G(\mathbb{Q}_p) - \text{equivariant vector bundles on } \mathscr{FL}_{G,\mu}\}$$
$$\xrightarrow{\pi^*_{\text{H-T}}} \{G(\mathbb{Q}_p) - \text{equivariant vector bundles on } \mathcal{S}_{K^p}\}$$
is isomorphic to the tensor functor
$$f_\infty: \mathrm{Rep}(M_\mu) \xrightarrow{\mathrm{pr}^*} \mathrm{Rep}(P^{std}_\mu) \to \{\text{automorphic bundles on } S_K\} \to \{G(\mathbb{Q}_p)\text{−equivariant vector bundles on } \mathcal{S}_{K^p}\}$$
and this isomorphism is independent of the choice of Siegel embedding, and also equivariant for the Hecke action of $G(\mathbf{A}^{p\infty})$.

⌟

3 Newton Stratification on the Flag Variety

4 Geometry of Newton Strata and Igusa Varieties

Def. (19.6.4.1) [$\mathscr{I}_{Mant}$]. The **Igusa variety** $\mathscr{I}_{Mant}$ is defined to be the projective system of $\overline{\mathbb{F}}_p$-schemes $(\mathscr{I}^b_{Mant,K^p,m})_{K^p\to 0, m\in\mathbb{Z}_+}$. ⌟

Prop. (19.6.4.2) [Igusa and Manton Varieties]. The perfect scheme Ig^b is the perfection of $\mathscr{I}^b_{Mant}$, via the natural map $\mathrm{Ig}^b \to \mathscr{I}^b_{Mant}$. ⌟

5 Cohomology of Igusa Varieties

We need to compute the alternating sum of cohomology groups $[H(\mathcal{I}\mathrm{g}^b, \overline{\mathbb{Q}_\ell})]$ as a virtual representation of $G(\mathbf{A}^{p\infty}) \times J_b(\mathbb{Q}_p)$.

It is enough to work with the classical object $\mathscr{I}^b_{Mant}$, because of(19.6.4.2) and the fact perfection doesn't change the étale topos**?**. And by Poincaré duality, it suffices to compute $[H_c(\mathcal{I}\mathrm{g}^b, \overline{\mathbb{Q}_\ell})]$. Sug Woo Shin has a formula expressing this as a sum of stable orbital integrals for G and its elliptic endoscopic groups**?**.

Notation (19.6.5.1).

- Let $F = F^+\mathcal{K}$, where F^+ is a totally real field and $\mathcal{K}$ is an imaginary quadratic field.
- Let $G/\mathbb{Q}$ be a unitary similitude group preserving an alternating Hermitian form $\langle -, - \rangle$ on $V \in \mathcal{V}\mathrm{ect}^n_F$.
- Let $(G, [h])$ be the Shimura datum with reflex field E.

- Let $\mathrm{Spl}_{F/F^+/\mathbb{Q}} = \{p \in \mathbf{P} : \forall v \in S(p) \subset \Sigma_{F^+}, v \text{ splits in } F\}$.
- Let $p \in \mathbf{P}$ be unramified in F and splits in $\mathcal{K}$.
- Let $\mathfrak{p} \in S_E(p)$.
- Let $K = K^p K_p \in G(\mathbf{A}^{p\infty}) \times G(\mathbb{Q}_p)$ be a compact open subgroup where K_p is hyperspecial?. The fact that p is unramified in F means that S_K has good reduction with integral model $\mathscr{S}_K/\mathcal{O}_{E_\mathfrak{p}}$.
- If G be a topological group, denote $\mathrm{Irr}^{\mathrm{adm}}(G)$ the set of isomorphism classes of irreducible admissible representations of G, and $\mathrm{Groth}(G)$ the corresponding Grothendieck group.?

⌟

Notation (19.6.5.2). For $F \in \texttt{NField}$, define $\ker^1(F, G) = \ker(H^1(F, G) \to \prod_{v\in\Sigma_F} H^1(F_v, G)$. ⌟

Let $K \in p\text{-}\texttt{LField}$, and G is an unramified group over K. Choose a hyperspecial group $\mathcal{K} \subset G(K)$, and a Haar measure of $G(K)$ s.t. $\mathrm{Vol}(\mathcal{K}) = 1$. Let $\mathscr{H}^{\mathrm{ur}}(G(K))$ be the subspace of $C_c^\infty(G(K))$ consisting of bi-K-invariant functions.

Def. (19.6.5.3) [Setup]. Suppose some technical conditions:

- all $p \in \mathbf{P}$ ramified in F are contained in $\mathrm{Spl}_{F/F^+/\mathbb{Q}}$.
- G is quasi-split in all finite places.

⌟

Remark (19.6.5.4). These follows from [Compact Unitary at Ramified Split Places, SS13]Chap10.? ⌟

Def. (19.6.5.5) [Endoscopic Triples]. For notation of Langlands dual,Cf.[Borel, Automorphic L-functions, 79]?. There is an action of Gal_F on $\widehat{G}$ given by the choice of slitting data.? An **endoscopic triple** for G is a triple (H, s, η) where

- H/F is a quasi-split connected reductive group,
- $s \in Z(\widehat{H})$,
- $\eta : \widehat{H} \to \widehat{G}$ is an embedding of complex Lie groups.
- $\eta(\widehat{H}) = Z_{\widehat{G}}(\eta(s))^0$.
- The $\widehat{G}$-conjugacy classes of η is fixed by Gal_F.
-

Cf.[Stable Trace Formula for Igusa Varieties, Shin]. ⌟

6 Torsion in the Cohomology of Unitary Shimura Varieties

19.7 Unitary Shimura Varieties

19.8 Supersingular-Loci

19.9 Drinfeld Modules

References are [Elliptic Modules, Drinfeld] and [Introduction to Drinfeld Modules, Hayes].

20 Automorphic Representations & Global Langlands Conjecture

20.1 Automorphic Representations over Archimedean Local Fields

Main References are [Bum98], [Bor97], [Automorphic Forms and L-Functions for the Group $GL(n,\mathbb{R})$, Goldfeld] and [A Course given by Liang Xiao]. Notice that [Bum98] has many gaps, and these gaps can be filled by [Bor97] or [?].

Notation (20.1.0.1).

- Let $K = \mathbb{R}$ or $\mathbb{C}$.
- $G = GL(n,K)^+, G_1 = SL(n,K), K = SO(n,K)$.
- Use notations defined in Arithmetic of Algebraic Groups.
- Use notations defined in Arithmetic Subgroups.
- B is the upper triangular matrices, $N(K)$ the group of unipotent upper triangular matrices in G, T the group of diagonal matrices, $Z(K)$ the group of scalar matrices.
- Define right regular action ρ of G on $C^\infty(G)$, and also the left regular action λ. We will write dX for $X \in \mathfrak{g}$ as the representation of Lie algebra of G via ρ, then it commutes with λ. So it induces a map of $U(\mathfrak{g})$ to the ring of left G-invariant differential operators on G(18.9.1.1).
- Fix a character ψ of K, define a character ψ_N on $N(K)$ by

$$\varphi_N(u) = \psi(\sum_{i=1}^{n-1} u_{i,i+1}).$$

⌟

Notation (20.1.0.2). If $n = 2$,

- G acts on $\mathscr{H}$ through linear fractional transformation(12.12.0.11) and fixes the measure $y^{-2}\mathrm{d}x\mathrm{d}y$. We will denote a, b, c, d the linear functionals on $\mathrm{Mat}(2,\mathbb{R})$ s.t. for $\gamma \in \mathrm{Mat}(2,\mathbb{R})$, $\gamma = \begin{bmatrix} a(\gamma) & b(\gamma) \\ c(\gamma) & d(\gamma) \end{bmatrix}$.
- Use the Lie algebra notations(3.7.2.11):

$$H = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad R = \frac{1}{2}\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}, \quad L = \frac{1}{2}\begin{bmatrix} 1 & -i \\ -i & -1 \end{bmatrix} \quad W = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = iH.$$

and the Casimir element in $\mathcal{Z} = Z(U(\mathfrak{g}))$:

$$\Delta = -\frac{1}{4}(H^2 + 2RL + 2LR).$$

- Let Γ be a discrete subgroup of G that the volume of $\Gamma\backslash\mathcal{H}$ is finite, we may also assume that $-1 \in \Gamma \subset SL(2,\mathbb{R})$.
- Let χ be a character of Γ and ω be a character of the center $Z(\mathbb{R}) \subset G$(the scalar matrices). Assume that $\omega(-1) = \chi(-1)$.

⌟

1 Basics

Prop. (20.1.1.1). In the coordinate(12.12.0.4), we have the following equation:

$$\frac{\partial}{\partial R} = e^{2i\theta}(iy\frac{\partial}{\partial x} + y\frac{\partial}{\partial y} + \frac{1}{2i}\frac{\partial}{\partial\theta}), \quad \frac{\partial}{\partial L} = e^{-2i\theta}(-iy\frac{\partial}{\partial x} + y\frac{\partial}{\partial y} - \frac{1}{2\,\mathrm{i}}\frac{\partial}{\partial\theta}), \quad \frac{\partial}{\partial H} = -i\frac{\partial}{\partial\theta}$$

So in particular

$$\Delta = \frac{\partial^2}{\partial\Delta^2} = -y^2(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}) + y\frac{\partial^2}{\partial x\partial\theta}.$$

⌟

Proof: $H = -iW$, and $\exp(tW) = k_t = \begin{bmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{bmatrix}$, so $dW = \partial/\partial\theta$ is clear.

For dR, first notice that

$$k_\theta \exp(tR) = \exp(e^{2ti\theta}R)k_\theta,$$

as

$$\begin{aligned} k_\theta \exp(tR)k_{-\theta} = C^{-1}\begin{bmatrix} e^{i\theta} & \\ & e^{-i\theta} \end{bmatrix}\exp(te)\begin{bmatrix} e^{-i\theta} & \\ & e^{i\theta} \end{bmatrix} C &= C^{-1}\begin{bmatrix} e^{i\theta} & \\ & e^{-i\theta} \end{bmatrix}\begin{bmatrix} 1 & t \\ & 1 \end{bmatrix}\begin{bmatrix} e^{-i\theta} & \\ & e^{i\theta} \end{bmatrix} C \\ &= C^{-1}\begin{bmatrix} 1 & e^{2i\theta}t \\ & 1 \end{bmatrix} C \\ &= \exp(e^{2i\theta}tR) \end{aligned}$$

where C is the Cayley transformation, notation as in(3.7.2.11),

Now

$$(dRf)(g) = \frac{d}{dt}f(bk_\theta \exp(tR)) = \frac{d}{dt}f(b\exp(e^{2i\theta}tR)k_\theta) = e^{2i\theta}\frac{d}{dt}f(b\exp(tR)k_\theta)$$

Then notice

$$R = 1/2H + \begin{bmatrix} 0 & i \\ 0 & 0 \end{bmatrix} + 1/2\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \exp(tR) \sim k_{t/2} + \begin{bmatrix} 1 & it \\ & 1 \end{bmatrix} + \begin{bmatrix} e^{t/2} & \\ & e^{-t/2} \end{bmatrix}$$

so we get the desired result.

For dL the calculation is similar to that of dR. □

Def. (20.1.1.2) [Cusps]. A **cusp** of Γ is a point in $\mathbb{P}^1(\mathbb{R})$ whose stablizer in Γ contains a non-trivial parabolic element(12.12.0.3).

Let ∞ be a cusp, then $\{\pm 1\}\Gamma_\infty = \{\pm 1\}\langle \begin{bmatrix} 1 & r \\ & 1 \end{bmatrix} \rangle$ for some $r > 1$. Then if $\Gamma_\infty = \langle - \begin{bmatrix} 1 & r \\ & 1 \end{bmatrix} \rangle$, then it is called an **irreducible cusp**, otherwise it is called a **regular cusp**. Similarly, for any other cusp $a = \xi(\infty)$, where $\xi \in SL(2,\mathbb{R})$, we called a is regular/irregular cusp iff ∞ is regular/irregular cusp w.r.t. $\Gamma' = \xi^{-1}\Gamma\xi$. ⌟

Def. (20.1.1.3) [Form Spaces]. Let $C^\infty(\Gamma\backslash G, \chi, \omega)$ be the space of smooth functions $F : G \to \mathbb{C}$ that

$$F(\gamma g) = \chi(\gamma)F(g), \quad \gamma \in \Gamma, g \in G,$$

$$F(zg) = \omega(z)F(g), \quad z \in Z(\mathbb{R}), g \in G.$$

Let the subspace $C_c^\infty(\Gamma\backslash G, \chi, \omega)$ be those functions f that $|f|$ is compactly supported in G_1. Similarly we define $C(\Gamma\backslash G, \chi, \omega)$ and $C_c(\Gamma\backslash G, \chi, \omega)$.

Define $C(\Gamma\backslash G, \chi, k)$ or $C_c(\Gamma\backslash G, \chi, k)$ to be the subspace of $C(\Gamma\backslash G, \chi)$ or $C_c(\Gamma\backslash G, \chi)$ consisting of functions F s.t. $\rho(k_\theta)F = e^{ik\theta}F$.

When ω is the character of $Z(\mathbb{R})$ that $\omega(Z(\mathbb{R}^+)) = 1$, then we denote $C^\infty(\Gamma\backslash G, \chi) = C^\infty(\Gamma\backslash G, \chi, \omega)$. ⌟

Def. (20.1.1.4) [Archimedean Automorphic Forms]. Let the space of **automorphic forms** $\mathcal{A}(\Gamma\backslash G, \chi, \omega)$ be the subspace of $C^\infty(\Gamma\backslash G, \chi, \omega)$ consisting of K-finite and $\mathcal{Z}$-finite functions satisfies the **condition of moderate growth**:

$$|F(g)| < C||g||^N$$

for some $C, N > 0$, where the height on G is induced from the inclusion

$$G \to M(n,\mathbb{R}) \times M(n,\mathbb{R}) : g \mapsto (g, g^{-1}).$$

When ω is trivial on $Z^+(\mathbb{R})$, let $\mathcal{A}(\Gamma\backslash G, \chi, k)$ be the subspace of $\mathcal{A}(\Gamma\backslash G, \chi)$ consisting of functions f that $\rho(k_\theta)(f) = e^{ik\theta}f$.

Automorphic forms are real analytic, by(20.1.1.29). ⌟

Def. (20.1.1.5) [Cuspidal Forms]. If ∞ is a cusp of Γ, then $\{\pm 1\}\Gamma_\infty = \{\pm 1\}\langle \begin{bmatrix} 1 & r \\ & 1 \end{bmatrix} \rangle$, so a $F \in \mathcal{A}(\Gamma\backslash G, \chi, \omega)$ is called **cuspidal** at ∞ iff $\chi(\tau_r) \neq 1$ or

$$\int_0^r F(\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix} g)dx = 0.$$

for any $g \in G$. Notice this is independent of r chosen.

More generally, if a is a cusp of Γ, then choose $\xi \in SL(2,\mathbb{R})$ that $\xi(\infty) = a$, then for $F \in \mathcal{A}(\Gamma\backslash G, \chi, \omega)$, $F'(g) = F(\xi g) \in \mathcal{A}(\Gamma'\backslash G, \chi', \omega)$, where $\Gamma' = \xi^{-1}\Gamma\xi, \chi'(\gamma') = \chi(\xi\gamma'\xi^{-1})$(Because left and right actions commute). Then F is called **cuspidal** at a iff F' is cuspidal at ∞.

The subspace of cuspidal forms is denoted by $\mathcal{A}_0(\Gamma\backslash G, \chi, \omega) \subset \mathcal{A}(\Gamma\backslash G, \chi, \omega)$. ⌟

Prop. (20.1.1.6) [Hecke Operators]. Similar as in(20.2.2.6), we can define the action of $\mathcal{R}_N$ on $C^\infty(\Gamma_0(N)\backslash\mathcal{G},\chi_d)$:

$$T_\alpha(f)(g)=\sum_i\chi_d(\alpha_i)^{-1}f(\alpha_i g),\quad \text{if } \Gamma_0(N)\alpha\Gamma_0(N)=\coprod_i\Gamma_0(N)\alpha_i.$$

and preserves automorphic or cuspidal forms. ⌟

Proof: This is an action because if $\Gamma_0(N)\alpha\Gamma_0(N)=\coprod_i\Gamma_0(N)\alpha_i,\Gamma_0(N)\beta\Gamma_0(N)=\coprod_j\Gamma_0(N)\beta_j$, then $[\alpha][\beta]=\coprod_{i,j}\Gamma_0(N)\alpha_i\beta_j$.

Also $f(\gamma x)=\chi(\gamma)f(x)$ for $\gamma\in\Gamma_0(N)$ because $\Gamma_0(N)\backslash\Gamma_0(N)\alpha\Gamma_0(N)$ is right $\Gamma_0(N)$-invariant. □

$\Gamma\backslash\mathcal{H}$

Def. (20.1.1.7) [Right Weight Action]. There are right actions of $GL(2,\mathbb{R})^+$ on $C^\infty(\mathcal{H})$ defined to by

$$(f|_k g)(z)=(\frac{c\overline{z}+d}{|cz+d|})^k f(\frac{az+b}{cz+d})$$

⌟

Proof: It is an action because**?** □

Def. (20.1.1.8) [Holomorphic Right Weight Action]. Besides the right weight action(20.1.1.7), there is another family of actions:

$$f[\gamma]_k(z)=\deg(\gamma)^{k/2}(cz+d)^{-k}f(\frac{az+b}{cz+d}).$$

⌟

Proof: This is an action because**?** □

Remark (20.1.1.9). This action is related to that of(20.1.1.7) via(20.1.2.9). ⌟

Lemma (20.1.1.10). If f is a holomorphic function on $\mathcal{H}$ and $\gamma\in SL_2(\mathbb{R})$ satisfies $\gamma^n\neq 1$ for any $n\neq 0$ and $f[\gamma]_k=f$, then $f=0$. ⌟

Proof: Use a Cayley transformation $\mathcal{H}\to\mathbb{D}$ to map the fixed point to origin, then γ corresponds to $\mathrm{diag}(\alpha,\alpha^{-1})$, where α is not a root of unity. Then if $f(z)=\sum a_n z^n$, the formula $f[\gamma]_k=f$ says $a_n\alpha^{2n+k}=a_n$. Because $\alpha^{2n+k}\neq 1$ for any n, $a_n=0$ for any n, thus $f=0$. □

Def. (20.1.1.11) [Form Spaces]. if Γ is a discrete subgroup of G_1, let $C^\infty(\Gamma\backslash\mathcal{H},\chi,k)$ be the space of smooth functions on $\mathcal{H}$ that

$$f|_k\gamma=\chi(\gamma)f,\quad \gamma\in\Gamma.$$

And elements in $C^\infty(\Gamma\backslash\mathcal{H},1,0)$ are called **automorphic functions**.

Let the subspace $C_c^\infty(\Gamma\backslash\mathcal{H},\chi,k)$ be those functions f that $|f|$ is compactly supported in $\Gamma\backslash\mathcal{H}$. ⌟

Def. (20.1.1.12) [Behavior at Cusps]. If ∞ is a cusp of Γ, then Γ contains some $\tau_r=\begin{bmatrix}1 & r\\ & 1\end{bmatrix}$ for $r>0$, then a continuous function $f(x+iy)$ on $\mathcal{H}$ is called

- **of at most linear exponential growth** at ∞ iff $|f(x+iy)|=O(e^{Ny})$ for $y\to\infty$

- **of moderate growth** at ∞ iff $|f(x+iy)| = O(y^N)$ for $y\to\infty$.
- **decay rapidly** at ∞ iff $|f(x+iy)|\leq y^{-N}$ for some $N>0$.
- **cuspidal** at ∞ iff either $\chi(\tau_r)\neq 1$ or $\int_0^r f(z+u)du = 0$ for any $z\in\mathscr{H}$.

If f is meromorphic on $\mathscr{H}$ then we have a Fourier expansion

$$f(z) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n z/r} = \sum_{n=-\infty}^{\infty} a_n q^n = T(q).$$

Then f is called **meromorphic/holomorphic/vanishes** at the cusp ∞ iff $T(q)$ does at $q=0$.

The general cusp case is reduced to the ∞ case the same way as in(20.1.1.5). Notice this is independent of possible r chosen. ⌟

Prop. (20.1.1.13) [Hecke Operators]. Similar as in(20.2.2.6), we can define the action of $\mathcal{R}_N$ on $C^\infty(\Gamma_0(N)\backslash\mathcal{H},\chi_d,k)$:

$$T_\alpha(f) = \sum_i \chi_d(\alpha_i)^{-1} f|_k\alpha_i (20.1.1.7), \quad \text{if } \Gamma_0(N)\alpha\Gamma_0(N) = \coprod_i \Gamma_0(N)\alpha_i.$$

and preserves automorphic or cuspidal automorphic forms. ⌟

Proof: This is an action because if $\Gamma_0(N)\alpha\Gamma_0(N) = \coprod_i \Gamma_0(N)\alpha_i, \Gamma_0(N)\beta\Gamma_0(N) = \coprod_j \Gamma_0(N)\beta_j$, then $[\alpha][\beta] = \coprod_{i,j}\Gamma_0(N)\alpha_i\beta_j$.

Also $T_\alpha(f)|_k\gamma = T_\alpha(f)$ for $\gamma\in\Gamma_0(N)$ because $\Gamma_0(N)\backslash\Gamma_0(N)\alpha\Gamma_0(N)$ is right $\Gamma_0(N)$-invariant. □

L^2-Spaces

Def. (20.1.1.14) [Inner Product on Form Spaces]. Notice that if $f,g\in C^\infty(\Gamma\backslash\mathscr{H},\chi,k)$(20.1.1.11), then $f\overline{g}$ is invariant under action of Γ, so we define the Hilbert space $L^2(\Gamma\backslash\mathscr{H},\chi,k)$ as the square-integrable functions in the inner product(20.1.0.1):

$$(f,g) = \int_{\Gamma\backslash\mathscr{H}} f(z)\overline{g}(z)\frac{dxdy}{y^2}.$$

⌟

Def. (20.1.1.15) [L^2-Spaces]. $L^2(\Gamma\backslash G,\chi)$ is defined to be the space of functions on G that is χ-invariant and that is square integrable on $\Gamma\backslash G_1$(because it can descend) with the quotient Haar measure(12.12.0.4)(notice that the absolute value descents to $\Gamma\backslash G_1$) that satisfies conditions in(20.1.1.3).

$L^2_0(\Gamma\backslash G,\chi)$ is the subspace of $L^0(\Gamma\backslash G,\chi)$ of cuspidal elements, where cuspidality is defined the same way as in(20.1.1.5) but in the sense that holds for a.e. g.

$L^2(\Gamma\backslash G,\chi,k)$ be the subspace of $L^2(\Gamma\backslash G,\chi)$ consisting of functions F that $\rho(k_\theta)F = e^{ik\theta}F$. ⌟

Prop. (20.1.1.16). The space $C_c(\Gamma\backslash G,\chi)$ is dense in $L^2(\Gamma\backslash G,\chi)$. ⌟

Proof: Firstly we show $C_c(\Gamma\backslash G,\chi)$ is dense in $L^2(\Gamma\backslash G,\chi)$. Let $\mathcal{F}$ be a Poincaré fundamental domain for Γ in $SL_2(\mathbb{R})$(20.1.1.24), then elements in $C_c(\mathcal{F})$ can be extended to elements of $C_c(\Gamma\backslash G,\chi)$, and in this way, $L^2(\Gamma\backslash G,\chi)$ is identified with $L^2(\mathcal{F})$, so the claim follows from(11.3.8.6). □

Cor. (20.1.1.17). The right regular action of G extends to a continuous unitary representation of G on $L^2(\Gamma\backslash G,\chi)$. $L^2_0(\Gamma\backslash G,\chi)$ is invariant under this representation. ⌟

Proof: We must verify continuity, and this is clear using the proposition because we can choose a compact supported function f to approximate, then the right action is uniformly continuous. The unitaricity is clear. The invariance of $L^2_0(\Gamma\backslash G,\chi)$ is clear. □

Remark (20.1.1.18). Can this be extended to arbitrary locally compact group G?**?**, compare with(11.10.2.9). ⌟

Prop. (20.1.1.19) [Two Form Spaces Equal]. There is an isomorphism of Hilbert spaces

$$\sigma_k : C^\infty(\Gamma\backslash\mathscr{H},\chi,k) \cong C^\infty(\Gamma\backslash G,\chi,k) : (\sigma_k f)(g) = (f|_k g)(i).$$

that preserves the inner products thus induces an isomorphism

$$\sigma_k : L^2(\Gamma\backslash\mathscr{H},\chi,k) \cong L^2(\Gamma\backslash G,\chi,k)$$

And we have(20.1.2.1):

$$\sigma_{k+2}R_k = dR\sigma_k, \quad \sigma_{k-2}L_k = dL\sigma_k, \quad \sigma_k\Delta_k = \Delta\sigma_k.$$

Also cuspidality and the behaviors at the cusps are compatible.

Also if $\Gamma = \Gamma_0(N)$, this isomorphic is compatible with the Hecke operator actions(20.1.1.13) and(20.1.1.6). ⌟

Proof: It can be verified that the inverse of σ_k is given by

$$f(z) = F(\begin{bmatrix} y & x \\ & 1 \end{bmatrix})$$

More precisely, if coordinates(12.12.0.4),

$$F(u,x,y,\theta) = f(x+iy)e^{ik\theta}, \quad f(z) = F(0,x,y,0).$$

Check the left action of Γ and $Z^+(\mathbb{R})$: For Γ actions(20.1.1.11) and(20.1.1.3), this is because $\sigma_k(f)(\gamma g) = f|_k(\gamma g)(i) = \sigma_k(f|_k\gamma)$. Finally check that σ_k preserves inner product, which is immediate from(20.1.1.14)(20.1.1.15) and(12.12.0.4).

The equations between R_k, L_k and R, L are easily verified from(20.1.1.1).

Th action of Hecke operators are compatible by the form $(\sigma_k f)(g) = (f|_k g)(i)$ as above.

Compatibility of behaviors at cusps: It suffices to check growth conditions, and this follows from**??**. □

Technicalities

Prop. (20.1.1.20).

$$k_\theta \begin{bmatrix} y_1 & \\ & y_2 \end{bmatrix} = \begin{bmatrix} y_1y_2D(\theta)^{-1} & \xi D(\theta)^{-1} \\ & D(\theta) \end{bmatrix} k_{\theta'}.$$

where

$$\theta' = \arctan(\frac{y_1}{y_2}\tan\theta), \quad D(\theta) = \sqrt{y_1^2\sin^2\theta + y_2^2\cos^2\theta}, \quad \xi = (y_2^2 - y_1^2)\sin\theta\cos\theta.$$

⌟

Proof: Hint: find θ' first. □

Prop. (20.1.1.21)[Gelfand]. Let $G = GL(n,\mathbb{R})^+, K = SO(n)$, denote $C_c^\infty(K\backslash G/K)$ to be the smooth functions $\varphi \in C^\infty(G)$ that $\varphi(k_1 g k_2) = \varphi(g)$, then $C_c^\infty(K\backslash G/K)$ is commutative. ⌟

Proof: Consider the map $\varphi \mapsto \widehat{\varphi} : \widehat{\varphi}(g) = \varphi(g^t)$, then it is an anti-involution of $C_c^\infty(K\backslash G/K)$:

$$(\widehat{\varphi_1 * \varphi_2})(g) = \int_G \varphi_1(g^t h)\varphi_2(h^{-1})dh = \int_G \widehat{\varphi_2}(h^{-t})\widehat{\varphi_1}(h^t g)dh = \int_G \widehat{\varphi_2}(h)\widehat{\varphi_1}(h^{-1}g)dh = (\widehat{\varphi_2} * \widehat{\varphi_1})(g)$$

But we find $\widehat{\varphi} = \varphi$, because we can use(12.11.5.1), $\varphi(g) = \varphi(d) = \widehat{\varphi}(d) = \widehat{\varphi}(g)$. □

Prop. (20.1.1.22). Let $G = GL(2,\mathbb{R})^+, K = SO(2)$, let σ be a character of K, then $C_c^\infty(K\backslash G/K, \sigma)$ is commutative. ⌟

Proof: The proof is the same as that of(20.1.1.21), but modified as

$$\widehat{\varphi}(g) = \varphi(\begin{bmatrix} -1 & \\ & 1 \end{bmatrix} g^t \begin{bmatrix} -1 & \\ & 1 \end{bmatrix}).$$

□

Siegel Sets

Def. (20.1.1.23) [Siegel Sets]. ⌟

Prop. (20.1.1.24)[Poincaré Fundamental Domain]. Fundamental domain for $\Gamma \subset GL(2,\mathbb{R})$ acting on $\mathscr{H}$ is defined in(11.10.1.35). There is a well-shaped open subset F with a set $F \subset F' \subset \overline{F}$ that F' is a fundamental domain for Γ acting on $\mathscr{H}$.

Notice that if $\mathcal{F}$ is a fundamental domain for Γ in $\mathscr{H} \cong SL_2(\mathbb{R})/SO(2,\mathbb{R})$, then the inverse image of $\mathcal{F}$ is a fundamental domain for Γ in $SL_2(\mathbb{R})$, because a.e. $z \in \mathscr{H}$ is not fixed by any $\gamma \in \Gamma$. ⌟

Proof: Choose a $z \in \mathscr{H}$ which is not fixed by any $\gamma \in \Gamma$, then for any $\gamma \in \Gamma$, draw the circle of points that have the same distance to z and $\gamma(z)$, then the intersection of all the part containing z is a fundamental domain.? □

Prop. (20.1.1.25) [Siegel]. If a Poincare fundamental domain Ω has finite area, then $\partial\Omega$ is a union of f.m. geodesics, and $\partial\overline{\Omega} \cap X$ is finite, and $\Gamma(\partial\overline{\Omega} \cap X)$ is the set of cusps for Γ. ⌟

Proof: The volume of Ω has a relation with the angles of geodesics of Ω, so it can only have f.m. vertices with interior angle$< 0.9\pi$. And the Γ-orbits of these angles intersect $\overline{\Omega}$ at f.m. vertices, which is because they consists of Γ-conjugates with the same distance with z_0, and a compact set meets f.m. geodesics of Ω, because Γz_0 is discrete in $\mathscr{H}$. In particular, Γ has f.m. vertices in the boundary.

Now if Γ has infinitely many vertices, there is a vertex b that all its Γ-conjugates have angles$> 0.9\pi$, then consider the Γ-conjugates of Ω with a vertex b, then all their angle at $b > 0.9\pi$, but this cannot be possible geometrically.

For any cusp x of Γ, suppose the Poincare fundamental domain is defined using z, notice there is a $\gamma \in \Gamma$ that $d(\gamma x, z)$ attains minimum, then γx must by in the boundary of Γ, as $d(\gamma_0 z, \gamma x) = d(z, \gamma x)$, and no other z are closer to γx. □

Prop. (20.1.1.26) [Siegel Set and Fundamental Set]. Siegel set is a nicely shaped substitutes for a fundamental domain:

- Let $a_1,\ldots,a_n \in \mathbb{R}\cup\{\infty\}$ be a representation of the Γ-orbits of cusps of Γ(20.1.1.25), let $\xi \in SL(2,\mathbb{R})$ be chosen that $\xi_i(a_i)=\infty$. If $c>0, d>0$ be chosen suitably, then the set $\cup\xi_i^{-1}\mathcal{F}_{c,d}$ contains a fundamental domain of Γ.
- Suppose ∞ is a cusp of Γ, then if d is large enough, then $\mathcal{F}_d^\infty$ contains a fundamental domain for Γ.

⌟

Proof: 1: $\xi_i\Gamma\xi_i^{-1}$ contains a unipotent subgroup generated by $\begin{bmatrix}1 & \delta_i\\ & 1\end{bmatrix}$, so if $d\geq\delta_i$, then $\xi_i^{-1}\mathcal{F}_{c,d}$ contains a nbhd of the cusp a_i in the fundamental domain F of Γ. so $F-\cup\xi_i^{-1}\mathcal{F}_{c,d}$ is precompact in $\mathcal{H}$, by(20.1.1.25). Now if $c=0, d=\infty$, then $F-\cup\xi_i^{-1}\mathcal{F}_{c,d}=\varnothing$, then this is true for some c,d.

For 2: because ∞ is a cusp, we may assume $F\in\mathcal{H}\cap\{x>0\}$. If d is large, then d will contain each of the pieces $\xi_i^{-1}\mathcal{F}_{c,d}\cap F$ in item1. □

Prop. (20.1.1.27)[Compatibility of Growth Conditions]. Let $G/\mathbb{R}$ be semisimple, f be a function on $\Gamma\backslash G(\mathbb{R})$, then the following are equivalent:

- f is of moderate growth/rapidly decreasing.
- f is of moderate growth/rapidly decreasing on each cusp of Γ.
- f is of moderate growth/rapidly decreasing on each Siegel set $\mathfrak{S}_{i,c,d}$.

⌟

Proof: Cf.[Bor97]P5.11.? We only prove for $SL(2,\mathbb{R})$. □

Harish-Chandra Theorem

Thm. (20.1.1.28) [Harish-Chandra]. If G is semisimple and $f\in C^\infty(G)$ be both K-finite and $\mathcal{Z}$-finite, then

- f is real analytic.
- $U(\mathfrak{g})f$ is an admissible $(\mathfrak{g},K)$-module.
- There exists $\alpha\in C_c^\infty(G)$ that

$$\alpha(kgk^{-1})=\alpha(g),\forall k\in K,\quad f*\alpha=f.$$

- If $|f(g)|<C||g||^N$, then all $U(\mathfrak{g})f$ satisfies similar inequalities with the same N, i.e. f is uniformly of moderate growth.

⌟

Proof: We prove only for $G=\mathrm{SL}(2)$. See [Harish-Chandra, Discrete series for semisimple Lie groups, II. Explicit determination of the characters. Acta. Math. 116 (1966)] or [Gan's notes, P24] for the general case.?

Because W lies in the Lie algebra of K and $W=iH$, the hypothesis implies $\mathcal{R}f$ is f.d., where $\mathcal{R}=\mathbb{C}[\Delta,H]$. Let V be the smallest closed G-invariant subspace of $C^\infty(G)$ containing f and let $V_0=U(\mathfrak{g})f$.

We first prove that

$$V_0=\bigoplus_{-\infty}^{\infty}(V_0\cap V(n)).$$

Notice there is a continuous projection of V onto $V(n)$:

$$E_n\varphi(g) = \frac{1}{2\pi}\int_0^{2\pi} e^{-in\theta}\varphi(gk_\theta)d\theta,$$

because f is K-finite, there is an N s.t. $f = \sum_{n=-N}^{N} E_n f$. Then notice any Df is also K-finite because D is combination of polynomials in R, L, H and R, L, H shift the weights, so the LHS is contained in the RHS. It's left to show now $E_nDf \in V_0$ for any n: E_nDf can be extracted using Lagrange polynomial in H, so it is clearly in V_0.

Next we show $V_0 \cap V(n)$ is of f.d.: Let $f_1, \ldots, f_k$ be a basis of $\mathcal{R}f$, because each f_k is K-finite. so if we use the decomposition of $U(\mathfrak{sl}_2(\mathbb{C}))$(3.7.8.24), only the R, L shifting of the E_nf will be considered, and clearly each $V_0 \cap V(n)$ is of f.d.

Now we show f is analytic: because f is $\mathcal{Z}$-finite, there is an equation $P(\Delta)f = 0$ where P is a monic function, and because Δ commutes with E_k and f is K-finite, $P(\Delta)E_kf = 0$. Now the $P(\Delta)E_kf = P(\Delta_k)E_kf$ by(20.1.1.1) and(20.1.2.1), and $P(\Delta_k)$ is an elliptic operator, so E_kf is analytic by(11.12.8.5).

Now we show V is the closure of V_0: Suppose not, then by Hahn-Banach there is a non-zero continuous linear functional Λ on V that $\Lambda(V_0) = 0$. If $F \in C^\infty(G)$, let $\varphi_F(g) = \Lambda(\rho(g)F)$, and let $\varphi = \varphi_f$. Clearly $dX\varphi_F = \varphi_{dXF}$, so $D\varphi_F = \varphi_{DF}$, which implies φ is $\mathcal{Z}$-finite and smooth, and also K-finite because f does. So by what we have proved, φ is analytic. But now φ is analytic and $D\varphi(1) = \varphi_{Df}(1) = 0$ because $Df \in V_0$, so $\varphi = 0$ by Taylor expansion. So $\Lambda(\rho(g)f) = 0$ for any g, contradiction because $\rho(g)f$ is dense in V.

So actually $V(n) \subset V_0$, because $E_nV_0 = V_0 \cap V(n) \subset V(n)$ is dense, and $V_0 \cap V(n)$ is of f.d., so $V(n) \subset V_0 = V_n$(11.8.1.8) and $V_0 = \oplus V(n)$ is an admissible $(\mathfrak{g}, K)$-module.

Let J be the convolution algebra(because G is unimodular) of functions α that $\alpha(kgk^{-1}) = \alpha(g)$, then it can be checked that convolution $- * \alpha$ commutes with action of K, so $f * J$ is in the same K-type space as f, thus K-finite and in a f.d. space.

Now we can approximate f by $f * J$: choose a Dirac sequence $\{\alpha_n\} \in C_c^\infty(G_1)$, we may replace $\{\alpha_n\}$ by the function $\beta_n(g) = \int_K \alpha_n(k^{-1}gk)dk$ to obtain a Dirac sequence in J. Then $f * \alpha_n \to f$ uniformly on compact sets. But $f * J$ is f.d., so there are some $f * \alpha = f$.

Finally for the growth estimate, it suffices to check for $D \in \mathfrak{g}$. Then $dX(f) = dX(f * \alpha) = f * (dX\alpha)$, from which the estimate is clear. □

Cor. (20.1.1.29) [Automorphic Forms Generate Admissible $(\mathfrak{g}, K)$-Modules]. The space $\mathcal{A}(\Gamma\backslash G, \chi, \omega)$ and $\mathcal{A}_0(\Gamma\backslash G, \chi, \omega)$ are stable under the action of $U(\mathfrak{g})$, and for $f \in \mathcal{A}(\Gamma\backslash G, \chi, \omega)$, f is analytic and $U(\mathfrak{g})f$ is an admissible $(\mathfrak{g}, K)$-module.

Moreover, if f satisfies condition of moderate growth(20.1.1.4) and $D \in U(\mathfrak{g})$, then Df satisfies similar conditions with the same constant N. ⌟

Proof: It suffices to prove for $\mathcal{A}(\Gamma\backslash G, \chi, \omega)$ because the cuspidality condition is clearly preserved by right action.

We want to use Harish-Chandra theorem(20.1.1.28) on $G(K)/Z(K)$. Now $|f|$ is constant on each fiber of $G(K) \to G(K)/Z(K)$. it suffices to compare the norm on $G(K)$ and $G(K)/Z(K)$.

We do this only for $GL(2, \mathbb{R})$**?**

The condition of moderate growth is compatible because the minimal $||g||$ in a $Z(\mathbb{R})$-orbit is achieved when $\deg g = 1$(20.1.1.4). So all the assertion follows from that of(20.1.1.28) and its proof. □

2 Maass Forms

Maass Forms

Def. (20.1.2.1) [Maass Operator]. A **Maass differential operators** on $C^\infty(\mathcal{H})$ is defined to be

$$R_k = (z-\overline{z})\frac{\partial}{\partial z}+\frac{k}{2} = iy\frac{\partial}{\partial x}+y\frac{\partial}{\partial y}+\frac{k}{2},\quad L_k = -(z-\overline{z})\frac{\partial}{\partial \overline{z}}-\frac{k}{2} = -iy\frac{\partial}{\partial x}+y\frac{\partial}{\partial y}-\frac{k}{2}$$

and

$$\Delta_k = -y^2(\frac{\partial^2}{\partial x^2}+\frac{\partial^2}{\partial y^2})+iky\frac{\partial}{\partial x} = -L_{k+2}R_k-\frac{k}{2}(1+\frac{k}{2}) = -R_{k-2}L_k+\frac{k}{2}(1-\frac{k}{2})$$

Δ_k is a symmetric(unbounded) operator on $L^2(\mathcal{H})$ with domain $C_c^\infty(\mathcal{H})$. ⌟

Proof: For the formula:?

For the symmetry: composed with the measure, the order2 part is just the ordinary Laplacian, and the order 1 part becomes $iy^{-1}\frac{\partial}{\partial x}$, then notice

$$\int_{\mathcal{H}} iy^{-1}(\frac{\partial f}{\partial x}\overline{g}+f\frac{\partial \overline{g}}{\partial x})dxdy = i\int_{\mathcal{H}} d(y^{-1}f\overline{g}dy) = 0$$

as f,g are compactly supported. □

Prop. (20.1.2.2) [Maass Operator and Weight Action]. For $f\in C^\infty(\mathcal{H}), g\in G$,

$$(R_kf)|_{k+2}g = R_k(f|_kg),\quad (L_kf)|_{k-2}g = L_k(f|_kg),\quad (\Delta_kf)|_kg = \Delta_k(f|_kg)$$

⌟

Proof: For R_k, because scalar doesn't matter, we may assume $g\in SL_2(\mathbb{R})$, and let $w=\frac{az+b}{cz+d}$, then

$$\frac{\partial}{\partial z} = \frac{\partial w}{\partial z}\frac{\partial}{\partial z} = (cz+d)^{-2}\frac{\partial}{\partial w},\quad (w-\overline{w}) = \frac{z-\overline{z}}{|cz+d|^2}.$$

So

$$(w-\overline{w})\frac{\partial}{\partial w} = (\frac{(cz+d)^2}{|cz+d|^2})(z-\overline{z})\frac{\partial}{\partial z}.$$

And for any smooth function $\varphi\in C^\infty(\mathcal{H})$,

$$(z-\overline{z})\frac{\partial}{\partial z}((\frac{c\overline{z}+d}{|cz+d|})^k\varphi) = (z-\overline{z})(\frac{c\overline{z}+d}{|cz+d|})^k\frac{\partial\varphi}{\partial z}+\frac{k}{2}[(\frac{c\overline{z}+d}{|cz+d|})^{k+2}-(\frac{c\overline{z}+d}{|cz+d|})^k]\varphi.$$

This is because

$$\frac{\partial}{\partial z}|cz+d| = \frac{c}{2}\frac{|cz+d|}{cz+d},\quad \frac{\partial}{\partial z}(\frac{c\overline{z}+d}{|cz+d|})^k = -\frac{k}{2}c(z-\overline{z})\frac{(c\overline{z}+d)^k}{|cz+d|^k(cz+d)} = \frac{k}{2}[(\frac{c\overline{z}+d}{|cz+d|})^{k+2}-(\frac{c\overline{z}+d}{|cz+d|})^k].$$

Thus,

$$\begin{aligned}R_k(f|_kg) &= [(z-\overline{z})\frac{\partial}{\partial z}+\frac{k}{2}](\frac{c\overline{z}+d}{|cz+d|})^kf(w) = [(z-\overline{z})(\frac{c\overline{z}+d}{|cz+d|})^k\frac{\partial}{\partial z}+\frac{k}{2}(\frac{c\overline{z}+d}{|cz+d|})^{k+2}]f(w)\\ &= (\frac{c\overline{z}+d}{|cz+d|})^{k+2}[(w-\overline{w})\frac{\partial}{\partial w}+\frac{k}{2}]f(w) = ((R_kf)|_{k+2}g)(z).\end{aligned}$$

The case of L_k is similar, and Δ_k follows. □

Cor. (20.1.2.3). The operator R_k, L_k, Δ_k maps functions between $C^\infty(\Gamma\backslash\mathscr{H},\chi,k)$ and arises and decreases weights respectively. ⌟

Prop. (20.1.2.4). For $f\in C^\infty(\Gamma\backslash\mathscr{H},\chi,k), g\in C^\infty(\Gamma\backslash\mathscr{H},\chi,k+2)$, if one of them decays rapidly at all cusps, then(20.1.1.14)

$$(R_kf,g)=(f,-L_{k+2}g).$$

In particular, $\Delta_k=-L_{k+2}R_k-\frac{k}{2}(1+\frac{k}{2})$ is symmetric on the subspace of $L^2(\Gamma\backslash\mathscr{H},\chi,k)$ consisting of rapidly decaying functions(Δ is unbounded and defined only on $C^\infty(\Gamma\backslash\mathscr{H},\chi,k)$ now, but will be extended to $L^2(\Gamma\backslash\mathscr{H},\chi,k)$ in(20.1.4.5) when $\Gamma\backslash\mathscr{H}$ is compact). ⌟

Proof: Let $\omega=y^{-1}f(z)\overline{g(z)}d\overline{z}$. It can be shown by definition and using(11.4.1.9) that $\omega(\gamma z)=\omega(z)$, so ω descends to a differential form on $\Gamma\backslash\mathscr{H}$, and because one of f,g decays rapidly at all cusps,

$$\begin{aligned}0=\int_{\Gamma\backslash\mathscr{H}}d(y^{-1}f(z)\overline{g(z)}d\overline{z})&=\int_{\Gamma\backslash\mathscr{H}}[\frac{\partial}{\partial y}(y^{-1}f\overline{g})+i\frac{\partial}{\partial x}(y^{-1}f\overline{g})]dx\wedge dy\\&=\int_{\Gamma\backslash\mathscr{H}}[(iy\frac{\partial f}{\partial x}+y\frac{\partial f}{\partial y})\overline{g}-\overline{(iy\frac{\partial g}{\partial x}-y\frac{\partial g}{\partial y})}f-f\overline{g}]\frac{dxdy}{y^2}\\&=\int_{\Gamma\backslash\mathscr{H}}[(R_kf)\overline{g}+f\overline{(L_{k+2}g)}]\frac{dxdy}{y^2}.\end{aligned}$$

so the conclusion follows. □

Cor. (20.1.2.5). If λ is an eigenvector of Δ_k on $C^\infty(\Gamma\backslash H,\chi,k)$, then either $\lambda=\frac{l}{2}(1-\frac{l}{2})$, where $1\le l\le k$ and $l\equiv k \mod 2$, or $\lambda\ge\frac{\varepsilon}{2}(1-\frac{\varepsilon}{2})$, where $\varepsilon=0$ or 1 that $k\equiv\varepsilon \mod 2$. In particular, eigenvalues of Δ_0 are≥ 0 and eigenvalues of Δ_1 are $\ge 1/4$. ⌟

Proof: This can be done by repeatedly using $\Delta_{k-2}L_k=L_k\Delta_k$ to reduce Δ_ε, or can be deduced from(20.1.4.11). □

Def. (20.1.2.6) [Maass Forms]. A twisted **Maass Form** of weight k and parameter s for Γ is an element in $C^\infty(\Gamma\backslash\mathscr{H},\chi,k)$(20.1.1.11) that is an eigenform for Δ_k of eigenvalue $\lambda=\frac{1}{4}-s^2$ and is of moderate growth at cusps of Γ(20.1.1.12). The space of Maass forms are denoted by $\mathcal{A}_{Maass}(\Gamma\backslash\mathscr{H},\chi,k)$. The space of cuspidal Maass forms are denoted by $\mathcal{A}_{CuspMaass}(\Gamma\backslash\mathscr{H},\chi,k)$.

A Maase form of weight 0 and $\chi=1$ is sometimes just a Maass form. The space of Maass form is denoted by $\mathcal{A}_{\mathrm{Maass}}(\Gamma\backslash\mathscr{H})$. ⌟

Def. (20.1.2.7) [Weak Maass Forms]. A **weak Maass form** of weight k and parameter s for Γ is an element in $C^\infty(\Gamma\backslash\mathscr{H},\chi,k)$(20.1.1.11) that is an eigenform for Δ_k of eigenvalue $\lambda=\frac{1}{4}-s^2$ and is of at most linear exponential growth at cusps of Γ(20.1.1.12). A **harmonic Maass form** is a Maass form of eigenvalue $\lambda=\frac{1}{4}-s^2$ where s is an integer. ⌟

Prop. (20.1.2.8) [Hecke Operators on Maass Forms]. If $\Gamma=\Gamma_0(N)$, the space of Maass forms is stable under the action of the Hecke algebra on $C^\infty(\Gamma_0(N)\backslash\mathscr{H},\chi,k)$(20.1.1.13), by(20.1.2.2). ⌟

Def. (20.1.2.9) [Holomorphic Modular Forms as Maass Forms]. There is a bijection

$$M_k(\Gamma,\chi)\cong\mathcal{A}_{Maass}(\Gamma\backslash\mathscr{H},\chi,k)^{L_k=0}:f\mapsto y^{k/2}f$$

that induces a bijection

$$S_k(\Gamma,\chi)\cong\mathcal{A}_{CuspMaass}(\Gamma\backslash\mathscr{H},\chi,k)^{L_k=0}.$$

⌟

Proof: Direct calculation shows $L_k(y^{k/2}f(z)) = 2iy^{(k+2)/2}\frac{\partial}{\partial\bar{z}}f(z)$, and by(11.4.1.9),

$$(\mathrm{Im}(z)^{k/2}f(z))|_k\gamma = (\frac{c\bar{z}+d}{|cz+d|})^k\,\mathrm{Im}(\gamma z)^{k/2}f(\gamma z) = (\frac{c\bar{z}+d}{|cz+d|})^k\cdot\frac{\mathrm{Im}(z)^{k/2}}{|cz+d|^k}f(\gamma z)$$
$$= \mathrm{Im}(z)^{k/2}(cz+d)^{-k}f(z) = \mathrm{Im}(z)^{k/2}(f[\gamma]_k)(z)$$

so their invariant properties are compatible. Also, if f is a holomorphic modular form, then each $y^{k/2}f[\gamma]_k$ is bounded by a polynomial of y at ∞, and conversely, if $f(q)$ is bounded by a polynomial of $\log(1/|q|)$, then**??** shows f is holomorphic at each cusp. And the cuspidal condition

$$\int_0^r \mathrm{Im}(z)^{k/2}f(z+u)du = \mathrm{Im}(z)^{k/2}\int_0^r f(z+u)du = 0$$

just means f is a cusp form. □

Prop. (20.1.2.10) [Non-holomorphic Eisenstein series is a Maass Form]. The non-holomorphic Eisenstein series $E(s,\nu+1/2)$ is a Maass form of parameter ν for $\Gamma(1)$. ⌟

Proof: $E(s,\nu+1/2)$ is automorphic and of moderate growth by(21.1.1.3) and(21.1.1.1).

To show $E(s,\nu+1/2)$ is an eigenfunction of Δ, if $\mathrm{Re}(\nu) > 1/2$, notice $\Delta(y^{\nu+1/2}) = (\frac{1}{4}-\nu^2)y^{\nu+1/2}$, and Δ is invariant under action of $SL(2,\mathbb{Z})$, thus each $\mathrm{Im}(\gamma(y^{\nu+1/2}))$ is an eigenfunction for Δ of eigenvalue $\frac{1}{4}-\nu^2$, so the same is true for $E(s,\nu+1/2)$.

For general ν, this can be seen from the Fourier coefficients of $E(s,\nu+1/2)$(21.1.1.2):**?** □

Prop. (20.1.2.11) [Maass Forms as Automorphic Forms]. If $f\in\mathcal{A}_{\mathrm{Maass}}(\Gamma\backslash\mathscr{H},\chi,k)$, then $\sigma_k(f)\in C^\infty(\Gamma\backslash G,\chi,k)$(20.1.1.19), and is an eigenform of Δ. In particular it is K-finite, $\mathcal{Z}$-finite, of moderate growth by(20.1.1.19), and it is cuspidal iff $\sigma_k(f)$ is cuspidal, so $\sigma_k(f)\in\mathcal{A}(\Gamma\backslash G,\chi,k)$. And f is cuspidal iff $\sigma_k(f)$ is cuspidal.

In fact, there are a bijections

$$\mathcal{A}_{\mathrm{Maass}}(\Gamma\backslash H,\chi,k,\lambda)\cong\mathcal{A}(\Gamma\backslash G,\chi,k,\lambda),\quad \mathcal{A}_{\mathrm{Maass}}(\Gamma\backslash H,\chi,k)\cong\mathcal{A}(\Gamma\backslash G,\chi,k)^{\Delta-ss}$$

$$\mathcal{A}_{CuspMaass}(\Gamma\backslash H,\chi,k)\cong\mathcal{A}_0(\Gamma\backslash G,\chi,k),\quad \mathcal{A}_{CuspMaass}(\Gamma\backslash H,\chi)\cong\mathcal{A}_0(\Gamma\backslash G,\chi)=L^2_0(\Gamma\backslash G,\chi)^{K-\mathrm{fin}}.$$

this is because when f is cuspidal, Δ is semisimple on the finite dimensional subspace $\mathcal{Z}f$ because of the spectral decomposition of $L^2_0(\Gamma\backslash G,\chi,k)$(20.1.4.8). ⌟

Cor. (20.1.2.12) [Modular Forms as Automorphic Forms]. Combine this and(20.1.2.9), we get a bijection

$$M_k(\Gamma,\chi)\cong\mathcal{A}(\Gamma\backslash G,\chi,k)^{L=0}$$

that induces a bijection

$$S_k(\Gamma,\chi)\cong\mathcal{A}_0(\Gamma\backslash G,\chi,k)^{L=0}.$$

⌟

Cor. (20.1.2.13) [Finitely Many Maass Forms of Given Type]. $\dim\mathcal{A}_{\mathrm{Maass}}(\Gamma_0(N)\backslash\mathscr{H},\chi,k,\lambda) < \infty$. ⌟

Proof: This follows from(20.1.1.29). □

Conj. (20.1.2.14) [Selberg Conjecture]. Let Γ be a congruence subgroup, for any cuspidal Maass form f, the eigenvalue λ of Δ_0 satisfies $\lambda\geq 1/4$, or equivalently, the parameter s is purely imaginary. In this case, the cuspidal representation generated by f is tempered.

This conjecture is true for $\Gamma=\Gamma(1)$ but wrong for some other congruence subgroups. ⌟

Harmonic Maass Forms

References are [Harmonic Maass Forms, Mock Modular Forms, And Quantum Modular Forms, Ken Ono], [Harmonic Maass Forms and Mock Modular Forms Theory and Applications].

Def. (20.1.2.15) [Harmonic Maass Forms]. A **harmonic Maass form** is a weak Maass form(20.1.2.7) of eigenvalue $\frac{k}{2}(1-\frac{k}{2})$, where k is an integer.

Any modular form corresponds to a harmonic Maass form, by(20.1.2.9). ⌟

Def. (20.1.2.16) [Mock Modular Forms]. A **Mock modular form** is the holomorphic part of a harmonic Maass form. ⌟

3 Whittaker Models

Def. (20.1.3.1)[Whittaker Function Space]. For $\psi \in \widehat{\mathbb{R}}$, denote $W_\psi =$ the space of smooth functions f on $GL(n,\mathbb{R})^+$ that satisfies

$$f(ug) = \psi_{\mathrm{Unip}(n)}(u)f(g), \quad u \in \mathrm{Unip}(n)$$

A function $f \in W$ is called:

- of **moderate growth** if for any compact set $\Omega \subset G$, $|f(\begin{bmatrix} y & \\ & 1 \end{bmatrix} g)| < C|y|^k$ for some $C, k > 0$ for any $g \in \Omega$ when $|y| \to \infty$.
- **rapidly decreasing** if for any compact set $\Omega \subset G$ and $k \in \mathbb{R}$, $|f(\begin{bmatrix} y & \\ & 1 \end{bmatrix} g)| < C|y|^k$ for some C for any $g \in \Omega$ when $|y| \to \infty$.

⌟

Lemma (20.1.3.2) [Whittaker Function]. Let $\mu, \lambda \in \mathbb{C}$ and $k \in \mathbb{Z}$. Let $W(\lambda,\mu,k)$ be the space of functions $f \in W$(20.1.3.1) on G s.t. $\Delta f = \lambda f$, $If = \mu f$, $f \in (C^\infty(G))^k$ and f is of moderate growth, then $W(\lambda,\mu,k)$ is 1-dimensional, and functions in this space are actually rapidly decreasing and analytic.

Moreover, the operators R, L map $W(\lambda,\mu,k)$ into $W(\lambda,\mu,k+2)$, $W(\lambda,\mu,k-2)$ respectively.

Also, for $|y| \to 0$ and μ imaginary, $W(\lambda,\mu,k)$ is bounded by a $|y|^{-1/2}$ for some $\varepsilon > 0$. ⌟

Proof: For $f \in W(\lambda,\mu,k)$, in coordinate(12.12.0.4), we have

$$f(g) = u^\mu \psi(x) e^{ik\theta} w(y), \quad w(y) = f(\begin{bmatrix} y^{1/2} & \\ & y^{-1/2} \end{bmatrix})$$

Thus it suffices to study the behavior of $w(y)$. By the expression of Δ(20.1.1.1), if $\psi(x) = e^{iax}$, then

$$w'' + (-a^2 + \frac{k}{2y} + \frac{\lambda}{y^2})w = 0$$

And this is the Whittaker's equation, and the only moderate growth function is rapidly decreasing and analytic. This is by direct calculation in [A course of Modern Analysis, Whittaker/Watson(1927)]**?**.

For the action of R, L, they preserve W because they are right actions. And Rf, Lf have the same eigenvalue of Δ, I because Δ, I are in the center of $U(\mathfrak{g})$. They shift the weight by(20.1.1.19) and(20.1.2.2). □

Prop. (20.1.3.3) [Uniqueness of Whittaker Models for $GL(2,\mathbb{R})$]. For $(\pi, V) \in \mathrm{Irr}^{\mathrm{adm}}((\mathfrak{g}, K))$, there exists at most one space $W(\pi,\psi) \in W$ consisting of K-finite functions $f \in W$ that is of moderate growth, and is invariant under the action of $U(\mathfrak{g})$ and K, and is infinitesimal equivalent to (π, V).

Moreover, functions in $W(\pi,\psi)$ are actually rapidly decreasing and analytic. The space $W(\pi,\psi)$ is called the **Whittaker model** of π, if it exists. ⌟

Proof: By(18.9.3.9), Δ, I acts by scalars λ,μ on V. By(18.9.3.26) or(18.9.3.34) if $V^k \neq 0$, then $\dim V^k = 1$. If $V^k \neq 0$, then the image of V^k under the isomorphism with $W(\pi,\psi)$ is in the space $W(\lambda,\mu,k)$. Thus $W(\pi,\psi)$ is the direct sum of the $W(\lambda,\mu,k)$ for all k that $V^k \neq 0$, so uniquely determined by(20.1.3.2). And the rapid decreasing and analytic properties are also consequences of(20.1.3.2). □

Prop. (20.1.3.4). If $(\pi, V) \in \mathrm{Irr}^{\mathrm{adm}}((\mathfrak{g}, K))$ has a Whittaker model, then there exists some $\xi \in V$ that $W_\xi(1) \neq 0$. ⌟

Proof: Because K intersect each connected component of G, we can assume some W_ξ is non-zero on K^0, thus by analyticity(20.1.3.3), its derivatives at 1 are not identically 0, thus there exists some $D \in U(\mathfrak{g})$ that $DW_\xi(1) = W_{D\xi}(1) \neq 0$. □

Prop. (20.1.3.5) [Whittaker Models for $GL(n,\mathbb{C})$]. This result is true if $\mathbb{R}$ is replaced by $\mathbb{C}$. ⌟

Proof: Cf.[Automorphic Forms on GL(2), Jacquet/Langlands (1970) Thm5.3. P232]?. □

Prop. (20.1.3.6) [Fourier-Maass Expansion]. ⌟

Proof: □

Cor. (20.1.3.7) [Rapidly Decreasing]. Cuspidal automorphic Forms are rapidly decreasing at any Siegel set. ⌟

Proof: Cf.[Gan's Notes, P26].? □

Prop. (20.1.3.8) [Existence of Whittaker Models]. The Whittaker model exists for the ⌟

Prop. (20.1.3.9) [Shalika's Local Multiplicity One Theorem]. Given a unitary irreducible representation V of $GL(n,F)$, a **Whittaker functional** on V^∞ is a $N(F)$-map $\lambda : V^\infty \to \psi_N$.

Then the space of Whittaker functionals on V^∞ is at most 1-dimensional. ⌟

Proof:

□

4 The Spectral Problem

The Spectral Problems for $\Gamma\backslash\mathscr{H}$ Compact

Def. (20.1.4.1). In this subsection we assume $\Gamma\backslash G_1$ is compact, or equivalently $\Gamma\backslash\mathscr{H}$ is compact, because K is compact. This condition makes $C^\infty(\Gamma\backslash\mathscr{H},\chi) = L^2(\Gamma\backslash\mathscr{H},\chi)$, and will make the decomposition having only discrete parts(20.1.4.2). ⌟

Prop. (20.1.4.2) [$L^2(\Gamma\backslash G,\chi)$ Totally Decomposable]. The space $L^2(\Gamma\backslash G,\chi)$ decomposes into a Hilbert space direct sum of subspaces that are invariant and irreducible under the right regular action ρ. ⌟

Proof: This follows from(20.8.2.3). □

Lemma (20.1.4.3). Let σ be the character on K that $\sigma(k_\theta)=e^{-ik\theta}$, $C_c^\infty(K\backslash G/K,\sigma)$ is commutative by(20.1.1.22), let ξ be a character of it. Let $H(\xi)$ be the subspace of $f\in L^2(\Gamma\backslash G,\chi,k)$ that $\pi(\varphi)f=\xi(\varphi)f$ for $\varphi\in C_c^\infty(K\backslash G/K,\sigma)$.

Then $H(\xi)$ are of f.d. and different $H(\xi),H(\eta)$ are orthogonal that $\oplus_\xi H(\xi)=L^2(\Gamma\backslash G,\chi,k)$. ⌟

Proof: Suppose $0\in f\in H(\xi)$, then by(18.9.4.1), we can find a $\varphi\in C_c^\infty(K\backslash G/K,\sigma)$ s.t. $\rho(\varphi)f\neq 0$. And by hypothesis $\rho(\varphi)f=\xi(\varphi)f$, thus $\xi(\varphi)\neq 0$, and f is an eigenvalue of $\rho(\varphi)$ which is compact and self-adjoint, so the $\xi(\varphi)$-eigenspace of $\rho(\varphi)$ is f.d. and $H(\varphi)$ is contained in this space, thus f.d.

To show the orthogonality, choose $\varphi\in C_c^\infty(K\backslash G/K,\sigma)$ that $\xi(\varphi)\neq\eta(\varphi)$. Considering $\varphi=\varphi_1+i\varphi_2$, where $\rho(\varphi_1),\rho(\varphi_2)$ are both self-adjoint, then we mays assume φ is self-adjoint. Then $H(\xi),H(\eta)$ are contained in different eigenspaces of $\rho(\varphi)$, so they are orthogonal.

Finally for the direct sum, it suffices to show that if f is orthogonal to all $H(\xi)$, then $f=0$. Given f, let $\varphi_0\in C_c^\infty(K\backslash G/K,\sigma)$ be chosen that $\rho(\varphi_0)f$ is near f that $\rho(\varphi_0)f,f$ are not orthogonal(18.9.4.1).

Consider the eigenspace decomposition of $\rho(\varphi_0)$ on $L^2(\Gamma\backslash G,\chi,k)$, then $f=f_0+f_1+f_2+\ldots$, then $\rho(\varphi_0)f=\lambda_1 f+\lambda_2 f+\ldots$. Because f is not orthogonal to $\rho(\varphi_0)f$, thus f_i is not orthogonal to f for some $i\geq 1$. Let V be the λ_i-eigenvalue of $\rho(\varphi_0)$, then V is f.d. and invariant under $\rho(\varphi)$ for all $\varphi\in C_c^\infty(K\backslash G/K,\sigma)$ because $C_c^\infty(K\backslash G/K,\sigma)$ is commutative(20.1.1.22). So V is a direct sum of elements of the spaces $H(\xi)$, so V is orthogonal to f, contradiction. □

Prop. (20.1.4.4). The space $L^2(\Gamma\backslash\mathscr{H},\chi,k)$ decomposes into a Hilbert space direct sum of eigenspaces for Δ_k. ⌟

Proof: By(20.1.1.19), it suffices to prove for $L^2(\Gamma\backslash G,\chi,k)$ and Δ. Because Δ are in the center of $U(\mathfrak{g})$, $H(\xi)$ are all Δ-invariant. So we finish by the lemma(20.1.4.3), as each $H(\xi)$ is f.d. so Δ is a self-adjoint operator on $H(\xi)$, because $C_c^\infty(\Gamma\backslash G,\chi)$ is dense(20.1.1.16). So it is a direct sum of Δ-eigenspaces. □

Prop. (20.1.4.5).

- The eigenvalues λ_i of Δ_k on $L^2(\Gamma\backslash\mathscr{H},\chi,k)$ tends to ∞, and satisfies $\sum\lambda_i^{-2}<\infty$.
- The laplacian Δ_k has an extension to a self-adjoint operator on the Hilbert space $L^2(\Gamma\backslash\mathscr{H},\chi,k)$. ⌟

Proof: Cf.[Bump P185].**?** □

<u>**The Spectral Problems for General Case**</u>

Prop. (20.1.4.6) [Gelfand, Graev and Piatetski-Shapiro]. Let $\varphi\in C_c^\infty(G)$, then

- There exists a constant $C(\varphi)$ that for all $f\in L_0^2(\Gamma\backslash G,\chi,\omega)$, we have $||\rho(\varphi)f||_{C(G)}\leq C(\varphi)||f||_2$.
- $\rho(\varphi)$ is a compact operator on $L_0^2(\Gamma\backslash G,\chi,\omega)$.

Notice this generalizes(20.8.2.1). ⌟

Proof: We may assume Γ has cusps, otherwise this is proved in(20.8.2.1). Conjugating Γ by an element of $SL(2,\mathbb{R})$, we may assume that ∞ is a cusp for Γ, and Γ_∞ is generated by $\begin{bmatrix}1&1\\&1\end{bmatrix}$. Then it suffices to prove that

$$\sup_{g\in\mathcal{G}_{c,d}}|\rho(\varphi)f(g)|\leq C_0||f||_2,$$

because we can do the same for other cusps of Γ, and use(20.1.1.26) to show that $\sup_{g\in F}|\rho(\varphi)f(g)|\leq C_0||f||_2$, hence for all $g\in\mathcal{H}$.

Now let $\varphi_\omega(g)=\int_{R^*}\varphi(zg)\omega(z)dz$, then

$$\begin{aligned}\rho(\varphi)f(g)&=\int_{Z(R)\backslash G}f(gh)\varphi_\omega(h)dh\\&=\int_{Z(\mathbb{R})\backslash G}f(h)\varphi_\omega(g^{-1}h)dh\\&=\int_{\Gamma_\infty Z(\mathbb{R})\backslash G}\sum_{\gamma\in\Gamma_\infty}f(\gamma h)\varphi_\omega(g^{-1}\gamma h)dh\\&=\int_{\Gamma_\infty Z(\mathbb{R})\backslash G}K(g,h)f(h)dh,\end{aligned}$$

where $K(g,h)=\sum_{\gamma\in\Gamma_\infty}\chi(\gamma)\varphi_\omega(g^{-1}\gamma h)$. Then we can estimate the kernel $K(g,h)$ and show it decays rapidly for h when g is fixed, and this will give the disired result, Cf.[Bump, P286]?.

2: Let $X(\Gamma)$ be the space obtained by compactifying $\Gamma\backslash G_1$ by adjoining cusps, and let Σ be the image of the unit ball in $L^2_0(\Gamma\backslash G,\chi,\omega)$ under $\rho(\varphi)$, then we can extend each $|\rho(\varphi)f|$ to $X(\Gamma)$ that it vanish at the cusps, by the corollary to item1 below(20.1.4.7), then Σ is bounded in the L^∞-norm by item1, and it is also equicontinuous, because its derivatives can be bounded uniformly for f:

$$(X\rho(\varphi)f)(g)=\rho(\varphi_X)f(g),\quad\varphi_X(g)=\frac{d}{dt}\varphi(\exp(-tX)g)$$

so the conclusion of item1 applied to φ_Xs shows the uniformly boundedness. Now Arzela-Ascoli shows that Σ is precompact in $C(X(\Gamma))$, thus also in $L^2(X(\Gamma))$. □

Cor. (20.1.4.7). If $\varphi\in C_c^\infty(G),f\in L^2_0(\Gamma\backslash G,\chi,\omega)$, then $\rho(\varphi)f$ is smooth and rapidly decreasing at cusps. ⌟

Proof: This is contained in the proof of(20.1.4.6) above, Cf.[Bump, P286]?. □

Prop. (20.1.4.8)[$L^2_0(\Gamma\backslash G,\chi,\omega)$ Totally Decomposable]. The space $L^2_0(\Gamma\backslash G,\chi,\omega)$ decomposes into a Hilbert space direct sum of irreducible subrepresentations of G, and if H is such a subrepresentation, then the $H^{K-\text{fin}}\subset H$ is dense, and $H^{K-\text{fin}}\in\mathrm{Irr}^{\text{adm}}((\mathfrak{g},K))$ is contained in $\mathcal{A}_0(\Gamma\backslash G,\chi,\omega)$.

Moreover, $\mathcal{A}_0(\Gamma\backslash G,\chi,\omega)$ is just the smooth part of $L^2_0(\Gamma\backslash G,\chi,\omega)$. ⌟

Proof: The proof is exactly the same as that of(20.1.4.2), but where we use(20.1.4.6) in place of(20.8.2.1). Lemma(18.9.4.1) is indispensable.

$H^{K-\text{fin}}\in\mathrm{Irr}^{\text{adm}}((\mathfrak{g},K))$ by(18.9.4.4). To show it is contained in $\mathcal{A}_0(\Gamma\backslash G,\chi,\omega)$, it suffices show that $H^k\subset\mathcal{A}_0(\Gamma\backslash G,\chi,\omega)$ for any k. For this, if $0\neq f\in H_k$, choose by(18.9.4.1) a function $\varphi\in C_c^\infty(G)$ that $\rho(\varphi)f\neq 0$, thus we can assume $\rho(\varphi)(f)=f$ by(18.9.4.1) and(20.8.2.1), as $\dim H^k<\infty$ by(18.9.4.3). Then by(20.1.4.7) f is smooth and decay rapidly, and it is clearly K-finite and $\mathcal{Z}$-finite, thus $f\in\mathcal{A}_0(\Gamma\backslash G,\chi,\omega)$.

The last assertion follows as any cuspidal form decays rapidly thus is contained in $L^2_0(\Gamma\backslash G,\chi,\omega)$(20.1.3.7). □

Cor. (20.1.4.9) [Finite Multiplicity].

- $L^2_0(\Gamma\backslash G,\chi,\omega)=\bigoplus_\pi\pi^{m(\pi)}$, where for each π, $m(\pi)$ is finite.

- Let $\mathcal{A}(\Gamma\backslash G,\chi,\omega,\lambda)$ be the λ-eigenspace of Δ on $\mathcal{A}(\Gamma,\chi,\omega)$, and $\mathcal{A}(\Gamma\backslash G,\chi,\omega,\lambda,k)$ be the k-part in K-decomposition of $\mathcal{A}(\Gamma\backslash G,\chi,\omega,\lambda)$, and $\mathcal{A}_0(\Gamma\backslash G,\chi,\omega,\lambda,k)$ the cuspidal part, then $\mathcal{A}_0(\Gamma\backslash G,\chi,\omega,\lambda,k)$ is of f.d.

⌟

Proof: 1: Let (π,V) be an irreducible unitary representation of G, let k be chosen that $V^k\neq 0$, let $0\neq\xi\in V^k$, then by(18.9.4.1) there is a $\varphi\in C_c^\infty(G)$ that $\pi(\varphi)\xi=\xi$ and $\pi(\varphi)$ is self-adjoint by(18.9.4.1) and(20.8.2.1), as $\dim H^k<\infty$ by(18.9.4.3). Now consider for any continuous linear map $T:V\to L_0^2(\Gamma\backslash G,\chi,\omega)$, $T\xi$ lies in the 1-eigenspace of the compact self-adjoint operator $\rho(\varphi)$, which is of f.d. as $\rho(\varphi)$ is compact by(20.1.4.6). Of course, T is determined by $T\xi$ because V is irreducible, so these T form a f.d. vector space, so the multiplicity is finite.

2: This follows from the first, because by(20.1.4.8) the K-finite parts of an irreducible subrepresentation of $L_0^2(\Gamma\backslash G,\chi,\omega)$ are just the space of cuspidal forms contained in it, and λ,k determined the action of Δ,I, so there are at most onw representation of G that satisfies these, by classification in(18.9.3.34) and(18.9.3.10), and they appear for finite multiplicity by item1, and for each of them, the k-part is of f.d., because they are admissible(18.9.4.4). So the conclusion follows. □

Remark (20.1.4.10) [Fundamental Theorem of Harish-Chandra]. In fact, Harish-Chandra showed that for any finite codimensional ideal $J\subset\mathcal{Z}$, The subspace $\mathcal{A}(\Gamma,\chi,\omega,J)$ of automorphic forms annihilated by J is an admissible $(\mathfrak{g},K)$-module.

In particular, any irreducible admissible $(\mathfrak{g},K)$-module π appears in $\mathcal{A}(\Gamma,\chi,\omega)$ with finite multiplicity.**?**

⌟

Thm. (20.1.4.11) [Main Theorem]. Let $\chi(-1)=(-1)^\varepsilon$, $\varepsilon=0,1$, (20.1.4.2) shows the representation $\mathcal{H}=L_0^2(\Gamma\backslash G,\chi)$ decomposes into Hilbert space direct sums of irreducible representations, and Δ acts as real scalars λ on each irreducible subspace(18.9.3.33), and μ acts by 0. So comparing the classification of representations of $GL(2,\mathbb{R})$(18.9.4.25), we can list what representation can appear in it by looking at eigenvalues λ of Δ:

- There is only one f.d. irreducible unitary subrepresentation of G occurring in $\mathcal{H}$, the trivial representation.
- If $\lambda\neq\frac{k}{2}(1-\frac{k}{2})$ for any $k\geq 1\in\mathbb{Z}$ and $k\equiv\varepsilon\mod 2$, then $\lambda\geq\frac{\varepsilon}{2}(1-\frac{\varepsilon}{2})$, and this subrepresentation is isomorphic to $P(\lambda,\varepsilon)$. And let $k'\equiv\varepsilon\mod 2$ be any integer, then the multiplicity of $P(\lambda,\varepsilon)$ is equal to the multiplicity of the eigenvalue λ of $\Delta_{k'}$ on $L^2(\Gamma\backslash\mathcal{H},\chi,k')$ because $L^2(\Gamma\backslash\mathcal{H},\chi,k')\cong L^2(\Gamma\backslash G,\chi,k')$ by(20.1.1.19).
- If $\lambda=\frac{k}{2}(1-\frac{k}{2})$ for some $k\geq 1\in\mathbb{Z}$ and $k\equiv\varepsilon\mod 2$, then this subrepresentation is isomorphic to either $D^+(k)$ or $D^-(k)$, and $D^\pm(k)$ have the same multiplicity in $\mathcal{H}$, equal to the dimension $\dim(M_k(\Gamma,\chi))$(20.2.1.16) of holomorphic modular forms of weight k for Γ.
  Also if $k'\equiv\varepsilon\mod 2$ is any integer$\geq k$(resp. $\leq -k$), then the multiplicity of $D^+(k)$(resp. $D^-(k)$) is equal to the multiplicity of the eigenvalue λ of $\Delta_{k'}$ on $L^2(\Gamma\backslash\mathcal{H},\chi,k')$ because $L^2(\Gamma\backslash\mathcal{H},\chi,k')\cong L^2(\Gamma\backslash G,\chi,k')$ by(20.1.1.19).

⌟

Proof: These follow from classification of irreducible representations of $GL(2,\mathbb{R})$(18.9.4.26).

Relation with modular forms: by(18.9.3.28), the multiplicity of $D^+(k)$ equals the dimension of the $\frac{k}{2}(1-\frac{k}{2})$-eigenspace of Δ_k on $L^2(\Gamma\backslash\mathcal{H},\chi,k)$, and any f in this eigenspace is annihilated by L_k by(20.1.2.1)(20.1.2.3). But(20.1.2.9) shows the dimension of space of functions annihilated by L_k equals the dimension of modular forms of weight k. Finally notice that complex conjugation interchanges $L^2(\Gamma\backslash\mathscr{H},\chi,k)$ and $L^2(\Gamma\backslash\mathscr{H},\chi,-k)$ and $\overline{\Delta_k}=\Delta_{-k}$(20.1.2.1), so the multiplicity of $D^+(k)$ and $D^-(k)$ equal. □

Eisenstein Series

Prop. (20.1.4.12). Let $\mathcal{A}^2(\Gamma\backslash G,\chi,\omega)=\mathcal{A}(\Gamma\backslash G,\chi,\omega)\cap L^2(\Gamma\backslash G,\chi,\omega)$, then this is exactly the space of smooth K-finite $\mathcal{Z}$-finite vectors in the discrete spectrum $L^2_{disc}(\Gamma\backslash G,\chi,\omega)$. ⌟

Proof:

□

20.2 Modular Forms

Main References are [?], [BGHZ] and [Mil17c], [Kat73].

Notation (20.2.0.1).
- Use notations as in Automorphic Representations over Archimedean Local Fields.

⌟

1 Modular Forms

Modular Groups

Def. (20.2.1.1) [Fuchsian Groups of the First Kind]. A **Fuchsian groups of the first kind** is a discrete subgroup $\Gamma \subset \mathrm{SL}(2,\mathbb{R})$ s.t. $\mathrm{Vol}(\mathrm{SL}(2,\mathbb{R})/\Gamma) < \infty$. ⌟

Def. (20.2.1.2) [Principle Congruence Subgroups]. For $N \in \mathbb{Z}_+$, there are Fuchsian subgroups:

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$$

where

$$\Gamma(N) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}(2,\mathbb{Z}) | a, d \equiv 1 (\mathrm{mod}\ N), b, c \equiv 0 (\mathrm{mod}\ N)\}.$$

$$\Gamma_1(N) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}(2,\mathbb{Z}) | a, d \equiv 1 (\mathrm{mod}\ N), c \equiv 0 (\mathrm{mod}\ N)\}.$$

$$\Gamma_0(N) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}(2,\mathbb{Z}) | c \equiv 0 (\mathrm{mod}\ N)\}.$$

⌟

Def. (20.2.1.3) [Congruence Subgroups]. A **congruence subgroup** is a Fuchsian subgroup $\Gamma \subset \mathrm{SL}(2,\mathbb{Z})$ that contains $\Gamma(N)$ for some N. In particular, a congruence subgroup has finite index in $\Gamma(1)$. ⌟

Def. (20.2.1.4) [Fricke Involution]. For $N \in \mathbb{Z}_+$, denote

$$w_N = \begin{bmatrix} & -1 \\ N & \end{bmatrix}, \quad W_N = \frac{1}{\sqrt{N}} w_N.$$

Then $W_N^2 = -1$, and $\Gamma_0(N)$ is stabilized by w_N and W_N. Denote

$$\Gamma_0^+(N) = \langle \Gamma_0, W_N \rangle \subset \mathrm{SL}(2,\mathbb{R}).$$

⌟

Proof:

$$w_N \begin{bmatrix} a & b \\ c & d \end{bmatrix} w_N^{-1} = \frac{-1}{N} \begin{bmatrix} Nd & c \\ N^2 b & Na \end{bmatrix} = \begin{bmatrix} -d & -c/N \\ -Nb & -a \end{bmatrix}.$$

□

Prop. (20.2.1.5). $\Gamma_0^+(4) = \langle T = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}, W_4\rangle$. In fact, if $\widetilde{T} = W_4 T W_4^{-1} = \begin{bmatrix} 1 & \\ 4 & 1 \end{bmatrix}$, then $\overline{\Gamma_0(4)} = \overline{\langle T, \widetilde{T}\rangle} \in \mathrm{PSL}(2;\mathbb{R})$. ⌟

Proof: □

Lemma (20.2.1.6) [Cartan Decomposition]. There is a complete set of coset representatives for $\mathrm{SL}(2,\mathbb{Z})\backslash \mathrm{GL}(2,\mathbb{Q})^+ / \mathrm{SL}(2,\mathbb{Z})$ consisting of the diagonal matrices $\mathrm{diag}(d_1, d_2)$, where $d_1, d_2 \in \mathbb{Q}^\times$ and d_1/d_2 is a positive integer.

More generally, for $N > 0$,

$$\mathrm{GL}(2,\mathbb{Q})^+ = \coprod_{d_1,d_2\in\mathbb{Q}^\times, d_1/d_2\in\mathbb{Z}_+} \mathrm{SL}(2,\mathbb{Z}) \begin{bmatrix} d_1 & \\ & d_2 \end{bmatrix} \Gamma_0(N).$$

Also, let Σ be the set of primes dividing N, $\mathbb{Z}_\Sigma$ be the localization of $\mathbb{Z}$ at these primes, and $G_0(N)$ be the subgroup of $\mathrm{GL}(2,\mathbb{Z}_\Sigma)^+$ consisting of matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ s.t. $c \in N\mathbb{Z}_\Sigma$. Then

$$G_0(N) = \coprod_{d_1,d_2\in\mathbb{Z}_\Sigma, d_1/d_2\in\mathbb{Z}_+} \Gamma_0(N) \begin{bmatrix} d_1 & \\ & d_2 \end{bmatrix} \Gamma_0(N).$$

⌟

Proof: The first assertion follows from(12.11.5.7), noticing the sign.

For the second assertion, for any $g \in G_0(N)$, let $g = \gamma_1 \,\mathrm{diag}(d_1, d_2)\gamma_2$ where $D = d_1/d_2 \in \mathbb{Z}$ and $(D, N) = 1$. Then for any $\begin{bmatrix} a & b \\ Dc & d \end{bmatrix} \in \Gamma_0(N)$, we can change (γ_1, γ_2) to $(\gamma_1 \begin{bmatrix} a & Db \\ c & d \end{bmatrix}, \begin{bmatrix} a & b \\ Dc & d \end{bmatrix}\gamma_2)$, in this way if $\gamma_2 = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$, we can change z to $Dxc + dz$. Now take k s.t. $(kx + z, N) = 1$, and let c be chosen s.t. $N|D(kz + x)c + z$, and $d = kDc + 1$, then $(Dc, d) = 1$, and we can find a, b s.t. $ad - Dbc = 1$. Then for this (a, b, c, d), $\begin{bmatrix} a & b \\ Dc & d \end{bmatrix}\gamma_2 \in \Gamma_0(N)$.

Finally, if $g \in G_0(N)$ and $\gamma_2 \in \Gamma_0(N)$, then automatically $\gamma_1 \in \Gamma_0(N)$. □

Prop. (20.2.1.7) [Conjugate of Congruence Subgroup]. If Γ is a congruence subgroup of level N and $\alpha \in \mathrm{GL}(2,\mathbb{Q})^+$, then $\alpha^{-1}\Gamma\alpha$ is a congruence subgroup.

In particular, $\alpha\Gamma\alpha^{-1} \cap \Gamma$ is also a congruence subgroup, and if $\alpha \in \mathrm{SL}(2,\mathbb{Z})$ with $\delta(\alpha) = D$, then $\alpha^{-1}\Gamma\alpha$ is a congruence subgroup of level DN. ⌟

Proof: Let M_1, M_2 be positive integers s.t. $M_1\alpha, M_2\alpha^{-1} \in \mathrm{Mat}(2;\mathbb{Z})$.(In the second case we can take $M_1 = 1, M_2 = D$). If A is a matrix that $A \equiv 1 \mod M_1M_2N$, then $\alpha^{-1}(A - 1)\alpha \equiv 1 \mod N$. Thus $\alpha^{-1}\Gamma\alpha$ contains $\Gamma(M_1M_2N)$. □

Cor. (20.2.1.8) [Congruence Topology]. We can define a topology on the group $\mathrm{GL}(2,\mathbb{Q})^+$ given by a basis at the origin given by the open subgroup $\Gamma(N)$. Then(20.2.1.7) can be used to show that this is truly a topology. In fact, it is restriction on $SL(2,\mathbb{Z})$ is the same as the topology given by the inclusion $\mathrm{SL}(2,\mathbb{Z}) \subset \mathrm{SL}(2,\widehat{\mathbb{Z}})$.

But unfortunately, $\mathrm{SL}(2,\mathbb{Z})$ is not compact in this topology, because otherwise $SL(2,\mathbb{Z})$ is closed in $\mathrm{SL}(2,\widehat{\mathbb{Z}})$, contradiction. ⌟

Lemma (20.2.1.9). The action of $\Gamma(1) = \mathrm{SL}(2,\mathbb{Z})$ on $\mathscr{H}$ is properly discontinuous(4.12.1.13). ⌟

Proof: Cf.[Bump P18]. □

Prop. (20.2.1.10). The subset $F = \{z \in \mathscr{H} || \operatorname{Re}(z)| < 1/2, |z| > 1\}$ is a fundamental domain for $\Gamma(1) = \mathrm{SL}(2,\mathbb{Z})$, and moreover, let $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, then $S^2 = -1, (ST)^3 = (TS)^3 = -1$, and

(1) two elements z, z' of $\overline{F}$ are equivalent under $\Gamma(1)$ iff
   (a) $\operatorname{Re}(z) = -1/2$ and $z' = z + 1$, then $z' = T(z)$.
   (b) $|z| = 1$ and $z' = -\frac{1}{z}$, then $z' = S(z)$.
(2) Let $z \in \overline{F}$, if the stabilizer of z is not ± 1, then
   (a) $z = \mathrm{i}$ and $\mathrm{Stab}(\mathrm{i}) = \langle S \rangle$.
   (b) $z = \rho = e^{2\pi \mathrm{i}/6}$ and $\mathrm{Stab}(\rho) = \langle TS \rangle$.
   (c) $z = \omega$, and $\mathrm{Stab}(\omega) = \langle ST \rangle$.

⌟

Proof: 1: Let Γ' be the subgroup of $\Gamma(1)$ generated by S and T. By(11.4.1.9),

$$\operatorname{Im}(\gamma(z)) = \frac{\operatorname{Im}(z)}{|cz+d|^2}.$$

and there is a $\gamma \in \Gamma'$ that $|cz + d|$ attains the minimal value, then $\operatorname{Im}(\gamma(z))$ attains a maximal value. Now there is a n that $z' = \operatorname{Re}(T^n\gamma(z)) \in [-1/2, 1/2]$. Now I claim that $|z'| \geq 1$, because otherwise

$$\operatorname{Im}(Sz') = \operatorname{Im}(-1/z') = \frac{\operatorname{Im}(z')}{|z'|^2} > \operatorname{Im}(z'),$$

contradiction.

2: Suppose $z, z' \in \overline{F}$ are Γ-conjugate, we can assume $\operatorname{Im}(z) \leq \operatorname{Im}(z')$. Suppose $z' = \gamma(z)$ and $z = x + iy$, then

$$(cx + d)^2 + (cy)^2 \leq 1.$$

Then $|c| < 2$. If $c = 0$, then $d = \pm 1$, and γ is a translation, thus we are in case $1.(a)$. If $c = 1$, then $d = 0$, unless $z = \rho$ or ω. If $d = 0$, then $\gamma = \begin{bmatrix} a & 1 \\ -1 & \end{bmatrix}$, thus $\gamma(z) = a - \frac{1}{z}$. If $a = 0$, then we are in case $1.(b)$, and if $a \neq 0$, then $z = \rho$ or ω. and the $c = -1$ case is similar. □

Def. (20.2.1.11) [Elliptic Points]. A point $z \in \mathscr{H}$ is called a **elliptic point** if it is the fixed point of an elliptic element γ of Γ(12.12.0.3). ⌟

Prop. (20.2.1.12). Let Γ be a discrete subgroup of $\mathrm{SL}(2,\mathbb{R})$ and z an elliptic point of Γ, then the stabilizer Γ_z of z in Γ is a finite cyclic subgroup . ⌟

Proof: Because $\mathrm{SL}(2,\mathbb{R})$ acts transitively on $\mathscr{H}$, by conjugacy we can assume the elliptic point is i for another Γ'. Then the stablizer of i in $\mathrm{SL}(2,\mathbb{R})$ is $\mathrm{SO}(2,\mathbb{R}) \cong S^1$, and $\mathrm{SO}(2,\mathbb{R}) \cap \Gamma'$ is a compact and discrete subgroup, so it is finite cyclic. □

Prop. (20.2.1.13) [Cusps and Elliptic Points for $\Gamma(1)$].

- The cusps of $\Gamma(1)$ are exactly $\mathbb{P}^1(\mathbb{Q})$, and each of them is $\Gamma(1)$-equivalent to ∞.

- The elliptic points of $\Gamma(1)$ are exactly those that are $\Gamma(1)$-conjugate to i or $\rho = e^{\pi\,\mathrm{i}/3}$, with corresponding stablizer group cyclic of order 4 and 6.

⌟

Proof: 1: Clearly ∞ is fixed by the parabolic matrix $T = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$. Now for any m/n that m,n is coprime, there exists integers r,s that $rm - sn = 1$. Let $\gamma = \begin{bmatrix} m & s \\ n & r \end{bmatrix}$, then $\gamma(\infty) = m/n$ thus m/n is also a cusp. Conversely, every parabolic matrix is conjugate to T, thus its fixed point is conjugate to ∞, which means the fixed point is in $\mathbb{Q} \cup \{\infty\}$.

2: For the elliptic points of $\Gamma(1)$, use(20.2.1.10). □

Siegel Modular Forms

Def. (20.2.1.14) [Siegel Modular Forms]. Let $\Gamma \subset \mathrm{Mp}(2,\mathbb{R})$ be a subgroup commensurable with $\mathrm{Mp}(2,\mathbb{Z})$, and let $(\rho, V_\rho) \in \mathrm{Rep}^{\mathrm{fd}}(\Gamma)$ that factors through a finite quotient of Γ, and let $k \in \frac{1}{2}\mathbb{Z}$, then a **Siegel modular form** of weight k and type ρ for Γ is a holomorphic function $f \in \mathcal{O}(\mathcal{H}; V_\rho)$ s.t. for $\gamma = (\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \pm\sqrt{c\tau + d}) \in \Gamma$,

$$f(\frac{a\tau + b}{c\tau + d}) = (\pm\sqrt{c\tau + d})^{2k} \rho_M(\gamma) f(\tau).$$

⌟

Def. (20.2.1.15) [Holomorphic Siegel Modular Forms]. ?

The space of holomorphic Siegel modular forms is denoted by $M(\Gamma, k, \rho)$. ⌟

Def. (20.2.1.16) [Siegel Modular Forms(of half Integral Weights)]. commensurable with $\mathrm{Mp}(2,\mathbb{Z})$, and let $(\rho, V_\rho) \in \mathrm{Rep}^{\mathrm{fd}}(\Gamma)$ that factors through a finite quotient of Γ, and let $k \in \frac{1}{2}\mathbb{Z}$, then the space $M_k^!(\Gamma, \rho)$ of (meromorphic)**Siegel modular form** of weight k and type ρ for Γ consists of functions $f \in C^\infty(\mathcal{H}; V_\rho)$ s.t.

- f is meromorphic.
- (weak modularity)For $\gamma = (\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \pm\sqrt{c\tau + d}) \in \Gamma$,

$$f(\frac{a\tau + b}{c\tau + d}) = (\pm\sqrt{c\tau + d})^{2k} \rho_M(\gamma) f(\tau).$$

- f is meromorphic at the cusps(20.1.1.12), i.e. for any $g = f[\gamma]_k$, the coefficients of the expansion

$$g(\tau) = \sum_{n \in \mathbb{Q}} \sum_{\gamma} c_{n,\gamma} q^n e_\gamma$$

vanishes for n small. Equivalently, $f[\gamma]_k$ are all meromorphic at ∞ for $\gamma \in \mathrm{Mp}(\mathbb{Q})$.

And a meromorphic modular form f is called a **holomorphic modular form** iff it is holomorphic and holomorphic at cusps(20.1.1.12). The subspace of holomorphic modular forms in $M^!(\Gamma, \rho)$ is denoted by $M(\Gamma, \rho)$.

A meromorphic modular form of weight 0 is called a **modular function**.

Denote $\mathrm{MF}^!_k(\Gamma,\mathbb{1})=\mathrm{MF}^!_k(\Gamma)$, $\mathrm{MF}_k(\Gamma,\mathbb{1})=\mathrm{MF}_k(\Gamma)$, and moreover we denote by $\mathrm{SF}_k(\Gamma,\chi)$ the set of **holomorphic cusp forms** consisting of all $f\in\mathrm{MF}_k(\Gamma,\rho)$ that vanishes at the cusps(20.1.1.12), and denote $\mathrm{SF}_k(\Gamma,\mathbb{1})=S_k(\Gamma)$.

Denote by $\mathrm{MF}^!(\Gamma)=\oplus_{k\geq 0}\mathrm{MF}^!_k(\Gamma)$ the graded ring of meromorphic modular forms, $\mathrm{MF}(\Gamma)=\oplus_{k\geq 0}\mathrm{MF}_k(\Gamma)$ the graded algebra of holomorphic modular forms for Γ, $\bigoplus_{k\geq 0}\mathrm{SF}_k(\Gamma)$ is a graded ideal of $\mathrm{MF}(\Gamma)$. ⌟

Prop. (20.2.1.17) [Fourier Expansions of Modular Forms]. Let $N\in\mathbb{Z}_+,k\in\mathbb{N}$ and $\Gamma\subset\Gamma(1)$ be a modular form of level N. Then $f\in\Omega(\mathcal{H},\mathbb{C})$ is in $\mathrm{MF}_k(\Gamma)$ iff it is weakly modular, and there exists some $r\in\mathbb{Z}_+$ s.t. f has a Fourier expansion

$$f(\tau)=\sum_{n\in\mathbb{N}}a_n e^{2\pi\mathrm{i}\,n/N},$$

where $a_n=O(n^r)$. ⌟

Proof: Cf.[Diamond, modular forms]P17. □

Thm. (20.2.1.18) [Valence Formula]. Let f be a meromorphic forms for Γ of weight $2k$, then

$$\frac{1}{2}\sum_{Q\text{ elliptic points with period }2}\mathrm{ord}_Q(f)+\frac{1}{3}\sum_{Q\text{ elliptic points with period }3}\mathrm{ord}_Q(f)+\sum_{Q\text{ others}}\mathrm{ord}_Q(f)=kd/6,$$

where the sum is over a set of representatives for points in $\Gamma\backslash\mathcal{H}^*$. ⌟

Proof: Cf.[Milne, P53].**?** □

Def. (20.2.1.19) [Hauptmodul]. Let Γ be a discrete subgroup of $SL(2,\mathbb{R})$ with exactly one cups, $k>0$, a **Hauptmodul** for Γ is an element in $M^!(\Gamma)$ s.t. it is holomorphic on $\mathcal{H}$ and has a simple pole at the cusp with residue 1, i.e. its Fourier series at the cusp is of the form

$$f(\tau)=q^{-1}+a_0+a_1q+\ldots.$$

⌟

Prop. (20.2.1.20) [Petersson Inner Product]. For a congruence subgroup $\Gamma\subset\Gamma(1)$(20.2.1.3) and $k,\in\mathbb{Z}_+$, $f\in M_k(\Gamma,\chi)$ and $g\in S_k(\Gamma,\chi)$, $f\overline{g}y^k$ is invariant under the action of Γ, thus we can define

$$(f,g)_{\mathrm{Pet}}=(f,g)_{\Gamma,k}\overset{\triangle}{=}\frac{1}{[\mathrm{SL}(2,\mathbb{Z}):\{\pm\}\Gamma]}\int_{\Gamma\backslash\mathcal{H}}f\overline{g}y^k\frac{\mathrm{d}x\mathrm{d}y}{y^2},$$

which is finite, and restricts to an inner product on $S_k(\Gamma,\chi)$. Moreover, this inner form is invariant of the Γ chosen. ⌟

Proof: To show it is finite, notice that $\Gamma\backslash\mathcal{H}$ is a finite translations of the fundamental domain of $\Gamma(1)$, and for $\alpha\in SL(2,\mathbb{Z})$,

$$\int_{\alpha(D)}f\overline{g}y^k\frac{\mathrm{d}x\mathrm{d}y}{y^2}=\int_D f\circ\alpha.\overline{g\circ\alpha}y(\alpha(z))^k\frac{\mathrm{d}x\mathrm{d}y}{y^2}=\int_D f[\alpha]_k.\overline{g[\alpha]_k}y^k\frac{\mathrm{d}x\mathrm{d}y}{y^2},$$

and $f[\alpha]_k,g[\alpha]_k$ are modular forms for $\Gamma'=\alpha^{-1}\Gamma\alpha,\chi'(\gamma')=\chi(\alpha\gamma\alpha^{-1})$, thus it suffices to prove the integral is finite on the fundamental domain F for $\Gamma(1)$(20.2.1.10). For this, notice g is of exponential decay for y, thus the integral is bounded by $\int_{y_1}^\infty e^{-cy}y^{k-2}\mathrm{d}y<\infty$. □

Prop. (20.2.1.21). If $\alpha \in \mathrm{GL}(2,\mathbb{R})^+$, $f \in M_k(\Gamma)$ and $g \in S_k(\alpha^{-1}\Gamma\alpha)$, then

$$(f[\alpha]_k, g)_{\alpha^{-1}\Gamma\alpha} = (f, g[\alpha^{-1}]_k)_\Gamma.$$

⌟

Proof: This is because for there is an isomorphism $\alpha : \alpha^{-1}\Gamma\alpha\backslash\mathscr{H} \cong \Gamma\backslash H$, and for any left Γ-invariant function φ,

$$\int_{\alpha^{-1}\Gamma\alpha\backslash H} \varphi(\alpha(\tau))d\mu(\tau) = \int_{\Gamma\backslash H} \varphi(\tau)d\mu(\tau)$$

and $(f\overline{g[\alpha^{-1}]}y^k)(\alpha\tau) = (f[\alpha]_k\overline{g}y^k)(\tau)$. □

Prop. (20.2.1.22) [Lower Bound on Petersson Inner Products]. For any $N \in \mathbb{Z}_+$ and $f = \sum_{n\in\mathbb{Z}_+} a_n q^n \in \mathrm{SF}(\Gamma(N))$,

$$[\Gamma(1) : \Gamma(N)]\cdot||f||_{\mathrm{Pet}} \geq \sum_{n\in\mathbb{Z}_+} \frac{|a_n|^2}{4\pi n e^{4\pi n}}.$$

⌟

Proof: Integrate on the region $\{\tau = x + \mathrm{i}\, y : |x| \leq 1/2, y \geq 1\}$. □

Prop. (20.2.1.23) [Twisted Modular Forms]. For each Dirichlet character $\chi \in \mathrm{Diri}(N)$, we can define a character of $\Gamma_0(N)$:

$$\chi_d(\begin{bmatrix} a & b \\ c & d \end{bmatrix}) = \chi(d).$$

Then we can define $\mathrm{MF}_k(N,\chi) = \mathrm{MF}_k(\Gamma_0(N),\chi)$(20.2.1.16) and $\mathrm{SF}_k(N,\chi) = \mathrm{SF}_k(\Gamma_1(N)) \cap \mathrm{MF}_k(N,\chi)$. Then there are direct sum decompositions:

$$\mathrm{MF}_k(\Gamma_1(N)) = \bigoplus_{\chi\in\mathrm{Diri}(N),\chi(-1)=(-1)^k} \mathrm{MF}_k(N,\chi), \quad \mathrm{SF}_k(\Gamma_1(N)) = \bigoplus_{\chi\in\mathrm{Diri}(N),\chi(-1)=(-1)^k} \mathrm{SF}_k(N,\chi).$$

Moreover, the summands are orthogonal w.r.t. the Petersson inner product(20.2.1.20). ⌟

Proof: Cf.[Diamond, P418]. □

Cor. (20.2.1.24) [Reduction to $\Gamma_0(N)$]. For any congruence subgroup $\Gamma(N)$, there exists $\alpha \in \mathrm{GL}(2,\mathbb{Q})^+$ s.t. $\begin{bmatrix} 1 & \\ & N \end{bmatrix} \Gamma_1(N) \begin{bmatrix} 1 & \\ & 1/N \end{bmatrix} \subset \Gamma(N)$. Thus if $f \in \mathrm{MF}_k(\Gamma(N))$, $f[\mathrm{diag}(1,N)]_k \subset \mathrm{MF}_k(\Gamma_1(N))$, which is a combination of modular forms in $\mathrm{MF}_k(\Gamma_0(N),\chi)$. Thus the study of congruence modular forms reduces to the study of $\mathrm{MF}_k(N,\chi)$. ⌟

Moduli Characterization

Prop. (20.2.1.25) [Elliptic Curves and Modular Curves]. Modular curves $Y_0(N), Y_1(N), Y(N)$ parametrizes elliptic curves over $\mathbb{C}$ with additional structures. ⌟

Proof: □

Cusp Forms

Def. (20.2.1.26) [Poincaré Series]. For any Fuchsian subgroup $\Gamma \subset \Gamma(1)$, $T = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$. Let h be the minimal positive integer that $T^h \subset \Gamma$, and define Γ_0 the subgroup of Γ generated by T^h. Then we define the **Poincaré series of weight** $2k$ **and character** n **for** Γ to be the series

$$\varphi_{k,n}(z) = \sum_{\Gamma_\infty \backslash \Gamma'} \frac{e^{\frac{2\pi \mathrm{i}\, n\gamma(z)}{h}}}{(cz+d)^{2k}},$$

where Γ' is the image of Γ in $\Gamma(1)/\{\pm 1\}$. ⌟

Prop. (20.2.1.27). For $k \in \mathbb{Z}_+, n \in \mathbb{N}$, The Poincaré series(20.2.1.26) $\varphi_{2k,n}$ converge absolutely on compact subsets of $\mathscr{H}$, and $\varphi_{2k,n} \in \mathrm{MF}_{2k}(\Gamma)$. Moreover,

- $\varphi_{2k,0}(\tau)$ vanishes at all finite cusps, and $\varphi_{2k,0}(\mathrm{i}\,\infty) = 1$.
- For $n \geq 1$, $\varphi_{2k,n}(\tau) \in \mathrm{SF}_k(\Gamma)$.

⌟

Proof: Cf.[Gunning, Lectures on Modular Forms]3.9.**?** □

Prop. (20.2.1.28) [Cusp Forms are Spanned by Poincaré Series]. For any Fuchsian subgroup $\Gamma \subset \Gamma(1)$ and $k \in \mathbb{Z}_+, n \in \mathbb{N}$, if $f = \sum_{n \in \mathbb{Z}_+} a_n e^{2\pi \mathrm{i}\, nz/h} \in \mathrm{SF}_k(\Gamma)$, then

$$\langle f, \varphi_{2k,n} \rangle_{\mathrm{Pet}} = \frac{h^{2k}(2k-2)!}{(4\pi)^{2k-1}} n^{1-2k} a_n.$$

Thus the Poincaré series $\{\varphi_{2k,n}(z)\}_{n \in \mathbb{Z}_+}$ span $S_{2k}(\Gamma)$. ⌟

Proof: Cf.[Gunning, Lectures on Modular Forms]3.11.Thm5.**?** □

Modular Forms of Half Integral Weights

References are [Modular Forms of Half Integral Weight, Shimura].

Prop. (20.2.1.29) [Theta Functions]. It follows from(20.4.1.6) that

$$\theta(\frac{\tau}{4\tau+1}) = \theta(-\frac{1}{4(-1/(4\tau)-1)}) = \sqrt{2\,\mathrm{i}(\frac{1}{4\tau}+1)} = \theta(-\frac{1}{4\tau}-1) = \sqrt{4\tau+1}\theta(\tau).$$

Thus by(20.2.1.5), $\theta^2 \in \mathrm{MF}_1(\Gamma_0(4), \chi_{-4})$. ⌟

Prop. (20.2.1.30) [Dedekind η-Function]. The Dedekind η-function(9.5.2.6)

$$\eta(\tau) = e^{2\pi \mathrm{i}\,\tau/24} \prod_{n \in \mathbb{Z}_+} (1 - e^{2\pi \mathrm{i}\, n\tau})$$

belongs to $\mathrm{MF}_{1/2}(\Gamma(1), \chi)$. ⌟

Proof: To show this, it suffices to show

$$\eta(\gamma(z)) = \varepsilon(\gamma)(cz+d)^{1/2}\eta(z)$$

for every $\gamma \in \Gamma(1)$, where $\varepsilon(\gamma)$ is a 24-th root of unity. Because $[\gamma]_k$ is an action(20.2.1.16), by5, it suffices to show for $S = \begin{bmatrix} & -1 \\ 1 & \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$. The case for T is clear from the last expression of $\eta(z)$. For S, it suffices to show that

$$\eta(-1/\tau) = \sqrt{\tau/\mathrm{i}}.\eta(\tau).$$

This is true when $\tau = \mathrm{i}$. So it suffices to show its logarithm derivative:

$$\frac{\eta'(-1/z)}{\eta(-1/z)}z^{-2} = \frac{1}{2z} + \frac{\eta'(z)}{\eta(z)}.$$

And notice

$$\frac{\eta'(z)}{\eta(z)} = \frac{2\pi\,\mathrm{i}}{24}(1 - 24\sum_{n\in\mathbb{Z}_+}\frac{ne^{2\pi\,\mathrm{i}\,nz}}{1-e^{2\pi\,\mathrm{i}\,nz}}) = \frac{2\pi\,\mathrm{i}}{24}(1 - 24\sum_{n\in\mathbb{Z}_+}\sigma(n)e^{2\pi\,\mathrm{i}\,nz}) = \frac{2\pi\,\mathrm{i}}{24}E_2(z).$$

So the assertion follows from(20.2.4.14). □

Thm. (20.2.1.31) [Serre-Stark]. Every modular forms of weight 1/2(for any level) is a linear combination of unary theta functions. ⌟

2 Hecke Algebras

Def. (20.2.2.1) [$G(N)$]. Define $G(N) = \cup_{\alpha\in GL(2,\mathbb{Q})^+}\Gamma_0(N)\alpha\Gamma_0(N)$. ⌟

Def. (20.2.2.2) [Hecke Algebra]. Notation as in(20.2.1.6), if $\alpha \in \Gamma_0(N)\backslash G(N)/\Gamma_0(N)$, then $\Gamma_0(N)\backslash\Gamma_0(N)\alpha\Gamma_0(N)$ is finite, and if $N=1$, there is a set of representatives $\{\alpha_1,\ldots,\alpha_h\}$ s.t.

$$\Gamma(1)\alpha\Gamma(1) = \coprod_i \Gamma(1)\alpha_i = \coprod_i \alpha_i\Gamma(1) = \Gamma(1)\alpha_i^t.$$

Let $\mathcal{R}'_N$ be the free Abelian group generated by $\Gamma_0(N)\backslash G(N)$ s.t. if $\Gamma_0(N)\alpha\Gamma_0(N) = \sum_i \Gamma_0(N)\alpha_i$, then $[\alpha][\beta] = \sum_i[\alpha_i\beta]$.

Define the **Hecke algebra** $\mathcal{R}_N$ of $\Gamma_0(N)$ to be the subalgebra of $\mathcal{R}'_N$ consisting by right $\Gamma_0(N)$-invariant elements. Then $\mathcal{R}_N$ is isomorphic to the free Abelian group generated by the double coset $\Gamma_0(N)\backslash G(N)/\Gamma_0(N)$, and is commutative. ⌟

Remark (20.2.2.3). Compare this definition with that of(18.1.5.12). ⌟

Proof:

$$\begin{aligned}\Gamma_0(N)\backslash\Gamma_0(N)\alpha\Gamma_0(N) &\cong \Gamma_0(N)\backslash\Gamma_0(N)\alpha\Gamma_0(N)\alpha^{-1} \\ &\cong \Gamma_0(N)\cap\alpha\Gamma_0(N)\alpha^{-1}\backslash\alpha\Gamma_0(N)\alpha^{-1} \\ &\cong \alpha^{-1}\Gamma_0(N)\alpha\cap\Gamma_0(N)\backslash\Gamma_0(N)\end{aligned}$$

which is finite by(20.2.1.7).

By decomposition(20.2.1.6), the transposition on $G(N)$ is an involution that identifies every double coset $\Gamma(1)\alpha\Gamma(1)$, thus $\sum_i \Gamma(1)\alpha_i = \sum_i \alpha_i^t\Gamma(1)$, and also $\Gamma(1)\alpha_i \cap \alpha_i^t\Gamma(1) \neq \varnothing$, as $\Gamma(1)\alpha_i\Gamma(1) = \Gamma(1)\alpha_i^t\Gamma(1)$, thus we can replace α_i by some element in $\Gamma(1)\alpha_i \cap \alpha_i^t\Gamma(1)$.

To show $\mathcal{R}_N$ is commutative, for any $\sigma \in \Gamma(1)\backslash GL(2,\mathbb{Q})^+/\Gamma(1)$, denote $\deg(\sigma)$ to be the cardinality of $\Gamma(1)\backslash\Gamma(1)\sigma\Gamma(1)$, $\sigma[i], i \leq \deg(\sigma)$ be a set of representatives, and let $m(\alpha,\beta,\sigma[i])$ be the cardinality of $\{(i,j)|\Gamma(1)\alpha_i\beta_j = \Gamma(1)\sigma[i]\}$, then $m(\alpha,\beta,\sigma[i])$ is independent of i as right action by $\Gamma(1)$ permutes $\{(i,j)\}$. Also we see $m(\alpha,\beta,\sigma[i])$ equals $1/\deg(\sigma)$ times the number of pairs $\{(i,j)|[\sigma] = [\alpha_i\beta_j]\}$, because $[\sigma] = [\alpha_i\beta_j]$ iff $\alpha_i\beta_j \in \Gamma(1)\sigma[i]$ for some i.

Then

$$m(\alpha,\beta,\sigma[i]) = \frac{1}{\deg(\sigma)}\#\{(i,j)|[\sigma] = [\alpha_i\beta_j]\} = \frac{1}{\deg(\sigma)}\#\{(i,j)|[\sigma^t] = [\beta_j^t\alpha_i^t]\} = m(\beta,\alpha,\sigma^t[i]).$$

But as $\sigma^t[i]$ is a permutation of $\sigma[i]$, we see $\mathcal{R}$ is commutative. □

Hecke Operators

Prop. (20.2.2.4). If Γ_1,Γ_2 are congruence subgroups of X, then for any $\alpha \in GL^+(2,\mathbb{Q})$, the double coset

$$\Gamma_1\alpha\Gamma_2 = \coprod_i \Gamma_1\beta_i$$

for some $\beta_i \in \mathrm{GL}^+(2,\mathbb{Q})$. Then we can define a map

$$\mathrm{Div}(X(\Gamma_1)) \to \mathrm{Div}(X(\Gamma_2)) : [\tau] \mapsto [\beta_i\tau],$$

which induces a morphism $\mathrm{Jac}(\Gamma_1) \to \mathrm{Jac}(\Gamma_2)$**?**. ⌟

Prop. (20.2.2.5) [Action on Modular Forms]. Let Γ_1,Γ_2 be congruence subgroups of $GL^+(2,\mathbb{R})$, then ⌟

Prop. (20.2.2.6) [Hecke Operators]. The Hecke algebra $\Gamma\backslash GL^+(2,\mathbb{R})/\Gamma$ acts on $M_k(\Gamma)$ via

$$T_\alpha(f) = \sum_i f[\alpha_i]_k \text{(20.1.1.8)}, \quad \text{if } \Gamma\alpha\Gamma = \coprod_i \Gamma\alpha_i.$$

and preserves $S_k(\Gamma)$. ⌟

Proof: This is an action because if $\Gamma_0(N)\alpha\Gamma_0(N) = \coprod_i \Gamma_0(N)\alpha_i, \Gamma_0(N)\beta\Gamma_0(N) = \coprod_j \Gamma_0(N)\beta_j$, then $[\alpha][\beta] = \coprod_{i,j}\Gamma_0(N)\alpha_i\beta_j$.

Also $T_\alpha(f)[\gamma]_k = T_\alpha(f)$ for $\gamma \in \Gamma_0(N)$ because $\Gamma_0(N)\backslash\Gamma_0(N)\alpha\Gamma_0(N)$ is right $\Gamma_0(N)$-invariant. And they are holomorphic at cusps because f is holomorphic at cusps thus all $f[\alpha_i]_k$ are holomorphic at cusps. Moreover, if f vanishes at cusps, then all $f[\alpha_i]_k$ vanishes at cusps. □

$\Gamma_0(N), \Gamma_1(N)$ Cases

Prop. (20.2.2.7) [Self-Adjointness]. The action of $\mathcal{R}_N$ on $S_k(\Gamma(N))$ is self-adjoint w.r.t to the Petersson inner product(20.2.1.20). ⌟

Proof: First notice $(\chi_d(\alpha)^{-1}f[\alpha]_k, g) = (f, \chi_d(\alpha)g[\alpha^{-1}]_k)$ for any $\alpha \in G_0(N)$ by(20.2.1.21), and $f, g \in M_k(N,\chi)$, thus $(\chi_d(\alpha)^{-1}f[\alpha]_k, g)$ only depends on the double coset $\Gamma_0(N)\alpha\Gamma_0(N)$. Thus

$$(T_\alpha f, g) = \sum_i (\chi_d(\alpha_i)^{-1}f[\alpha_i]_k, g) = \deg(\alpha)(\chi_d(\alpha)^{-1}f[\alpha]_k, g) = \deg(\alpha)(f, \chi_d(\alpha)g[\alpha^{-1}]_k)$$

However, $\det(\alpha)\alpha^{-1}$ has the same Smith normal form as α, thus it is in the same double coset as α, thus

$$\deg(\alpha)(f, \chi_d(\alpha)g[\alpha^{-1}]_k) = \deg(\alpha)(f, \chi_d(\alpha)^{-1}g[\alpha]_k) = (f, T_\alpha g).$$

□

Cor. (20.2.2.8) [Hecke Eigenforms]. The Hecke algebra is commutative and acts as self-adjoint operators on $S_k(N,\chi)$, thus there is a basis consisting of eigenfunctions for each T_α, called the **Hecke eigenforms**. ⌟

Prop. (20.2.2.9) [$T(n)$]**.** Let $T(n)$ be the sum of operators $T_{\mathrm{diag}(d_1,d_2)}$ where $d_1, d_2 \in \mathbb{N}, d_2|d_1$ and $d_1 d_2 = n$.

Equivalently by Cartan decomposition, if Δ_n is the subset of $GL(2,\mathbb{Z}) \cap G_0(N)$ consisting of matrices of determinant n, then

$$\Delta_n = \coprod_{a,d>0, ad=n, b\in\mathbb{Z}/N} \Gamma_0(N)\begin{bmatrix} a & b \\ & d \end{bmatrix}$$

and

$$T(n)f = \sum_{a,d>0, ad=n, b\in\mathbb{Z}/N} \chi(d)^{-1} f[\begin{bmatrix} a & b \\ & d \end{bmatrix}]_k.$$

⌟

Proof: By column reduction, we can make any matrix in Δ_n the form as above, and if two elements of the form $\begin{bmatrix} a & b \\ & d \end{bmatrix}$ differ by an element of $\Gamma_0(N)$, they differ by an upper-triangular matrix in $\Gamma_0(N)$, thus a, d are determined, and also $b \mod d$. □

Cor. (20.2.2.10).

- $T(1) = \mathrm{id}$.
- If $(m,n) = 1$, then $T(m) \cdot T(n) = T(mn)$.
- If p is a prime that $(p,N) = 1$ and $n \geq 1$, then $T(p^n) \cdot T(p) = T(p^{n+1}) + pR(p) \cdot T(p^{n-1})$, where $R(p)$ is the coset $\Gamma_0(N)\begin{bmatrix} p & \\ & p \end{bmatrix}$.
- $\mathcal{R}_N$ is generated by $T(p), R(p), R(p)^{-1}$.

⌟

Proof: 1: Trivial.

2: This follows from Chinese remainder theorem.

3: Omitted. □

Prop. (20.2.2.11) [Explicit Hecke Operators]. Let $f = \sum A(m)q^m \in S_k(N,\chi)$, then for $(n,N)=1$, $T(n)f$ has a Fourier expansion

$$T(n)f = \sum B(m)q^m,$$

where

$$B(m) = \sum_{ad=n, a|m} (\frac{a}{d})^{k/2}\chi(d)^{-1} dA(\frac{md}{a}).$$

⌟

Proof:

$$\begin{aligned}(T(n)f)(z) &= \sum_{ad=n} \sum_{b \mod d} (\frac{a}{d})^{k/2}\chi(d)^{-1} f(\frac{az+b}{d}) \\ &= \sum_{ad=n} \sum_{b \mod d} (\frac{a}{d})^{k/2} \sum_{m=1}^{\infty} A(m)\exp(2\pi i \frac{amz}{d})\exp(2\pi i\frac{mb}{d}) \\ &= \sum_{m=1}^{\infty} \sum_{ad=n, d|m} (\frac{a}{d})^{k/2}\chi(d)^{-1} dA(m)\exp(2\pi i\frac{amz}{d})\end{aligned}$$

Thus $B(m) = \sum_{ad=n,a|m} (\frac{a}{d})^{k/2}\chi(d)^{-1} dA(\frac{md}{a})$. □

Prop. (20.2.2.12) [Normalized Hecke Eigenforms]. If $f = \sum c_n q^n \neq 0 \in M_k(N,\chi)$ that satisfies

$$T(n)f = n^{1-k/2}\chi(n)^{-1}\lambda(n)f$$

for all $(n,N)=1$ and $\lambda(n) \in \mathbb{C}$, then $c_1 \neq 0$, and if f is normalized that $c_1 = 1$, then $c_n = \lambda(n)$ for all such n. In particular, c_n are all real, because $T(n)$ is Hermitian(20.2.2.7). ⌟

Proof: By(20.2.2.11),

$$n^{1-k/2}\lambda(n)A(m) = \sum_{ad=n,a|m} (\frac{a}{d})^{k/2}\chi(d)^{-1} dA(\frac{md}{a}),$$

thus for $(m,n)=1$, $\lambda(n)A(m) = A(mn)$, and $\lambda(n) = A(n)$. □

New Forms

Def. (20.2.2.13) [Old and New Forms]. Let $\alpha_d = \mathrm{diag}(d,1)$, and let $S_k(\Gamma_1(N))[d]$ be the subspace of $S_k(\Gamma_1(N))$ consisting of elements of the form $f + g[\alpha_d]_k$, $f, g \in S_k(\Gamma_1(N/d))$, and let

$$S_k(\Gamma_1(N))_{\text{old}} = \sum_{p\in\mathbf{P}, p|N} S_k(\Gamma_1(N))[p],$$

called the space of **old forms of level** N. Also the space

$$S_k(\Gamma_1(N))_{\text{new}} = S_k(\Gamma_1(N))^{\perp}_{\text{old}},$$

called the space of **new forms of level** N. ⌟

Remark (20.2.2.14). Omitting the $p \in$ `Prime` condition in the definition of oldforms doesn't change the space. ⌟

Remark (20.2.2.15). The dimension of newforms and oldforms are calculated by [Dimensions of the Spaces of Cusp Forms and Newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$]. ⌟

Prop. (20.2.2.16). $S_k(\Gamma_1(N))_{\text{old}}$ and $S_k(\Gamma_1(N))_{\text{new}}$ are both stable under action of $\mathcal{R}_N$. In particular, they have a orthogonal basis of Hecke eigenforms for the Hecke operators, by(20.2.2.7)(20.2.2.8). ⌟

Proof: By(20.2.2.10), for $R(n)$, $R(n)(f+g[\alpha_p]) = R(n)f + (R(n)g)[\alpha_p]$, for $T(\ell)$, $\ell \neq p$, $T(\ell)(f+g[\alpha_p]) = T(\ell)f + (T(\ell)g)[\alpha_p]$ because d is prime to ℓ. □

Prop. (20.2.2.17) [Strong Multiplicity One]. If $f \in S_k(\Gamma_0(N),\chi)_{\text{new}}, f' \in S_k(\Gamma_0(N'),\chi)_{\text{new}}$ are normalized new eigenforms having the same eigenvalues for a.e. T_p, then $N = N'$ and $f = f'$. ⌟

Proof: Cf.[On some results of Artin and Lehner, Casselman].**?** □

3 Dimension Formulae

Def. (20.2.3.1) [Notations]. In this subsection,

- Γ is a **congruence subgroup of** $\mathrm{SL}(2,\mathbb{Z})$.
- g is the genus of $X(\Gamma)$.
- d is the degree of the map $X(\Gamma) \to X(1)$ which is equal to $[SL(2,\mathbb{Z}) : \{\pm 1\}\Gamma]$.
- ε_2 is the number of elliptic points with period 2.
- ε_3 is the number of elliptic points with period 3.
- ε_∞ is the number of cusps.
- $\varepsilon_\infty^{\text{reg}}$ is the number of regular cusps(20.1.1.2).
- ε_∞^{irr} is the number of irregular cusps.

⌟

Prop. (20.2.3.2) [Genus Formula].

$$g = 1 + \frac{d}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2}.$$

⌟

Proof: Cf. [Diamond, P68].**?** □

Thm. (20.2.3.3) [Dimension Formulae for k Even]. For $k \in 2\mathbb{Z}$,

$$\dim(\mathrm{MF}_k(\Gamma)) = \begin{cases} \frac{(k-1)d}{12} + (\frac{1}{4} - \{\frac{k}{4}\})\varepsilon_2 + (\frac{1}{3} - \{\frac{k}{3}\})\varepsilon_3 + \frac{1}{2}\varepsilon_\infty & k \geq 2 \\ 1 & k = 0 \\ 0 & k < 0 \end{cases}$$

and

$$\dim(\mathrm{SF}_k(\Gamma)) = \begin{cases} \frac{(k-1)d}{12} + (\frac{1}{4} - \{\frac{k}{4}\})\varepsilon_2 + (\frac{1}{3} - \{\frac{k}{3}\})\varepsilon_3 - \frac{1}{2}\varepsilon_\infty & k \geq 4 \\ g & k = 2 \\ 0 & k \leq 0 \end{cases}$$

⌟

Proof: Cf.[Diamond P87]. □

Cor. (20.2.3.4). For any Fuchsian group $\Gamma \subset \mathrm{SL}(2,\mathbb{R})$ and $k \in \mathbb{Z}$,

$$\dim \mathrm{MF}_k(\Gamma) \leq \frac{\mathrm{Vol}(\mathrm{SL}(2;\mathbb{R})/\Gamma)}{4\pi} \cdot k + 1.$$

In particular, $\mathrm{MF}_0(\Gamma) = 0$. ⌟

Proof: Cf.[Modular Forms, 1-2-3]P12. □

Cor. (20.2.3.5). For any Fuchsian subgroup $\Gamma \subset \mathrm{SL}(2;\mathbb{R})$, any three $f, g, h \in \mathrm{MF}_*(\Gamma)$ are note alg.independent. ⌟

Proof: Otherwise for n large, $\dim \mathrm{MF}_n(\Gamma) = \Omega(n^2)$. □

Prop. (20.2.3.6) [Dimension Formulae for k Odd]. For k odd,

- if $k < 0$ or $-\mathbf{1} \in \Gamma$, then $\mathrm{MF}_k(\Gamma) = \mathrm{SF}_k(\Gamma) = 0$.
- If $k \geq 3$, $-\mathbf{1} \notin \Gamma$, then

$$\dim(\mathrm{MF}_k(\Gamma)) = (k-1)(g-1) + \lfloor \frac{k}{3} \rfloor \varepsilon_3 + \frac{k}{2}\varepsilon_\infty^{\mathrm{reg}} + \frac{k-1}{2}\varepsilon_\infty^{irr}$$

$$\dim(\mathrm{SF}_k(\Gamma)) = (k-1)(g-1) + \lfloor \frac{k}{3} \rfloor \varepsilon_3 + (\frac{k}{2} - 1)\varepsilon_\infty^{\mathrm{reg}} + \frac{k-1}{2}\varepsilon_\infty^{irr}$$

- If $k = 1$, $-\mathbf{1} \notin \Gamma$, then

$$\dim(\mathrm{MF}_1(\Gamma)) \begin{cases} = \varepsilon_\infty^{\mathrm{reg}}/2 & \varepsilon_\infty^{\mathrm{reg}} > 2g-2 \\ \geq \varepsilon_\infty^{\mathrm{reg}}/2 & \varepsilon_\infty^{\mathrm{reg}} \leq 2g-2 \end{cases}, \quad \dim(\mathrm{SF}_1(\Gamma)) = \dim(\mathrm{MF}_1(\Gamma)) - \varepsilon_\infty^{\mathrm{reg}}/2.$$

⌟

Proof: Cf.[Diamond P91]. □

Explicite Dimension Formulae for $\Gamma(N), \Gamma_1(N), \Gamma_0(N)$

Lemma (20.2.3.7). For $N \in \mathbb{Z}_{\geq 2}$,

$$\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}/(N))$$

is surjective. ⌟

Proof: Cf.[**?**]P101. □

Prop. (20.2.3.8) [Degrees for $\Gamma(N), \Gamma_1(N), \Gamma_0(N)$].

- The degree of the mapping $X(N) \to X(1)$ is

$$d = d_N = [\mathrm{SL}(2,\mathbb{Z}) : \{\pm 1\}\Gamma(N)] = \begin{cases} 1/2N^3 \prod_{p|N}(1 - 1/p^2) & N > 2 \\ 6 & N = 2 \end{cases}$$

- There is a coset decomposition $\Gamma_1(N) = \coprod_{j=1}^N \Gamma(N) \begin{bmatrix} 1 & j \\ & 1 \end{bmatrix}$, in particular, $d = [\mathrm{SL}(2,\mathbb{Z}) : \{\pm 1\}\Gamma_1(N)] = d_N/N, N \geq 2$.

- There is a coset decomposition $\Gamma_0(N) = \coprod_{y \mod N,(y,N)=1} \Gamma_1(N) \begin{bmatrix} x & k \\ N & y \end{bmatrix}$, where x, k are chosen that $xy - kN = 1$. In particular, $d = [\mathrm{SL}(2,\mathbb{Z}) : \Gamma_0(N)] = 2d_N/N\varphi(N), N \geq 2$.

⌟

Proof: 1: By(20.2.3.7), the map $SL(2,\mathbb{Z}) \to SL(2,\mathbb{Z}/N\mathbb{Z})$ is surjective, so $[\Gamma(N) : \Gamma(1)] = \#SL(2,\mathbb{Z}/N\mathbb{Z})$. Let $N = \prod p_i^{n_i}$, then $SL(2,\mathbb{Z}/N\mathbb{Z}) \cong \prod_i SL(2,\mathbb{Z}/p_i^{n_i}\mathbb{Z})$, and calculating depending on e_{11} is invertible or e_{12} is invertible, $\#SL(2,\mathbb{Z}/p_i^{n_i}\mathbb{Z}) = 2(p^{n_i} - p^{n_i-1})p^{2n_i} - (p^{n_i} - p^{n_i-1})^2 p^{n_i} = p_i^{3n_i} - p_i^{3n_i-2}$. Thus $\#\,\mathrm{SL}(2,\mathbb{Z}/(N)) = N^3 \prod_{p|N}(1-p^{-2})$, and we get the desired formula. □

Prop. (20.2.3.9) [Elliptic Points for $\Gamma(N), \Gamma_1(N), \Gamma_0(N)$]. For $N \in \mathbb{Z}_+$,

- There are on elliptic points for $\Gamma(N)$ for $N \geq 2$.
- There are on elliptic points for $\Gamma_1(N)$ for $N \geq 4$.
- The elliptic points of period 2 for $\Gamma_0(N)$ corresponds to the ideals $J \subset \mathrm{Ideal}(\mathbb{Z}[i])$ s.t. $\mathbb{Z}[i]/J \cong \mathbb{Z}/(N)$, and the elliptic points of period 3 for $\Gamma_0(N)$ corresponds to the ideals $J \subset \mathrm{Ideal}(\mathbb{Z}[\omega])$ s.t. $\mathbb{Z}[\omega]/J \cong \mathbb{Z}/(N)$.

⌟

Proof: Cf.[Diamond]P56, 95.**?** □

Lemma (20.2.3.10). Let $s = a/c, s' = a'/c' \in \mathbb{P}^1(\mathbb{Q})$ with $(a,c) = (a',c') = 1$, then for any $\gamma \in SL(2,\mathbb{Z})$,

$$s' = \gamma(s) \iff \begin{bmatrix} a' \\ c' \end{bmatrix} = \pm\gamma \begin{bmatrix} a \\ c \end{bmatrix}.$$

⌟

Proof: □

Lemma (20.2.3.11). Let $s = a/c, s' = a'/c' \in \mathbb{P}^1(\mathbb{Q})$ with $(a,c) = (a',c') = 1$, then

- $\Gamma(N)s' = \Gamma(N)s \iff \begin{bmatrix} a' \\ c' \end{bmatrix} \equiv \pm \begin{bmatrix} a \\ c \end{bmatrix} \mod N$
- $\Gamma_1(N)s' = \Gamma_1(N)s \iff \begin{bmatrix} a' \\ c' \end{bmatrix} \equiv \pm \begin{bmatrix} a + jc \\ c \end{bmatrix} \mod N$, for some j.
- $\Gamma_0(N)s' = \Gamma_0(N)s \iff \begin{bmatrix} ya' \\ c' \end{bmatrix} \equiv \begin{bmatrix} a + jc \\ c \end{bmatrix} \mod N$, for some y relatively prime to N and some j.

⌟

Proof: Use(20.2.3.10).

1: One direction is clear, for the other, If $\begin{bmatrix} a' \\ c' \end{bmatrix} \equiv \pm \begin{bmatrix} a \\ c \end{bmatrix} \mod N$, take b, d that $ac - bd = 1$, then $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ maps $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ to $\begin{bmatrix} a \\ c \end{bmatrix}$. As $\Gamma(N)$ is normal in $\Gamma(1)$, it suffices to prove for $\begin{bmatrix} a \\ c \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Then $a' \equiv 1 \mod N$, take integers β, δ that $a'\delta - c'\beta = (1-\alpha')/N$, let $\gamma = \begin{bmatrix} a' & \beta N \\ c' & \delta N \end{bmatrix}$, then $\gamma \in \Gamma(N)$ and $\begin{bmatrix} a' \\ c' \end{bmatrix} = \gamma \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

2 follows from 1 and the coset decomposition $\Gamma_1(N) = \coprod_{j=1}^{N} \Gamma(N)\begin{bmatrix}1 & j\\ & 1\end{bmatrix}$.

3: There is a coset decomposition $\Gamma_0(N) = \coprod_{y \mod N,(y,N)=1} \Gamma_1(N)\begin{bmatrix}x & k\\ N & y\end{bmatrix}$, where x, k are chosen that $xy - kN = 1$. Then

$$\Gamma_0(N)s' = \Gamma_0(N)s \iff \begin{bmatrix}a'\\ c'\end{bmatrix} \equiv \pm\begin{bmatrix}xa+kc+jcy\\ cy\end{bmatrix} \mod N, \exists j, (y,N)=1$$
$$\iff \begin{bmatrix}ya'\\ c'\end{bmatrix} \equiv \begin{bmatrix}a+jc\\ cy\end{bmatrix} \mod N, \exists j, (y,N)=1$$

□

Prop. (20.2.3.12) [Cusps for $\Gamma(N), \Gamma_1(N), \Gamma_0(N)$]. For $N \in \mathbb{Z}_+$,

- $\varepsilon_\infty(\Gamma_0(N)) = \sum_{d|N} \varphi((d, N/d))$.
-

⌟

Proof: 1: By(20.2.3.11), if $\Gamma_0(N)s' = \Gamma_0(N)s$, then $\begin{bmatrix}ya'\\ c'\end{bmatrix} \equiv \begin{bmatrix}a+jc\\ c\end{bmatrix} \mod N$, which means first $(c, N) = (c', N)$. So we consider the equivalence classes with $(c, N) = d$. In this case any equivalence class has a representative that $c = d$. Consider the equivalence relations between them, then $\begin{bmatrix}a'\\ d\end{bmatrix}$ represents the same cusp as $\begin{bmatrix}a\\ d\end{bmatrix}$ iff $(y_0 + iN/d)a' \equiv a + jd \mod N$ for some i, j, which is equivalent to $a' \equiv y_0 a \mod (c, N, a'N/d) = (d, N/d)$. So there are $\sum_{d|N} \varphi((d, N/d))$ many equivalence classes(cusps). □

Prop. (20.2.3.13) [Regular Cusps]. All the cusps of $\Gamma_0(N)$ and $\Gamma(N)$ are regular. The only irregular cusp of $\Gamma_1(N)$ are $s = 1/2$ for $N = 4$. ⌟

Proof: Cf.[?]P103. □

Thm. (20.2.3.14) [Lists of Statistics for $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$]. For $N \in \mathbb{Z}_+$,

Γ	d	ε_2	ε_3	ε_∞
$\Gamma_0(N), N > 2$	$\frac{2d_N}{N\varphi(N)}$	$\begin{cases}\prod_{p|N}(1+(\frac{-1}{p})) & 4 \nmid N\\ 0 & 4|N\end{cases}$	$\begin{cases}\prod_{p|N}(1+(\frac{-3}{p})) & 9 \nmid N\\ 0 & 9|N\end{cases}$	$\sum_{d|N} \varphi((d, N/d))$
$\Gamma_1(2)(= \Gamma_0(2))$	3	1	0	2
$\Gamma_1(3)$	4	0	1	2
$\Gamma_1(4)$	6	0	0	3
$\Gamma_1(N), N > 4$	d_N/N	0	0	$\frac{1}{2}\sum_{d|N} \varphi(N)\varphi(N/d)$
$\Gamma(1)(= \Gamma_1(1))$	1	1	1	1
$\Gamma(N), N > 1$	d_N	0	0	d_N/N

where

$$d_N = \begin{cases}1/2\prod_{p|N} N^3(1-1/p^2) & N > 2\\ 6 & N = 2\end{cases}.$$

⌟

Proof: Cf.[Diamond P107].

The numbers $\varepsilon_2(\Gamma_0(N))$ and $\varepsilon_3(\Gamma_0(N))$ follow from(20.2.3.9) and the informations on $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$(14.4.1.46). □

Example (20.2.3.15) [Statistics for $X_0(p)$]. For $p \in \mathtt{Prime}$,

- $\Gamma(1) = \coprod_j \Gamma_0(p)\alpha_j$, where $\alpha_j = \begin{bmatrix} 1 & \\ j & 1 \end{bmatrix}$ when $j \in \{0, \ldots, p-1\}$ and $\alpha_\infty = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$.
- $\varepsilon_\infty = 2$.
- $\varepsilon_2(\Gamma_0(p)) = 1 + \left(\frac{-1}{p}\right)$.
- $\varepsilon_3(\Gamma_0(p)) = 1 + \left(\frac{-3}{p}\right)$.
- $d = p + 1$.
- $g = \begin{cases} \lfloor \frac{p+1}{12} \rfloor - 1 & , p \equiv 1 (\mathrm{mod}\ 12) \\ \lfloor \frac{p+1}{12} \rfloor & , \text{otherwise} \end{cases}$.

⌟

Proof: Only the first one need a proof:? □

Cor. (20.2.3.16) [List of Dimension Formulae for $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$]. For $N \in \mathbb{Z}_+$,

Γ	$g(X(\Gamma))$	$\dim(M_k(\Gamma))$& $\dim(S_k(\Gamma))$, $2\vert k, k \geq 2$	$\dim(M_k(\Gamma))$& $\dim(S_k(\Gamma))$, $2\vert k+1, k \geq 3$
$\Gamma_0(N), N > 2$	long expression, cf.(20.2.3.2)	expression too long	expression too long
$\Gamma_1(2)(\Gamma_0(2))$	0	$\lfloor \frac{k}{4} \rfloor \pm 1$	0
$\Gamma_1(3)$	0	$\lfloor \frac{k}{3} \rfloor \pm 1$	$\lfloor \frac{k}{3} \rfloor \pm 1$
$\Gamma_1(4)$	0	$\frac{k-1\pm 3}{2}$	$\frac{k-1\pm 2}{2}$
$\Gamma_1(N), N > 4$	$1 + \frac{d_N}{12N} - \frac{1}{4}\sum_{d\vert N} \varphi(d)\varphi(N/d)$	$\frac{(k-1)d_N}{12N} \pm \frac{1}{4}\sum_{d\vert N} \varphi(d)\varphi(N/d)$	$\frac{(k-1)d_N}{12N} \pm \frac{1}{4}\sum_{d\vert N} \varphi(d)\varphi(N/d)$
$\Gamma(1)(\Gamma_1(1))$	0	1	1
$\Gamma(2)$	0	$\frac{k-1\pm 3}{2}$	0
$\Gamma(N), N > 2$	$1 + \frac{d_N(N-6)}{12N}$	0	$\frac{(k-1)d_N}{12N} \pm \frac{d_N}{2N}$

⌟

Proof: These follow from(20.2.3.2)(20.2.3.3)(20.2.3.6)(20.2.3.14) and(20.2.3.13). □

Remark (20.2.3.17) [Dimension for MF_1]. The only case that is not calculated is the dimensions of $\dim(M_1(\Gamma))$. But we may use(20.2.3.4) to get that

$$\dim \mathrm{MF}_1(\Gamma_1(N)) \leq \frac{d_N}{12N} + 1.$$

⌟

Cor. (20.2.3.18) [Low Genus Cases]. For $N \in \mathbb{Z}_+$,

- $g(X(N)) = 0$ iff $N \in \{1, 2, 3, 4, 5\}$.
- $g(X(N)) = 1$ iff $N = 6$.
- $g(X_1(N)) = 0$ iff $N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$.

- $g(X_1(N)) = 1$ iff $N \in \{11, 14, 15\}$.
- $g(X_0(N)) = 0$ iff $N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$.
- $g(X_0(N)) = 1$ iff $N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$.

⌟

Proof: If $N = \prod_p p^{e_p}$,

1, 2:

3, 4:

$$g(X_1(N)) = 1 + \frac{1}{24}\prod_{p|N} p^{2e_p}(1-\frac{1}{p^2}) - \frac{1}{4}\prod_p p^{e_p-2}(p-1)[(p+1)-e_p(p-1)],$$

so if $g(X_1(N)) = 0$,

$$\prod_p \frac{p^{e_p}(p+1)}{[(p+1)+e_p(p-1)]} < 6.$$

Then it can be verified that $e_2 \le 3, e_3 \le 2, e_5 \le 1, e_7 \le 1, e_{11} \le 1$, $e_p = 0$ for $p > 11 \in \mathbf{P}$. Then the assertion follows. 4 is similar.

5, 6:**?** □

<u>**Low Dimensional Tabulatetes**</u>

Prop. (20.2.3.19). Let $N, k \in \mathbb{Z}_+$ s.t. $2k(N+1) = 24$, then

$$\mathrm{SF}_{2k}(\Gamma_0(N)) = \mathrm{SF}_{2k}(\Gamma_1(N)) = \mathbb{C}.g(\tau).$$

where $g(\tau) = (\eta(\tau)\eta(N\tau))^k$. ⌟

Proof: Cf.[Koblitz]P130 or [Diamond]P75.

By**?**, $g(\tau)^{N+1} = \Delta(\tau)\Delta(N\tau) \in \mathrm{SF}_{24}(\Gamma_0(N))$, and it is non-vanishing on $\mathscr{H}$ as Δ does(20.2.4.23). So $(f(\tau)/g(\tau))^{N+1} \in \mathrm{MF}_0^!(\Gamma_0(N))$.

But $\mathrm{ord}_{\tau=\infty}\, g(\tau)^{N+1} = N+1$, and

$$g^{N+1}[S]_{24}(\tau) = N^{-12} q_N^{N+1} \prod[(1-q_N^n)^{24}(1-q_N^n)^{24}],$$

so $\mathrm{ord}_{\tau=0}\, g(\tau)^{N+1} = N+1$. So $(f(\tau)/g(\tau))^{N+1} \in \mathrm{MF}_0(\Gamma_0(N)) = \mathbb{C}$(20.2.3.4). □

4 Elliptic Eisenstein Series

Def. (20.2.4.1) [Eisenstein Series]. Let Γ be a congruence subgroup of $\Gamma(1)$, define the space of elliptic **Eisenstein series** $\mathrm{Eis}_k(\Gamma, \chi)$ to be the orthogonal complement of $\mathrm{SF}_k(\Gamma, \chi)$ in $\mathrm{MF}_k(\Gamma, \chi)$. Also denote $\mathrm{Eis}_k(\Gamma) = \mathrm{Eis}_k(\Gamma, 1)$. ⌟

Prop. (20.2.4.2) [Dimensions of Eisenstein Series]. Notation as in(20.2.3.1), by(20.2.3.3) and(20.2.3.6), the dimensions of the space of Eisenstein series satisfy:

$$\dim(E_k(\Gamma)) = \begin{cases} \varepsilon_\infty & k \ge 4, 2|k \\ \varepsilon_\infty - 1 & k = 2 \\ 1 & k = 0 \\ \varepsilon_\infty^{\mathrm{reg}} & k \ge 3, 2|k+1, -1 \notin \Gamma \\ \varepsilon_\infty^{\mathrm{reg}}/2 & k = 1, -1 \notin \Gamma \\ 0 & k < 0 \text{ or } 2|k+1, -1 \in \Gamma \end{cases}$$

And also the dimension of $E_k(\Gamma_0(N)), E_k(\Gamma_1(N)), E_k(\Gamma(N))$ can be read off from(20.2.3.16). ⌟

Eisenstein Series for $\Gamma(1)$

Def. (20.2.4.3). In this subsubsection, denote $q = e^{2\pi\,\mathrm{i}\,\tau}$. ⌟

Prop. (20.2.4.4) [Weakly Modular Forms and Lattices]. Let $\mathcal{L}$ be the set of lattices in $\mathbb{C}$. If $F : \mathcal{L} \to \mathbb{C}$ is a function of weight $2k$, i.e. $F(\lambda\Gamma) = \lambda^{-2k}F(\Gamma)$ for $\lambda \in \mathbb{C}^*$, then $f(z) = F(\Gamma(z, 1))$ is a weakly modular form on $\mathscr{H}$ for $\Gamma(1)$ of weight $2k$, and this is a bijection between functions of weight $2k$ on $\mathcal{L}$ and weakly modular functions on $\mathscr{H}$ for $\Gamma(1)$ of weight $2k$. ⌟

Proof: By the hypothesis, there is a function f on $\mathscr{H}$ that for any w_1, w_2 with $w_1/w_2 \in \mathscr{H}$,

$$F(\Gamma(w_1, w_2)) = w_2^{-2k} f(w_1/w_2).$$

Then the invariance of F under $\mathrm{SL}(2, \mathbb{Z})$ action implies f is weakly modular of weight $2k$. □

Prop. (20.2.4.5) [Eisenstein Series for $\mathrm{SL}(2, \mathbb{Z})$]. Let $k > 2$ be an even integer and Γ a lattice of $\mathbb{C}$, define the **Eisenstein series of weight** k to be

$$G_k(\Gamma) = \sum_{\omega\in\Lambda,\omega\neq 0} \frac{1}{\omega^k},$$

and also for a complex number z, let Λ_z be the lattice generated by 1 and z, and let $G_k(z) = G_k(\Gamma_z)$. Then $G_k(z) \in \mathrm{MF}_k(\Gamma(1))$, and

$$G_k(z) = 2\zeta(k) + 2\frac{(2\pi\,\mathrm{i})^k}{(k-1)!}\sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n$$

And denote

$$E_k(z) = G_k(z)/2\zeta(k) = \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0),\gcd(m,n)=1} \frac{1}{(m\tau + n)^k} = 1 - \frac{2k}{B_k}\sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n$$

the **normalized Eisenstein series**. ⌟

Proof: $G_k(z)$ is weakly modular of weight k by(20.2.4.4). For the expansion, notice by(11.4.3.11),

$$\pi\cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty}(\frac{1}{z+n} + \frac{1}{z-n}),$$

and by definition

$$z\cot(\pi z) = \pi\,\mathrm{i} - \frac{\pi\,\mathrm{i}}{1-q} = \pi\,\mathrm{i} - 2\pi\,\mathrm{i}\sum_{n=1}^{\infty} q^n$$

where $z \in \mathscr{H}$.

Taking $(k-1)$-th derivative of this, we get

$$\sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^k} = \frac{(-2\pi\,\mathrm{i})^k}{(k-1)!}\sum_{n=1}^{\infty} n^{k-1}q^n,$$

thus

$$\begin{aligned} G_k(z) &= \sum_{(m,n)\neq(0,0)} \frac{1}{(n\tau+m)^k} \\ &= 2\zeta(k) + 2\sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}} \frac{1}{(n\tau+m)^k} \\ &= 2\zeta(k) + \frac{2(-2\pi\,\mathrm{i})^k}{(k-1)!}\sum_{n=1}^{\infty}\sum_{a=1}^{\infty} a^{k-1}q^{an} \\ &= 2\zeta(k) + 2\frac{(2\pi\,\mathrm{i})^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n \end{aligned}$$

Finally the assertion about $E_k(z)$ follows from(21.7.4.1).

To show the Eisenstein series is orthogonal to any cusp form, notice for any cusp form $f \in \mathcal{S}_k(\Gamma(1))$,

$$f(\gamma\tau)(\mathrm{Im}(\gamma\tau))^k = f(z)\overline{\tau(\gamma,z)}^{-k}\,\mathrm{Im}(z)^k$$

and by(20.2.4.5)

$$G_k(\tau) = \sum_{(m,n)\neq 0\in\mathbb{Z}^2} \frac{1}{(m\tau+n)^k} = \sum_{\Gamma(1)_\infty\backslash\Gamma(1)} \frac{1}{\tau(\gamma,\tau)^k},$$

so

$$\begin{aligned} \int_{\Gamma(1)\backslash\mathscr{H}} f(\tau)\overline{G_k(z)}y^k\frac{\mathrm{d}x\mathrm{d}y}{y^2} &= \int_{\Gamma(1)\backslash\mathscr{H}}\sum_{\Gamma(1)_\infty\backslash\Gamma(1)} f(z)\overline{\tau(\gamma,z)}^{-k}y^k\frac{\mathrm{d}x\mathrm{d}y}{y^2} \\ &= \int_{\Gamma(1)\backslash\mathscr{H}}\sum_{\Gamma(1)_\infty\backslash\Gamma(1)} f(\gamma z)(\mathrm{Im}(\gamma z))^k\frac{\mathrm{d}x\mathrm{d}y}{y^2} \\ &= \int_{\Gamma(1)_\infty\backslash\mathscr{H}} f(z)(\mathrm{Im}\,z)^k\frac{\mathrm{d}x\mathrm{d}y}{y^2} \\ &= \int_0^\infty[\int_0^1 f(x+iy)\mathrm{d}x]y^{k-2}\mathrm{d}y = 0 \end{aligned}$$

as f is a cusp form. □

Cor. (20.2.4.6). By(20.2.4.5) and(9.5.1.12):

$$E_4(z) = 1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n,\quad E_6(z) = 1-504\sum_{n=1}^{\infty}\sigma_5(n)q^n$$

$$E_8(z) = 1+480\sum_{n=1}^{\infty}\sigma_7(n)q^n,\quad E_{10}(z) = 1-264\sum_{n=1}^{\infty}\sigma_9(n)q^n$$

$$E_{12}(z) = 1+\frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n,\quad E_{14}(z) = 1-24\sum_{n=1}^{\infty}\sigma_{13}(n)q^n.$$

⌟

Cor. (20.2.4.7) [Ramanujan Identities]. By(20.2.4.8),

$$\dim \mathrm{MF}_6(\Gamma(1)) = \dim \mathrm{MF}_8(\Gamma(1)) = \dim \mathrm{MF}_{10}(\Gamma(1)) = \dim \mathrm{MF}_{14}(\Gamma(1)) = 1,$$

so there are identities:

$$E_4^2 = E_8, \quad E_4E_6 = E_{10}, \quad E_6E_8 = E_4E_{10} = E_{14}$$

which give equations like:

$$\sigma_7(n) = \sigma_3(n) + 120\sum_{m=1}^{n-1}\sigma_3(m)\sigma_3(n-m)$$

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 1054\sum_{m=1}^{n-1}\sigma_3(m)\sigma_5(n-m).$$

⌟

Cor. (20.2.4.8) [Modular Forms for $\Gamma(1)$].

$$\mathrm{MF}_*(\Gamma(1)) = \mathbb{C}[E_4, E_6], \quad \mathrm{SF}_*(\Gamma(1)) = \Delta.\,\mathrm{MF}_*(\Gamma(1)).$$

Thus for $k \geq 4$ even,

$$\dim(S_k(\Gamma(1))) = \begin{cases} \lfloor \frac{k}{12} \rfloor - 1 & k \equiv 2 \mod 12 \\ \lfloor \frac{k}{12} \rfloor & \text{otherwise} \end{cases}.$$

$$\mathrm{MF}_k(\Gamma(1)) = \mathrm{MF}_k(\Gamma(1)) \oplus \mathbb{C}E_k.$$

⌟

Proof: Cf.[Diamond P88] or [Koblitz, Modular Forms]P118. □

Cor. (20.2.4.9). $\mathrm{MF}(\Gamma(1)) = \mathrm{MF}(\Gamma(1), \mathbb{Z})_{\mathbb{C}}$, $\mathrm{SF}(\Gamma(1)) = \mathrm{SF}(\Gamma(1), \mathbb{Z})_{\mathbb{C}}$(20.2.6.4). ⌟

Proof: By(20.2.4.20), E_4, E_6 have Fourier coefficients in $\mathbb{Z}$. □

Eisenstein Series for $\Gamma_0(N)$

Cf.[Diamond] or [Koblitz]P131.

Prop. (20.2.4.10). For $k, N \in \mathbb{Z}_+, k \geq 3$ and $\chi \in \mathrm{Diri}(N)$ s.t. $\chi(-1) = (-1)^k$, there is an Eisenstein series

$$G_{k,\chi}(\tau) = \frac{1}{2}L(1-k,\chi) + \sum_{n\in\mathbb{Z}_+}(\sum_{d|n}\chi(d)d^{k-1})e^{2\pi \mathrm{i}\,\tau} \in \mathrm{MF}_k(\Gamma_0(N), \chi).$$

⌟

Proof: □

Prop. (20.2.4.11) [Connection with Dedekind eta-Functions]. For $p \in \mathtt{Prime}_{\geq 3}$, let

$$h(\tau) = \prod_{a_2=1} p - 1G_3^{(0,a_2)((\mathrm{mod}\ \ p))}(\tau), \quad f(\tau) = \prod_{a_2=1}\frac{p-1}{2}G_3^{(0,a_2)((\mathrm{mod}\ \ p))}(\tau),$$

then

- $h(\tau) = (-1)^{(p-1)/2} f(\tau)$,
- $f(\tau) \in \mathrm{MF}_{3(p-1)/2}(\Gamma_0(p), \left(\frac{-}{p}\right))$, $h(\tau) \in \mathrm{MF}_{3(p-1)}(\Gamma_0(p))$.
- $f(\tau)$ is a constant multiple of $(\eta^p(\tau)/\eta(p\tau))^3$.

⌟

Proof: Cf.[Koblitz]P135, 136.**?** □

General Eisenstein Series

Quasimodular Forms

Def. (20.2.4.12) [Almost Modular Forms]. For a discrete subgroup $\Gamma \subset \mathrm{SL}(2;\mathbb{R})$, let $\widehat{M}_k^{\leq p}(\Gamma)$ be the space of functions in $C^\infty(\mathscr{H})$ of the form $F(\tau) = \sum_{r=0}^p f_r(\tau)(-4\pi y)^{-r}$, where f_r are holomorphic on $\mathscr{H}$ and holomorphic at the cusps, and $F[\gamma]_k = F$ for any $\gamma \in \Gamma$.

Denote $\widehat{\mathrm{MF}}_k(\Gamma) = \cup_{p=0}^\infty \widehat{\mathrm{MF}}_k^{\leq p}(\Gamma)$ and the graded ring $\widehat{\mathrm{MF}}_*(\Gamma) = \oplus_{k\geq 0}\widehat{\mathrm{MF}}_k(\Gamma)$, called the space of **almost modular forms**. ⌟

Def. (20.2.4.13) [Quasi-Modular Forms]. The graded ring $\widetilde{\mathrm{MF}}_*(\Gamma)$ of **quasi-modular forms** is defined to be the constant terms(f_0) of functions in $\widehat{\mathrm{MF}}_*(\Gamma)$. Any almost modular function is determined by its constant term, so $\widetilde{\mathrm{MF}}_*(\Gamma)$ is canonically isomorphic to $\widehat{\mathrm{MF}}_*(\Gamma)$.**?** ⌟

Proof: □

Eisenstein Series of Weight 2

Def. (20.2.4.14) [$E_2(\tau)$]. Denote

$$G_2(\tau) = \frac{1}{2}\sum_{n\neq 0}\frac{1}{n^2} + \frac{1}{2}\sum_{m\neq 0}\sum_{n\in\mathbb{Z}}\frac{1}{(m\tau+n)^2}.$$

This summation is convergent but not absolutely convergent, and

$$E_2(\tau) = \frac{6}{\pi^2}G_2(\tau) = 1 - 24q - 72q^2 + \ldots \in \widetilde{M}_2^{\leq 1}(\Gamma(1))$$

with

$$G_2^*(\tau) = G_2(\tau) - \frac{\pi}{2\,\mathrm{Im}(\tau)}, \quad E_2^*(\tau) = \frac{6}{\pi^2}G_2^*(\tau) = E_2(\tau) - \frac{3}{\pi\,\mathrm{Im}(\tau)} \in \widehat{M}_2^{\leq 1}(\Gamma(1)).$$

In particular, $E_2(\tau)$ satisfies

$$E_2[\gamma]_2(\tau) = E_2(\tau) + \frac{12}{2\pi\,\mathrm{i}}\frac{c}{c\tau+d}, \quad \gamma \in \Gamma(1)$$

⌟

Proof: For $\varepsilon \in \mathbb{R}_+$, define

$$G_{2,\varepsilon}(\tau) = \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)}\frac{1}{(mz+n)^2|mz+n|^\varepsilon},$$

then it is absolutely convergent and

$$G_{2,\varepsilon}(\gamma(\tau)) = (cz+d)^2|cz+d|^{2\varepsilon}G_{2,\varepsilon}(\tau).$$

Then it suffices to show that $\lim_{\varepsilon\to 0} G_{2,\varepsilon}(\tau) = G_2^*(\tau)$.

Define

$$I_\varepsilon(\tau) = \int_{-\infty}^{\infty} \frac{\mathrm{d}t}{(z+t)^2|z+t|^{2\varepsilon}},$$

then

$$G_{2,\varepsilon}(\tau) - \sum_{m\in\mathbb{Z}_+} I_\varepsilon(m\tau) = \sum_{n\in\mathbb{Z}_+} \frac{1}{n^{2+2\varepsilon}} + \sum_{m\in\mathbb{Z}_+}\Big(\sum_{n\in\mathbb{Z}} \frac{1}{(m\tau+n)^2|m\tau+n|^{2\varepsilon}} - \int_n^{n+1} \frac{\mathrm{d}t}{(m\tau+t)^2|m\tau+t|^{2\varepsilon}}\Big).$$

This sum is absolutely convergent for $\varepsilon > -1/2$, thus when $\varepsilon \to 0$, it just equals $G_2(\tau)$.

On the other hand, for $\varepsilon > -1/2$,

$$I_\varepsilon(x+\mathrm{i}\,y) = \int_{-\infty}^{\infty} \frac{\mathrm{d}t}{(x+t+\mathrm{i}\,y)^2((x+t)^2+y^2)^\varepsilon} = \frac{I(\varepsilon)}{y^{1+2\varepsilon}},$$

where $I(\varepsilon) = \int_{-\infty}^{\infty}(t+\mathrm{i})^{-2}(t^2+1)^{-\varepsilon}\mathrm{d}t$. We have $I(0) = 0$, and

$$I'(0) = \int_{-\infty}^{\infty} \frac{\log(t^2+1)}{(t+\mathrm{i})^2}\mathrm{d}t = \Big(\frac{1+\log(t^2+1)}{t+\mathrm{i}} - \arctan t\Big)\Big|_{-\infty}^{\infty} = -\pi.$$

For $\varepsilon \in \mathbb{R}_+$, $\sum_{m\in\mathbb{Z}_+} I_\varepsilon(m\tau) = I(\varepsilon)\zeta(1+2\varepsilon)/y^{1+2\varepsilon}$, so $\lim_{\varepsilon\to 0}\sum_{m\in\mathbb{Z}_+} I_\varepsilon(m\tau) = -\pi/2y$. □

Eisenstein Series of Weight 1

Prop. (20.2.4.15). For $N \in \mathbb{Z}_+, k = 1$, we can modify to give a definition of

$$G_{1,\chi}(\tau) \in \mathrm{MF}_1(\Gamma_0(N), \chi).$$

⌟

Prop. (20.2.4.16) [Eisenstein Series of Weight 1]. For $N \in \mathbb{Z}_+$, the set

$$\{E^{\psi,\varphi,1}\}$$

is a basis for $\mathrm{Eis}_1(\Gamma_1(N))$. In fact, for any $\chi \in \mathrm{Diri}(N)$, the set

$$\{E^{\psi,\varphi,1}, \varphi\psi = \chi\}$$

is a basis for $\mathrm{Eis}_1(\Gamma(N), \chi)$(20.2.4.1). ⌟

Proof: Cf.[Diamond]P141. □

Derivatives

Prop. (20.2.4.17) [Derivations of Modular Forms]. Let Γ be a discrete subgroup of $\mathrm{SL}(2;\mathbb{R})$ and $f\in\mathrm{MF}_k(\Gamma)$, then

$$Df\overset{\triangle}{=}\frac{1}{2\pi\,\mathrm{i}}\frac{\partial}{\partial\tau}f=q\frac{\partial}{\partial q}f=\sum_{n=1}^{\infty}na_nq^n$$

satisfies

$$(Df)[\gamma]_{k+2}(\tau)=(Df)(\tau)+\frac{k}{2\pi\,\mathrm{i}}\frac{c}{cz+d}f(z),\quad \gamma\in\Gamma.$$

In particular, by(20.2.4.14), $\theta_k(f)=D(f)-\frac{k}{12}E_2f\in\mathrm{MF}_{k+2}(\Gamma)$, called the **Serre derivation** of f.
⌟

Proof: This follows form differentiating the equation $f(\frac{az+b}{cz+d})=(cz+d)^kf(z)$. □

Cor. (20.2.4.18).

$$D(E_2)=\frac{E_2^2-E_4}{12},\quad D(E_4)=\frac{E_2E_4-E_6}{3},\quad D(E_6)=\frac{E_2E_6-E_4}{2}$$

⌟

Proof: $D(E_4)$ and $D(E_6)$ follows from(20.2.4.17) by comparing coefficients, for $D(E_2)$, differentiating the equation $E_2(\frac{a\tau+b}{c\tau+d})=(c\tau+d)^2E_2(\tau)+\frac{12}{2\pi\,\mathrm{i}}c(c\tau+d)$, we get

$$D(E_2)[\gamma]_4(z)=D(E_2)(z)+\frac{2c}{2\pi\,\mathrm{i}}\frac{E_2(\tau)}{c\tau+d}+\frac{12c^2}{(2\pi\,\mathrm{i})^2}\frac{1}{(c\tau+d)^2}.$$

Thus by(20.2.4.14), we see $D(E_2)-\frac{1}{12}E_2^2\in\mathrm{MF}_4(\Gamma(1))$, then we can compare coefficients. □

Prop. (20.2.4.19) [Structure of $\widetilde{M}_*(\Gamma)$]. Let Γ be a discrete subgroup of $\mathrm{SL}(2;\mathbb{R})$, then

- $D(\widetilde{M}_k^{\leq p}(\Gamma))\subset\widetilde{M}_{k+2}^{\leq p+1}(\Gamma)$. In particular, $D(\widetilde{M}_*(\Gamma))\subset\widetilde{M}_*(\Gamma)$.
- If $\varphi\in\widetilde{M}_2^{\leq 1}(\Gamma)$, then for any $k,p\in\mathbb{N}$, $\widetilde{M}_k^{\leq p}(\Gamma)=\bigoplus_{r=0}^{p}M_{k-2r}(\Gamma)\varphi^r$. In particular, $\widetilde{M}_*(\Gamma(1))=\mathbb{C}[E_2,E_4,E_6]$.
- If $\varphi\in\widetilde{M}_2^{\leq 1}(\Gamma)$, then for $p,k\geq 0$,

$$\widetilde{M}_k^{\leq p}(\Gamma)=\begin{cases}\bigoplus_{r=0}^{p}D^r(M_{k-2r}(\Gamma)), & p<k/2\\ \oplus_{r=0}^{k/2-1}D^r(M_{k-2r}(\Gamma))\bigoplus\mathbb{C}\cdot D^{k/2-1}\varphi, & p\geq k/2\end{cases}$$

⌟

Proof: Cf.[BGHZ]P59. □

Δ-Function and j-Function

Def. (20.2.4.20) [Discriminant Function]. The modular **discriminant function**

$$\Delta(q(\tau))=\frac{(2\pi)^{12}}{1728}(E_4^3-E_6^2)=\sum_{n\in\mathbb{Z}_+}\tau(n)q^n=(2\pi)^{12}\Big(q-24q^2+252q^3-1472q^4+4830q^5-6048q^6-16744q^7+\dots\Big)$$

by(20.2.4.6). So $\Delta(z)\in\mathrm{SF}_{12}(\Gamma(1))$, and the coefficients $\tau(n)$ are called the **Ramanujan τ-function**.
⌟

Cor. (20.2.4.21).

$$E_6^2 - E_{12} = -(1008 + \frac{24 \cdot 2730}{691})\frac{\Delta(z)}{(2\pi)^{12}}.$$

In particular, $\tau(n) \equiv \sigma_{11}(n) \mod 691$. ⌟

Proof: Consider $E_6^2 - E_{12} \in \mathrm{SF}_{12}(\Gamma(1))$, and $\mathrm{SF}_{12}(\Gamma(1))$ is 1-dimensional and generated by Δ(20.2.4.8), thus $E_6^2 - E_{12} = c\Delta$ for some constant $c \in \mathbb{C}$. By comparing the degree 1 term of both sides:

$$\frac{\Delta(z)}{(2\pi)^{12}}(q(\tau)) = \frac{1}{1728}(E_4^3(q) - E_6^2(q)) = q - 24q^2 + \ldots.$$

$$E_{12}(\tau) = 1 + \frac{24 \cdot 2730}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n, \quad E_6(z) = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n$$

by(20.2.4.6) and(20.2.4.20), so $c = -1008 - \frac{24 \cdot 2730}{691}$. Then the formula

$$691(E_6^2 - E_{12}) = 691c\Delta,$$

modulo 691 gives $\tau(n) \equiv \sigma_{11}(n) \mod 691$. □

Cor. (20.2.4.22) [*j*-Function]. By(20.2.1.18), the discriminant function $\Delta(z)$ has exactly one simple zero at ∞, thus we can define the ***j*-function** on $\mathscr{H}$ as

$$j : \mathscr{H} \to \mathbb{C}, j(q(\tau)) = 1728\frac{E_4(\tau)^3}{E_4^3(\tau) - E_6^2(\tau)} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \ldots \in \frac{1}{q} + \mathbb{Z}[[q]]$$

which is an automorphic function for $\Gamma(1)$, and it induces an isomorphism

$$j : X(1) \cong \mathbb{P}^1_{\mathbb{C}}.$$

In particular, $\mathrm{MF}^!_0(\Gamma(1)) = \mathbb{C}(j(z))$. ⌟

Proof: To show it surjects onto $\mathbb{C}$, notice it induces a holomorphic map $X(1) \cong \mathbb{P}^1 \to \mathbb{P}^1$, and it maps ∞ to ∞ with no ramification, thus it has degree 1. So it is surjective. □

Prop. (20.2.4.23).

$$\Delta(q(\tau)) = (2\pi)^{12}\eta(q(\tau))^{24} = q\prod_{n=1}^{\infty}(1 - q^n)^{24}.$$

In particular, $\Delta(\tau)$ is non-vanishing on $\tau \in \mathscr{H}$. ⌟

Proof: By(20.2.1.30), $\eta^{24}(\tau) \in \mathrm{SF}_{12}(\Gamma(1))$, which has dimension 1 and is spanned by $\Delta(\tau)$(20.2.4.8). Thus the assertion follows by comparing coefficients. □

Zeros of Eisenstein Series

Thm. (20.2.4.24) [Rankin-Swinnerton.Dyer]. If $n \in \mathbb{N}, s \in \{2, 3, 4, 5, 0, 7\}$ and $k = 6n + s \geq 2$, then the Eisenstein series $E_{2k} \in M_{2k}(\Gamma(1))$ has at least weighted zero exactly $s/12$ at i and ω(which suffices to determine its zeros), and all the other n zeros are non-elliptic and located on arc between i and ω. ⌟

Proof: Firstly, by the valence formula(20.2.1.18) and by rationality reason, E_{2k} has at least weighted zero $s/6$ at i and ω. So by valence formula, it suffices to show that E_{2k} has at least n zeros on the arc between i and ω.

Let

$$\begin{aligned}F_{2k}(\theta) &= \frac{1}{2}e^{\mathrm{i}\,k\theta}E_{2k}(e^{\mathrm{i}\,\theta})\\ &= \frac{1}{2}\sum_{(c,d)\in\mathbb{Z}^2\setminus(0,0),\gcd(c,d)=1}\frac{1}{(ce^{\mathrm{i}\,\theta/2}+de^{-\mathrm{i}\,\theta/2})^{2k}}\\ &= 2\cos(k\theta)+\frac{1}{2}\sum_{(c,d)\in\mathbb{Z}^2\setminus(0,0),c^2+d^2>1,(c,d)=1}\frac{1}{(ce^{\mathrm{i}\,\theta/2}+de^{-\mathrm{i}\,\theta/2})^{2k}}.\end{aligned}$$

Then it suffices to show that $F_{2k}(\theta)$ has at least n zeros when $\theta\in(\pi/2,2\pi/3)$. For this, we may assume $n\geq 1$. Notice for these theta,

$$|ce^{\mathrm{i}\,\theta/2}+de^{-\mathrm{i}\,\theta/2}|^2=c^2+2cd\cos\theta+d^2\geq\frac{1}{2}(c^2+d^2),$$

and for $N\in\mathbb{Z}_{\geq 5}$, the number of integral solutions to $c^2+d^2=N$ is at most $2(2\sqrt{N}+1)\leq 5\sqrt{N}$.

$$\begin{aligned}\Big|\frac{1}{2}\sum_{c^2+d^2>1,(c,d)=1}\frac{1}{(ce^{\mathrm{i}\,\theta/2}+de^{-\mathrm{i}\,\theta/2})^{2k}}\Big| &\leq 1+3^{-k}+4(\frac{5}{2})^{-k}+\sum_{N=10}^{\infty}5\sqrt{N}(\frac{N}{2})^{-k}\\ &\leq 1+3^{-k}+4(\frac{2}{5})^k+\frac{5\cdot 9^{\frac{3}{2}}}{k-\frac{3}{2}}(\frac{2}{9})^k\\ &< 1.0214\end{aligned}$$

Thus, when $m\in\mathbb{Z}$ and $k/2\leq m\leq 2/3k$, $F_{2k}(m\pi/k)$ is strictly positive or negative according as m is even or odd. So by intermediate property(3.2.10.9), there are at least $\lfloor\frac{2k}{3}\rfloor-\lceil\frac{k}{2}\rceil=n$ zeros when $\theta\in(\pi/2,2\pi/3)$. □

5 Arithmetic Modular Forms

Def. (20.2.5.1) [Modular Forms]. For $R_0\in\mathcal{CR}\mathrm{ing}$, $N\in\mathbb{Z}_+$, $k\in\mathbb{N}$, the space $M(R_0,N,k)$ of **modular forms of level N and weight k over R_0** consists of rules f that functorially associates a section $f(E/S,\alpha_N)\in\Gamma(S,\omega_{E/S}^{\otimes k})$ to each datum $(E/S,\alpha_N)$, where $S\in\mathcal{S}\mathrm{ch}/R_0$, $E\in\mathcal{E}\mathrm{ll}/S$, and $\alpha_n:E/S[n]\cong(\mathbb{Z}/(n))_S^2$ is an isomorphism.

Such a modular form is automatically meromorphic at cusps, simply because $\mathrm{Tate}(q)$ is an Elliptic curve over $\mathbb{Z}[[q]]$. ⌟

Def. (20.2.5.2)[q-Expansions and Holomorphic Modular Forms]. For $f\in M(R_0,N,k)$(20.2.5.1), if $R_0\in\mathcal{CR}\mathrm{ing}/\mathbb{Z}[\frac{1}{N},\mu_N]$, the **$q$-expansion** of f is defined to be

$$f((\mathrm{Tate}(q^N),\alpha_N)_{R_0})\in(\mathbb{Z}((q))\otimes R_0)\omega_{\mathrm{can}}.$$

where $\mathrm{Tate}(q)$ is the Tate curve, and α_N is any level N-structure on $\mathrm{Tate}(q^N)$.

For any $R_0\in\mathcal{CR}\mathrm{ing}$, $f\in M(R_0,N,k)$ is said to be **holomorphic at cusps** if the q-expansion of f restricted to $R_0[\frac{1}{N},\mu_N]$ is an element is contained in $(\mathbb{Z}[[q]]\otimes R_0)\omega_{\mathrm{can}}$ for any choice of α_N. The space of holomorphic modular forms is denoted by $S(R_0,N,k)$. ⌟

Def. (20.2.5.3) [Kodaira-Spencer Maps]. If $T \in \mathcal{S}\mathrm{ch}$, S/T is smooth, and $f : E \to S \in \mathcal{E}\mathrm{ll}/S$, then there is an exact sequence

$$0 \to f^*\Omega_{S/T} \to \Omega_{E/T} \to \Omega_{E/S} \to 0$$

thus an exact sequence

$$0 \to T_{E/S} \to T_{E/T} \to f^*T_{S/T} \to 0.$$

Thus inducing a homomorphism

$$T_{S/T} \cong f_*f^*T_{S/T} \to R^1 f_* T_{E/S} = \mathrm{Lie}(E/S)^2 R^1 f_* \Omega^1_{E/S} \cong \mathrm{Lie}(E/S)^2.$$

Thus inducing a **Kodaira-Spencer map** of $\mathcal{O}_S$-modules

$$\mathrm{KS}_{E/S} : \omega^2_{E/S} \to \Omega^1_{S/T}.$$

And if $S/T \subset \overline{S}/T, \overline{S} \setminus S = S^\infty$, $E/S \subset \overline{E}/\overline{S}$ is an extension to a curve of genus 1, and the identity $e \in E(S)$ also extends to a map $\overline{e} \in \overline{E}(\overline{S})$, with $\overline{\omega}_{\overline{E}/\overline{S}} = \overline{e}^*\Omega_{\overline{E}/\overline{S}}$ extending $\omega_{E/S}$, then the Kodaira-Spencer map extends to a map

$$\mathrm{KS}_{\overline{E}/\overline{S}} : \omega^2_{\overline{E}/\overline{S}} \to \Omega^1_{\overline{S}/T}(\log S^\infty).$$

⌟

Prop. (20.2.5.4) [Kodaira-Spencer Map for Modular Curves].

- If $T = \mathrm{Spec}\,\mathbb{Q}, S = Y(N), N \geq 3$, and E/S is the universal curve, then the Kodaira-Spencer map(20.2.5.3) is an isomorphism. And on q-expansions of modular forms along any cusp t, it is of the form
$$f(q^{1/N})(\mathrm{d}\log t)^2 \mapsto f(q^{1/N})\,\mathrm{d}\log q.$$
- If $\overline{S} = X(N)_\mathbb{Q}$, and $\overline{E^{\mathrm{uni}}}$ is the regular minimal model of the universal elliptic curve, then the extended Kodaira-Spencer map(20.2.5.3) is an isomorphism. In fact, over $\mathbb{Z}[\frac{1}{N}, \zeta_N]$ and at any cusp, the square of the canonical differential ω_{can} on $\mathrm{Tate}(q^N)$ is mapped to the $N\,\mathrm{d}\log q$.
- If $S = Y(N)^{\mathrm{ord}}$, and $T = \mathrm{Spec}\,\mathbb{Z}[\mu_N]$, then S/T is smooth by, and the Kodaira-Spencer map on the q-expansions of modular forms is of the form
$$f(q^{1/N})(\mathrm{d}\log t)^2 \mapsto f(q^{1/N})\,\mathrm{d}\log q = Nf(q^{1/N})\,\mathrm{d}\log(q^{1/N}),$$
so we can define a map $\frac{1}{N}\mathrm{KS}_{Y(N)/\mathbb{Z}[\mu_N]}$.

⌟

Proof: [Katz, p-adic properties of modular forms and modular curves]A1. Prop3.17. and Cor3.18.**?**
□

Cor. (20.2.5.5) [Modular Forms as Sections on Modular Curves]. If $N \in \mathbb{Z}_{\geq 3}$ and $R_0 \in \mathcal{CR}\mathrm{ing}/\mathbb{Z}[\frac{1}{N}]$, there are isomorphisms

$$S(R_0, N, k) \cong \Gamma(X(N), \overline{\omega}^k \otimes \Omega^1_{X(N)/\mathbb{Q}} \otimes_{\mathbb{Z}[\frac{1}{N}]} R_0) \subset \Gamma(X(N), \overline{\omega}^k \otimes_{\mathbb{Z}[\frac{1}{N}]} R_0) \cong M(R_0, N, k),$$

where the middle inclusion is given by Kodaira-Spencer isomorphism(20.2.5.4).

Thus in general, for any $\mathbb{Z}[\frac{1}{N}]$-module K, we can define a **modular form of level N and weight k with coefficients in M which is holomorphic at cusps** to be a section in

$$\Gamma(X(N), \omega^k \otimes_{\otimes\mathbb{Z}[\frac{1}{N}]} M).$$

⌟

Thm. (20.2.5.6) [q-**Expansion Principle**]. For $N \in \mathbb{Z}_{\geq 3}, M \in \mathcal{M}\mathrm{od}_{\mathbb{Z}[\frac{1}{N}]}$, and f a modular form of level N and weight k with coefficients in M which is holomorphic at cusps. Suppose on each of the $\varphi(N)$ connected components of $X(N)_{\mathbb{Z}[\frac{1}{N}]}\mathbb{Z}[\frac{1}{N}, \zeta_N]$, there exists at least one cusp that the q-expansion of f vanishes, then f vanishes. ⌟

Proof: Cf.[Kat73]P84?. □

Cor. (20.2.5.7). Situation as in(20.2.5.6), if $N \subset M \in \mathcal{M}\mathrm{od}_{\mathbb{Z}[\frac{1}{N}]}$, and on each of the $\varphi(N)$ connected components of $X(N)_{\mathbb{Z}[\frac{1}{N}]}\mathbb{Z}[\frac{1}{N}, \zeta_N]$, there exists at least one cusp that the q-expansion of f is contained in $N \otimes_{\mathbb{Z}[\frac{1}{N}]} \mathbb{Z}[\frac{1}{N}, \zeta_N] \otimes \mathbb{Z}[[q]]$, then f is a modular form with coefficients in N. ⌟

Proof: The image of f in $\Gamma(X(N), \omega^k \otimes_{\otimes \mathbb{Z}[\frac{1}{N}]} M/N)$ is trivial. □

6 Arithmetics

Prop. (20.2.6.1) [Number Field of f]. If $f \in S_k(\Gamma_1(N))$ is a normalized eigenform, then the coefficients $a_n(f)$ are algebraic integers, and generate a number field K_f, called the **number field of** f. ⌟

Proof: Cf.[Diamond, P238]. □

Prop. (20.2.6.2). if $f \in \mathrm{SF}_2(N, \chi)$ is a normalized eigenform, then for any $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, f^σ is also a normalized eigenform in $\mathrm{SF}_2(N, \chi^\sigma)$, where $\chi^\sigma(n) = \chi(n)^\sigma$. And if f is a newform, then so is f^σ. ⌟

Proof: Cf.[Diamond, P239].? □

Cor. (20.2.6.3) [Integrality of Modular Forms]. $S_2(\Gamma_1(N))$ has a basis of modular forms with integral coefficients. ⌟

Proof: Let $f \in S_2(\Gamma_1(N))$ be a newform of level $M|N$, and K_f the number field of f. Let $\alpha_1, \ldots, \alpha_d$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$, and $\Sigma^\infty = \{\sigma_1, \ldots, \sigma_d\}$ the set of embeddings of K into $\mathbb{C}$. Let

$$g_i = \sum_{j=1}^{d} \sigma_j(\alpha_i) f^{\sigma_j},$$

then by linear independence of characters, the matrix $(\sigma_i(\alpha_j))$ is non-degenerate, so $\mathrm{span}\{g_1, \ldots, g_d\} = \mathrm{span}\{f, \ldots, f^{\sigma_d}\}$, and $g_i \in S_2(\Gamma_1(N))$ by(20.2.6.2). Then by(20.2.2.13), applying this for all old and new forms of $S_2(\Gamma_1(N))$, the assertion follows. □

Prop. (20.2.6.4)[Integral Modular Forms]. If $A \subset \mathbb{C}$ be a subring, denote $M_k(\Gamma, A) = M_k(\Gamma) \cap A[[q]]$ ⌟

7 Modular Forms Mod p

Def. (20.2.7.1) [Modular Forms Mod p]. Define $\mathrm{MF}_k(\Gamma, \mathbb{F}_p) = M_k(\Gamma, \mathbb{Z}) \otimes \mathbb{F}_p$, called the space of **modular forms mod p of weight k.** ⌟

Prop. (20.2.7.2) [Serre's Equality]. There is an isomorphism $M_{p+1}(SL(2, \mathbb{Z}), \mathbb{F}_p) \cong M_2(\Gamma_0(p), \mathbb{F}_p)$ ⌟

Proof: Because $E_k(z)1-\frac{2k}{B_k}\sum_{n=1}^\infty\sigma_{k-1}(n)q^n$, and by Kummer's congruence(22.3.1.1) $\mathrm{ord}_p(B_{p-1})=-1$, thus $E_{p-1}\mod 1\mod p$. Then multiplying by $E_{p-1}:M_2(\Gamma_0(p),\mathbb{F}_p)\to M_{p+1}(\Gamma_0(p),\mathbb{F}_p)$ raises the level by $p-1$. Then we compose with the natural averaging map $M_{p+1}(\Gamma_0(p),\mathbb{F}_p)\to M_{p+1}(SL(2,\mathbb{Z}),\mathbb{F}_p)$, which is dual to the natural inclusion $M_{p+1}(SL(2,\mathbb{Z}),\mathbb{F}_p)\to M_{p+1}(\Gamma_0(p),\mathbb{F}_p)$.

Why isomorphism.? □

8 Non-Congruent Modular Forms

Cf.[Non-Congruuent Modular Forms, Ling Long].

Thm. (20.2.8.1) [Unbounded Denominators Conjecture]. Let N be any positive integer and let $f(\tau)\in\mathbb{Z}[[q^{1/N}]]$ for $q=e^{\pi\,\mathrm{i}\,\tau}$ be a holomorphic function on the upper half plane. Suppose there exists an integer k and a finite index $\Gamma\subset SL(2,\mathbb{Z})$ that f is Γ-invariant, and f is meromorphic at the cusps of Γ, then $f(\tau)$ is a modular form for some congruent subgroup of $\mathrm{SL}(2,\mathbb{Z})$. ⌟

Proof: Cf.[the Unbounded Denominator Conjecture]. □

3

20.3 Hilbert and Siegel Modular Forms

20.4 Theta Correspondence

1 Theta Functions

Def. (20.4.1.1) [Poisson Summation for Lattices]. Let V be a vector space of dimension n with an Haar measure μ, $\Gamma \subset V$ a full lattice, and $\Gamma' \subset V^\vee$ be its $\mathbb{Z}$-dual, Let $V = \mu(V/\Gamma)$, then for any Schwartz function $f \in \mathcal{S}(V)$,

$$\sum_{x\in\Gamma} f(x) = \frac{1}{V}\sum_{y\in\Gamma'} \widehat{f}(y).$$

⌟

Proof: This is just**??**. □

Def. (20.4.1.2) [Quadratic Lattices]. Let V be a real inner product space with an Haar measure μ normalized that for an orthonormal basis e_i of V, $V/\mathbb{Z}\{e_i\}$ has volume 1, then we can identify V with V^* by this inner product. Let Γ be a full lattice, then its $\mathbb{Z}$-dual Γ^D is defined to be the lattice $V^D = \{y \in V | (x, y) \in \mathbb{Z}, \forall x \in \Gamma\}$. the **level of** Γ is defined to be the minimal $N \in \mathbb{Z}_+$ s.t. $NV^D \subset V$. It is called a **unimodular lattice** if $\mathrm{Vol}(V/\Gamma) = 1$. ⌟

Def. (20.4.1.3) [Theta Functions]. Situation as in(20.4.1.2), for any $x_0 \in \Gamma$, we can define **theta functions**

$$\theta_{\Gamma,x_0} : \mathscr{H} \times \mathbb{C} \to \mathbb{C} : \theta_{\Gamma,x_0}(\tau, z) = \sum_{x\in\Gamma} e^{-\pi\,\mathrm{i}[(x,x)\tau+(x,x_0)z]}.$$

and

$$\theta_\Gamma(\tau) = \theta_{\Gamma,0}(\tau, 0), \quad \Theta_\Gamma(t) = \theta_\Gamma(\mathrm{i}\, t) = \sum_{x\in\Gamma} e^{-\pi t(x,x)}.$$

⌟

Cor. (20.4.1.4). With the notation as in(20.4.1.3), the theta function satisfies

$$\Theta_\Gamma(t) = \frac{t^{-n/2}}{\mu(V/\Gamma)}\Theta_{\Gamma^D}(t^{-1})$$

⌟

Proof: Notice that $\Theta_{s\Gamma}(t) = \Theta_\Gamma(s^2 t)$, so this formula follows from(20.4.1.1) applied to $t^{-1/2}\Gamma$ and $f(x) = e^{-\pi(x,x)}$. □

Thm. (20.4.1.5) [Hecke-Schoenberg]. Given $k \in \mathbb{Z}_+$ and a lattice Γ of rank k, level N and discriminant Δ, then

$$\theta_\Gamma(\tau) \in \mathrm{MF}_k(\Gamma_0(N), \left(\frac{\Delta}{-}\right)).$$

⌟

Proof: □

Def. (20.4.1.6) [Simple Theta Function]. The simple theta function θ is defined to be

$$\theta(\tau) = \sum_{n\in\mathbb{Z}} e^{2\pi\,\mathrm{i}\, n^2\tau}.$$

Then by(20.4.1.4) it satisfies

$$\theta(\tau + 1) = \theta(\tau), \quad \theta(-\frac{1}{4\tau}) = \sqrt{-2\,\mathrm{i}\,\tau}\theta(\tau).$$

⌟

Self-Dual Lattices

Def. (20.4.1.7) [Self-Dual Lattices]. Situation as in(20.4.1.3), a **self-dual lattice** is a lattice Γ in V that $V^D = V$. Equivalently, if $\{f_i\}$ is a $\mathbb{Z}$-basis of Γ, then the matrix $A = ((e_i, e_j))_{i,j}$ is a matrix with integer coefficients and determinant 1. The last equivalence is because $\Gamma' \subset \Gamma$ equals Γ if $\mu(V/\Gamma) = \mu(V/\Gamma')$, but this is equivalent to $\mu(V/\Gamma) = 1$, because $\mu(V/\Gamma) \cdot \mu(V/\Gamma') = 1$.

A self-dual lattice is called **even lattice** iff $(x, x) \in 2\mathbb{Z}$ for any $x \in \Gamma$. ⌟

Example (20.4.1.8) [E_{8k}]. Let $V = \mathbb{R}^{8k}$ with the canonical inner product, denote E_{8k} the set of vectors $\sum_i x_i e_i$ in V that

$$2x_i \in \mathbb{Z}, x_i - x_j \in \mathbb{Z}, \sum_{i=1}^{8k} x_i \in 2\mathbb{Z}.$$

Notice E_8 is compatible with the root system E_8(3.9.3.2), and the root system just consists of all vectors in E_8 of length $\sqrt{2}$.

Then E_{8k} is a self-dual and even. ⌟

Cor. (20.4.1.9). Let $k \geq 2$, then all the vectors in E_{8k} of length $\sqrt{2}$ are $\{\pm e_i \pm e_j | i \neq j\}$. ⌟

Remark (20.4.1.10). For more examples of self-dual lattices, see[Ser73]Chap5. ⌟

Prop. (20.4.1.11) [Theta Function for Self-Dual Even Lattices]. Let $\Gamma \subset V$ be a self-dual even lattice(20.4.1.7), then the dimension n of V is divisible by 8, and the theta function $\theta_\Gamma(z) \in M_{n/2}(\Gamma(1))$. ⌟

Proof: We first show that

$$\theta_\Gamma(-1/z) = (-\mathrm{i}\, z)^{n/2} \theta_\Gamma(z)$$

and because both sides are holomorphic functions on $\mathcal{H}$, it suffices to show this for $z = it, t > 0$. Thus it suffices to show

$$\Theta_\Gamma(t^{-1}) = t^{-n/2} \Theta_\Gamma(t).$$

And this is just(20.4.1.4), because Γ is self-dual(20.4.1.7).

Then $\theta_\Gamma[ST]_{n/2} = (-\mathrm{i})^{n/2} \theta_\Gamma$(20.2.1.10), but $(ST)^3 = 1$, so $(-\mathrm{i})^{3n/2} = 1$, so $8|n$, and $\theta_\Gamma \in M_{n/2}(\Gamma(1))$. □

Thm. (20.4.1.12) [Siegel's Mass Formula]. Cf.[Chao Li]. ⌟

Prop. (20.4.1.13) [Theta Function for Non-Even Self-Dual Lattices]. If we consider theta function for non-even self-dual lattices in $\mathbb{R}^n$, then we get a modular form of weight $n/2$ w.r.t. the subgroup of $\mathrm{SL}(2, \mathbb{Z})$ generated by the elements S and T^2. This image of this subgroup has index 3 in $\mathrm{PSL}(2, \mathbb{Z})$, and it has two cusps, thus two Eisenstein series.

In particular, we can apply this to the lattice $\{e_i\}$, and use this information to obtain formula giving the number of ways to represent an integer into a sum of n squares. ⌟

Proof: □

Twisted Theta Functions

2 Jacobi Forms

Cf.[Jacobi Forms, Zagier].

Def. (20.4.2.1)[Jacobi Forms]. A **Jacobi form** for $\mathrm{SL}(2,\mathbb{Z})$ is a holomorphic function $\varphi:\mathscr{H}\times\mathbb{C}\to\mathbb{C}$ s.t.

- For any $\begin{bmatrix}a & b\\ c & d\end{bmatrix}\in\mathrm{SL}(2,\mathbb{Z})$,

$$\varphi(\frac{a\tau+b}{c\tau+d},\frac{z}{c\tau+d})=(c\tau+d)^k e^{2\pi\mathrm{i}\,\frac{mcz}{c\tau+d}}\varphi(\tau,z).$$

- For any

⌟

Prop. (20.4.2.2). The theta functions $\theta_{\Gamma,x_0}(\tau,z)$ defined in(20.4.1.3) is a Jacobi form of weight rank $\Gamma/2$ and index (x_0,x_0). ⌟

3 Theta Lifts

References are [Borcherds] and [Borcherds Products on 0(2, l) and Chern Classes of Heegner Divisors].

20.5 Adelic Automorphic Representations

Main references are [Bum98], [Gan07], [G-H11], [Borel, Casselman, Automorphic forms, representations and L-function (Corvallis)], [Automorphic Forms on GL(2), Jacquet and Langlands(1970)]. [Introduction to Langlands Program, Cogdell].

Notation (20.5.0.1).

- Use notations defined in Adeles and Ideles.
- Use notations defined in Admissible Representations of $\mathrm{GL}(n)$ over p-Adic Number Fields.
- Use notations defined in Arithmetic of Algebraic Groups.
- Use notations defined in Automorphic Representations over Archimedean Local Fields.
- Fix a global field F and let $\mathbf{A} = \mathbf{A}_F$.
- Fix a linear algebraic group $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}\,/F$ with center Z.
- Fix a central character $\omega : Z(\mathbf{A}_F)/Z(F) \to \mathbb{C}^\times$. Notice if $G = \mathrm{GL}(2)$, ω is just a Hecke character.

⌟

Def. (20.5.0.2) [Lie Algebra]. Let $\mathfrak{g}_\infty = \mathrm{Lie}(G(\mathbf{A}_\infty))$ be the Lie algebra of $G(\mathbf{A})$, $\mathcal{Z} = Z(U(\mathfrak{g}_\infty))$. ⌟

Notation (20.5.0.3) [Group-Theoretic Notations].

- If $G = \mathrm{GL}(n)$, B is the Borel subgroup of upper triangular matrices, $\mathrm{Unip}(n)$ is the subgroup of upper triangle unipotent matrices.
- M_n is the **mirabolic subgroup** of B with $a_{n,n} = 1$, which is isomorphic to $\mathrm{GL}(n-1) \ltimes \mathbb{A}^n$.
- T the group of diagonal matrices. T_1 is the subgroup of T that $a_{nn} = 1$.
- Denote w^0 the matrix$= \sum_{i=1}^n e_{i,n-i}$.
- If $n = 2$, denote $w_0 = \begin{bmatrix} & -1 \\ 1 & \end{bmatrix}, w_1 = \begin{bmatrix} & 1 \\ -1 & \end{bmatrix}$,
$$t(y) = \begin{bmatrix} y & \\ & y^{-1} \end{bmatrix}, \quad n(z) = \begin{bmatrix} 1 & z \\ & 1 \end{bmatrix} \quad y \in F^*, z \in F.$$
following5.

⌟

Def. (20.5.0.4). For $\alpha \in F^{n-1}$, let $\psi_{N,\alpha}$ be a character of $N(F)$ given by $\psi_N(g) = \sum_i \psi(\alpha_i g_{i,i+1})$. For $\alpha = (1, \ldots, 1)$, denote $\psi_{N,\alpha}$ by ψ_N. ⌟

Def. (20.5.0.5) [Global Norm]. Take an embedding $G \hookrightarrow \mathrm{GL}(n)$ over F. Define the norm on $G(\mathbf{A}_F)$ by
$$||g|| = \prod_v \max(|g_{ij}|_v, |g_{ij}^{-1}|_v).$$
Notice in non-Archimedean places $||g||_v = 1$ for $g \in GL(m, \mathcal{O}_v)$, so it is definable. ⌟

Remark (20.5.0.6) [Delete]. The reason to formulate automorphic forms in the Adelic setting:

1: we want a theory that deals with $\mathcal{A}(G, \Gamma)$ for all choices of Γ simultaneously.

2: we want a framework in which the roles of the $(\mathfrak{g}, K)$-action and the $\mathcal{H}(G, \Gamma)$-action are parallel, i.e. so that they are actions of the same kind.

3: To describe the process of attaching an L-function to a classical modular form in terms of representation theory, it is cleanest to use the adelic framework, as demonstrated in Tate's thesis.

4: The questions about the absolute Galois group $\mathrm{Gal}_{\mathbb{Q}}$, like what finite groups are quotients of $\mathrm{Gal}_{\mathbb{Q}}$, or where there extensions of $\mathbb{Q}$ with given ramification conditions, can be understood via automorphic forms. And automorphic forms can be understood via Langlands dual groups. ⌟

1 Automorphic Representations

Admissible Representations and Tensor Product Theorem

Def. (20.5.1.1) [Admissible Representations]. A **smooth representation** of $G(\mathbf{A}_F)$ is defined to be a commuting smooth $G(A_f)$-action and a $(\mathfrak{g}_\infty, K_\infty)$-module structure(15.4.3.5). The category of smooth representations of $G(\mathbf{A}_F)$ is denoted by $\mathrm{Rep}^{\mathrm{alg}}(G/F)$.

Any $(\pi, V) \in \mathrm{Rep}^{\mathrm{alg}}(G(\mathbf{A}_F))$ induces a representation of $K = K_f \times K_\infty$. Then this representation is called an **admissible representation** iff every vector is K-finite, and for any irreducible representation ρ of K, $\dim V^\rho < \infty$. By(18.1.5.25), it can be checked that this is equivalent to: for any irreducible representation ρ_∞ of K_∞ and an open compact subgroup $U \subset K_f$, $\dim V^{\rho_\infty} \cap V^U < \infty$. The category of admissible representations of $G(\mathbf{A}_F)$ is denoted by $\mathrm{Rep}^{\mathrm{adm}}(G/F)$. ⌟

Def. (20.5.1.2) [Restricted Tensor Representation]. Given a set of locally compact groups G_v and a.e. their compact subgroups K_v, $(\rho_v, V_v) \in \mathrm{Rep}^{\mathrm{alg}}(G_v), \xi_v^0 \in V_v^{K_v}$ are given for a.e. v, then we can define the **restricted tensor representation**

$$(\rho, V) = \bigotimes_v{}' (\rho_v, V_v, \xi_v^0)$$

of $G(\mathbf{A}_F) = \prod'(G_v, K_v)$ on $\otimes_v' V_v$ by

$$\rho(\otimes_v g_v)(\otimes_v \xi_v) = \otimes_v \rho_v(g_v)\xi_v.$$

⌟

Def. (20.5.1.3) [Global Hecke Algebra]. For $v \in \Sigma_F$, let $\mathcal{H}_{G(F_v)}$ be the Hecke algebras constructed in(18.1.5.12) and(18.9.4.11). As $\mathcal{H}_{G(F_v)}$ has a spherical idempotent $e_v^0 = e_{K_v}$(20.5.1.1), we can define the **global Hecke algebra**

$$\mathcal{H}_{G(\mathbf{A}_F)} = \bigotimes_v{}' (\mathcal{H}_{G(F_v)}, e_v^0).$$

Then by definition of representations in(20.5.1.12) and(18.9.4.12)(18.1.5.16),

$$\mathrm{Rep}^{\mathrm{alg}}(G(\mathbf{A}_F)) = \mathrm{Rep}^{\mathrm{alg}}(\mathcal{H}_{G(\mathbf{A}_F)}).$$

⌟

Thm. (20.5.1.4) [Tensor Product Theorem, Flath]. For $(\rho, V) \in \mathrm{Irr}^{\mathrm{adm}}(G/F)$, there exists uniquely for each $v \in \Sigma_F^\infty$ a $(\rho_v, V_v) \in \mathrm{Irr}^{\mathrm{adm}}((\mathfrak{g}_\infty, K_v))$, and for each $v \in \Sigma_F^{\mathrm{fin}}$ a $(\pi_v, V_v) \in \mathrm{Irr}^{\mathrm{alg}}(G(F_v))$ s.t. for a.e. v, V_v contains a non-zero K_v-fixed vector ξ_v^0, and

$$(\rho, V) = \bigotimes{}' (\rho_v, V_v, \xi_v^0).$$

Conversely, any such a restricted tensor product is in $\mathrm{Irr}^{\mathrm{adm}}(G/F)$. ⌟

Proof: By considering the global Hecke algebra, this follows immediately from(20.5.1.3) and(18.9.4.12)(18.1.5.16) □

Cor. (20.5.1.5)[Contragradient Representations]. For any $\rho = \otimes_v \rho_v \in \mathrm{Irr}^{\mathrm{adm}}(G/F)$, we can define the **contragradient** of ρ as $\widehat{\rho} = \otimes_v \widehat{\rho_v}$(18.1.2.7) $\in \mathrm{Irr}^{\mathrm{adm}}(G/F)$. ⌟

Cor. (20.5.1.6)[Irreducible Representations of K].

$$\mathrm{Irr}(K) = \bigotimes_v{}' \mathrm{Irr}(K_v).$$

⌟

Proof: This is similar to the proof of(20.5.1.4). □

Automorphic Representations

Def. (20.5.1.7) [L^2-Space]. Define $L^2(G/F, \omega)$ the space of all measurable functions φ on $G(A)$ that satisfies

$$\varphi(zg) = \omega(z)\varphi(g), \forall z \in Z(A), \quad \varphi(\gamma g) = \varphi(g), \forall \gamma \in G(F)$$

and square integrable module the center:

$$\int_{Z(A)G(F)\backslash G(A)} |\varphi(g)|^2 dg < \infty.$$

Then the right action of $G(A)$ on $L^2(G(F)\backslash G(A), \omega)$ is continuous, by(11.10.2.9). ⌟

Def. (20.5.1.8) [Cuspidality]. A function $\varphi \in L^2(G(F)\backslash G(\mathbf{A}_F), \omega)$ is called **cuspidal** iff for any proper parabolic subgroup $P = MU$, where U is the unipotent radical,

$$\int_{U(F)\backslash U(\mathbf{A}_F)} \varphi(ng)dn = 0$$

a.e. $g \in G(\mathbf{A}_F)$. The closed space of all cuspidal elements in $L^2(G(F)\backslash G(\mathbf{A}_F), \omega)$ is denoted by $L^2_0(G(F)\backslash G(A), \omega)$. $L^2_0(G(F)\backslash G(A), \omega)$ is stable under the right action of $G(A)$.

Thus a function $\varphi \in L^2(GL(n, F)\backslash GL(n, \mathbf{A}_F), \omega)$ is cuspidal iff

$$\int_{M_{r\times s}(F)\backslash M_{r\times s}(A)} \varphi(\begin{bmatrix} I_r & X \\ & I_s \end{bmatrix} g)dX = 0$$

a.e. g for any $r + s = n, 1 < r < n$, as these are the maximal proper parabolic subgroups of $\mathrm{GL}(n)$. ⌟

Def. (20.5.1.9)[Smooth Functions on $G(\mathbf{A}_F)$].

- The space $C^\infty(G(\mathbf{A}_F))$ of **smooth functions on** $G(\mathbf{A}_F)$ is defined to be the restricted tensor product $\bigotimes' C^\infty(G_v)$ w.r.t. $f_{v,0} = \chi_{\mathscr{K}_v}$.
- The space $C_c^\infty(G(\mathbf{A}_F))$ of **compactly supported smooth functions on** $G(\mathbf{A}_F)$ is defined to be the restricted tensor product $\bigotimes' C_c^\infty(G_v)$ w.r.t. $f_{v,0} = \chi_{K_v}$. $C_c^\infty(G(A))$ acts on $L^2(G(F)\backslash G(\mathbf{A}_F), \omega)$.

- $G(\mathbf{A}_F)$ acts on $C^\infty(G(\mathbf{A}_F))$ by right translation, and induces an action of $\mathfrak{g}_\infty$ thus an action of $U(\mathfrak{g}_\infty)$ on it. A function f is called $\mathcal{Z}$-finite if it is contained in a f.d. space that is invariant under the action of $\mathcal{Z}$.
- A **K-finite function** $f \in C^\infty(G(\mathbf{A}_F))$ is a vector that is contained in a f.d. space that is right-invariant under K. Equivalently, it is $\mathcal{K}_\infty$-finite and is right-invariant under an open compact subgroup of $G(A_f)$.
- A function $f \in C^\infty(G(\mathbf{A}_F))$ is said to **have moderate growth** iff $|f(g)| \le C||g||^N$(20.5.0.1) for some constant $C > 0$ and any $g \in G(\mathbf{A}_F)$.
- A function $f \in C^\infty(G(\mathbf{A}_F))$ is said to be **rapidly decreasing** if for any $k \in \mathbb{Z}_+$, $|f(g)| \le C_k||g||^{-k}$ for any $g \in G(\mathbf{A}_F)$ and some constant C_k.

⌟

Def. (20.5.1.10) [Adelic Automorphic Forms]. We denote by $\mathcal{A}(G/F,\omega)$ the space of **adelic automorphic forms** consisting of smooth functions on $G(\mathbf{A}_F)$(20.5.1.9) that satisfies

- $\varphi(zg) = \omega(z)\varphi(g), \forall z \in Z(A), \quad \varphi(\gamma g) = \varphi(g), \forall \gamma \in G(F)$.
- K-finite and $\mathcal{Z}$-finite(20.5.1.9).
- of moderate growth(20.5.1.9).

And the space $\mathcal{A}_0(G/F,\omega)$ of **cusp forms** the automorphic forms that is cuspidal in sense of(20.5.1.8). $\mathcal{A}(G/F,\omega)$ is a $(\mathfrak{g}_\infty, K_\infty)$-module, and $G(A_F^f)$ acts smoothly on it. The subspace $\mathcal{A}_0(G/F,\omega)$ is stable under both actions. ⌟

Prop. (20.5.1.11) [Analytic Properties]. Any automorphic form f is real analytic when restricted to $G(\mathbf{A}_\infty)$, and is of moderate growth.

Any cusp form f is rapidly decreasing. In particular, $f \in L^2_0(G/F)$ if G is semisimple. ⌟

Proof: It is real analytic by(20.1.1.29). The growth condition reduces immediately to the Archimedean case(20.1.3.7). □

Def. (20.5.1.12) [Automorphic Representations]. $\mathcal{A}(G/F,\omega)$ and $\mathcal{A}_0(G/F,\omega)$ afford smooth representations of $GL(n,A)$ by definition(20.5.1.10). So we define an **automorphic representation** to be an irreducible smooth representation of $G(A)$ that can be realized as a quotient of a subrepresentation of $\mathcal{A}(G/F,\omega)$, and an **automorphic cuspidal representation** to be an irreducible smooth representation of $G(\mathbf{A}_F)$ that can be realized as a subrepresentation of $\mathcal{A}_0(G(F)\backslash G(\mathbf{A}),\omega)$. The category of automorphic representations of $G(\mathbf{A}_F)$ is denoted by $\mathrm{Irr}^{\mathrm{auto}}(G/F,\omega)$. The category of cuspidal representations of $G(\mathbf{A}_F)$ is denoted by $\mathrm{Irr}^{\mathrm{cusp}}(G/F,\omega)$. ⌟

Remark (20.5.1.13). There is a general method of constructing subrepresnetations of $\mathcal{A}(G(F)\backslash G(A),\omega)$ using Eisenstein series**?**, but no known methods for constructing subrepresnetations of $\mathcal{A}_0(G(F)\backslash G(A),\omega)$. ⌟

Thm. (20.5.1.14) [Automorphic Representations are Admissible, Harish-Chandra].

$$\mathrm{Irr}^{\mathrm{cusp}}(G/F,\omega) \subset \mathrm{Irr}^{\mathrm{auto}}(G/F,\omega) \subset \mathrm{Irr}^{\mathrm{adm}}(G/F).$$

⌟

Proof: Le $V_1 \subset V_2 \subset \mathcal{A}(G(F)\backslash G(A),\omega)$ be submodules s.t $V_2/V_1 \cong \pi$, then we can assume V_2 is generated by an element $f \in V_2\backslash V_1$, because otherwise change V_2 by the submodule V_2' generated by f and V_1 by $V_1 \cap V_2'$.

f is killed by an ideal J_∞ of finite codimension in $\mathcal{Z}_\infty$, and is invariant under the action of a compact open subset $U \subset G(\mathbf{A}_F^f)$. Let

$$G(F)\backslash G(A)/U = \coprod_i \Gamma_i\backslash G(A_\infty)$$

as in(15.4.3.13), then there is an isomorphism of $(\mathfrak{g}_\infty, K_\infty)$-modules

$$\mathcal{A}(G(F)\backslash G(A),\omega,J_\infty)^U \cong \oplus_i \mathcal{A}(\Gamma_i\backslash G(A_\infty),1,\omega_\infty,J_\infty)(20.1.4.10),$$

which is admissible by the fundamental theorem of Harish-Chandra(20.1.4.10). Thus $V_2 \subset \mathcal{A}(G(F)\backslash G(A),\omega,J)^U$ is also admissible. □

2 $\mathrm{Irr}^{\mathrm{auto}}(\mathrm{GL}(n)/F)$

Main references are [Bum98]Chap3.

Basics

Prop. (20.5.2.1). $GL(n,\mathbf{A}_F)$ is unimodular. ⌟

Proof: This is because $GL(n,F_v)$ is unimodular for any $v \in \Sigma_F$ and because we can calculate the restricted product measure by(14.4.4.5). □

Def. (20.5.2.2) [Congruence Subgroups]. For $N \in \mathbb{Z}_+$, define the congruence subgroup(15.4.2.3) $\mathcal{K}_0(N) \subset GL(2,\mathbf{A}_F^f)$ as follows: $\mathcal{K}_0(N) = \prod_{v\in\Sigma_F^{\mathrm{fin}}} \mathcal{K}_0(N)_v$, where

$$\mathcal{K}_0(N)_v = \begin{cases} GL(2,\mathcal{O}_v) & v \nmid N \\ \mathcal{K}_0(N_v) \subset F_v(18.11.1.8) & v | N \end{cases}$$

⌟

Prop. (20.5.2.3). If $F = \mathbb{Q}$, then the inclusion induces homeomorphisms

$$\Gamma_0(N)\backslash GL(2,\mathbb{R})^+ \cong GL(2,\mathbb{Q})\backslash GL(2,A)/K_0(N).$$

$$\Gamma_0(N)\backslash SL(2,\mathbb{R}) \cong GL(2,\mathbb{Q})Z(A)\backslash GL(2,A)/K_0(N)$$

Thus the definition of congruence subgroups(20.2.1.3) are compatible with that of(15.4.3.13) ⌟

Proof: Because $\mathrm{Cl}(\mathbb{Q}) = 1$ and $\det(\mathcal{K}_0(N)) = \prod_{v\in\Sigma_F^{\mathrm{fin}}} \mathcal{O}_v^*$, item3 of(15.4.3.12) shows

$$GL(2,A) = GL(2,\mathbb{Q})GL(2,\mathbb{R})K_0(N) = GL(2,\mathbb{Q})GL(2,\mathbb{R})^+K_0(N),$$

so the map

$$GL(2,\mathbb{R})^+ \to GL(2,\mathbb{Q})\backslash GL(2,A)/K_0(N)$$

is surjective. Now if g_∞' and g_∞ has the same image, then $g_\infty' = \gamma g_\infty k_0$, so $g_\infty' = \gamma_\infty g_\infty, \gamma_f = k_0^{-1}$. Then γ_∞ belongs to $\Gamma_0(N)$. Thus there is a bijection

$$\Gamma_0(N)\backslash GL(2,\mathbb{R})^+ \cong GL(2,\mathbb{Q})\backslash GL(2,A)/K_0(N).$$

2 follows from 1 by modulo the center. □

Cor. (20.5.2.4). The quotient space $GL(n,F)Z(A)\backslash GL(n,A)$ has finite measure. ⌟

Proof: For the general case, Cf.[Humphreys, Arithmetic Groups, (1980)?].

Because $K_0(N)$ is compact, it suffices to prove that $GL(n,F)Z(A)\backslash GL(n,A)/K_0(N)$ has finite measure(because $GL(n,F)$ and $GL(n,A)$ are both unimodular, the measure is compatible). But this space is homeomorphic to $\Gamma_0(N)\backslash SL(2,\mathbb{R})$, which has finite measure because $\Gamma(1)\backslash SL(2,\mathbb{R})$ does and $\Gamma_0(N)$ is of finite index in $\Gamma(1)$. □

Def. (20.5.2.5) [Global Siegel Sets]. For $c,d>0$, then the global Siegel set $\mathfrak{S}_{c,d}=K_f\times\mathfrak{S}_{c,d,\infty}$??. And denote $\overline{\mathfrak{S}_{c,d}}$ its image in $Z(A)\backslash GL(2,A)$. ⌟

Prop. (20.5.2.6). For c,d suitable chosen, $GL(2,A)=GL(2,F)\mathfrak{S}_{c,d}$. ⌟

Proof: We prove only for $F=\mathbb{Q}$?: This is true for $c\leq\sqrt{3}/2$ and $d\geq 1$ because of the shape of the fundamental domain of $GL(2,\mathbb{R})$ for $SL(2,\mathbb{Z})$(20.2.1.10). □

Prop. (20.5.2.7) [Contragradient Representations]. For $(\pi,V)\in\mathrm{Irr}^{\mathrm{adm}\,/\,\mathrm{cusp}}(\mathrm{GL}(n)/F,\omega)$,

- its contragradient $(\widehat{\pi},\widehat{V})\in\mathrm{Irr}^{\mathrm{adm}\,/\,\mathrm{cusp}}(\mathrm{GL}(n)/F,\omega^{-1})$, and $\widehat{V}$ can be chosen to be the space of all functions $g\mapsto\varphi(g^{-t})$.
- if $n=2$, then $\widehat{\pi}\cong\pi\otimes(\omega^{-1}\circ\det)$.

⌟

Proof: It suffices to analyze each place. Notice for cuspidal representations, it suffices to show for finite places, because we can use strong multiplicity one(20.5.3.8).

For admissible case we only prove for $n=2$ and F totally real(the problem is we haven't studied $\mathbb{C}$).?

Let $\widehat{V}$ be the space of functions of the form $\widehat{\varphi}(g)=\varphi(g^{-t})$, then the right action of G on $\widehat{V}$ corresponds back to the restriction of the right action composed with the automorphism $g\mapsto g^{-t}$. Thus the result follows from(18.11.1.15) and its Archimedean analogy for $(\mathfrak{g}_\infty,K_\infty)$-modules(18.9.3.35). □

Spectral Problem

Prop. (20.5.2.8) [Gelfand, Graev and Piatetski-Shapiro]. Let $\varphi\in C_c^\infty(GL(n,A))$, then

- There exists a constant $C(\varphi)$ that for all $f\in L_0^2(GL(n,F)\backslash GL(n,A),\omega)$, we have $||\rho(\varphi)f||_{C(G)}\leq C(\varphi)||f||_2$.
- $\rho(\varphi)$ is a compact operator on $L_0^2(GL(n,F)\backslash GL(n,A),\omega)$.

⌟

Proof: The proof is the same as that of(20.1.4.6), but use global Siegel sets(20.5.2.5), Cf.[Bump, P297]?. □

Cor. (20.5.2.9) [$L_0^2(GL(n,F)\backslash GL(n,A),\omega)$ Totally Decomposable]. The space $L_0^2(GL(n,F)\backslash GL(n,A),\omega)$ decomposes into a Hilbert space direct sum of irreducible invariant subspaces over $GL(n,A)$. ⌟

Proof: The proof is exactly the same as(20.1.4.2), but where we use(20.5.2.8) in place of(20.8.2.1) and lemma?? in place of lemma(18.9.4.1). □

Prop. (20.5.2.10) [Irreducible Cuspidal Representations Admissible]. If $(\pi, V) \in \mathrm{Irr}^{\mathrm{uni}}(GL(n,A))$ is contained in the decomposition of $\mathcal{H} = L_0^2(GL(n,F)\backslash GL(n,A),\omega)$ in(20.5.2.9), then $V^{K-\mathrm{fin}} \subset V$ is dense, $V^{K-\mathrm{fin}} \subset \mathcal{A}_0(GL(n,F)\backslash GL(n,A),\omega) \in \mathrm{Rep}^{\mathrm{alg}}(\mathrm{GL}(n)/F,\omega)$.

In particular,

$$\mathcal{A}_0(GL(n,F)\backslash GL(n,A),\omega) \subset L_0^2(GL(n,F)\backslash GL(n,A),\omega),$$

and

$$\mathcal{A}_0(GL(n,F)\backslash GL(n,A),\omega) = \bigotimes_{\pi\in\mathrm{Irr}^{\mathrm{cusp}}(\mathrm{GL}(n)/F,\omega)} m_\pi \pi$$

by(20.5.1.11) and(20.5.2.9). ⌟

Proof: This is general by(18.9.4.4), and for the containment in $\mathcal{A}_0$ by a similar argument as in(20.1.4.8) using a similar lemma as lemma(20.1.4.7).

The irreducible smooth $GL(n,A)$-representations are admissible by(20.5.1.14). □

Adelization

Prop. (20.5.2.11) [Global Hecke Algebra]. There are isomorphisms

$$\Gamma_0(N)\backslash G_0(N)/\Gamma_0(N)(20.2.1.6) \cong \prod_{v\in\mathbf{P}\backslash S_f(N)}' K_v\backslash GL(2,\mathbb{Q}_v)/K_v.$$

$$\Gamma_0(N)\backslash G_0(N) \cong \prod_{v\in\mathbf{P}\backslash S_f(N)}' K_v\backslash GL(2,\mathbb{Q}_v)$$

which induces an isomorphism $\mathcal{R}_N \cong \prod_{v\in\mathbf{P}\backslash S_f(N)} \mathcal{H}_{K_v}$ (20.2.2.2)(18.11.1.13). ⌟

Prop. (20.5.2.12) [Adelization of Maass Forms]. Let χ be a Dirichlet character (mod N) and ω be the adelized Hecke character of χ(14.4.4.32), then define a character λ_d of $K_0(N)$(20.5.2.2) by

$$\lambda_d(\begin{bmatrix} a & b \\ c & d\end{bmatrix}) = \prod_{v\in S_f(N)} \omega_v(d_v).$$

By(20.5.2.3) there is a homeomorphism

$$\Gamma_0(N)\backslash GL(2,\mathbb{R})^+ \cong GL(2,\mathbb{Q})\backslash GL(2,A)/K_0(N),$$

which induces a map

$$f\mapsto \varphi_f : C^\infty(\Gamma_0(N)\backslash GL(2,\mathbb{R})^+,\chi_d|\cdot|^\lambda) \to C^\infty(GL(2,\mathbb{Q})\backslash GL(2,A),\omega|\cdot|^\lambda) : \varphi(\gamma g_\infty k_0) = f(g_\infty)\lambda_d(k_0)$$

and this map identifies K-finiteness, $\mathcal{Z}$-finiteness and moderate growth, thus induces a map

$$\mathcal{A}(\Gamma_0(N)\backslash GL(2,\mathbb{R})^+,\chi_d) \to \mathcal{A}(GL(2,\mathbb{Q})\backslash GL(2,A),\omega)$$

compatible with $(\mathfrak{g}_\infty, K_\infty)$-action, and the image are the automorphic forms satisfying $\pi(k_0)\varphi = \lambda(k_0)\varphi$ for $k_0 \in K_0(N)$.

This map also identifies cuspidality, thus it induces a map

$$\mathcal{A}_0(\Gamma_0(N)\backslash GL(2,\mathbb{R})^+,\chi_d) \to \mathcal{A}_0(GL(2,\mathbb{Q})\backslash GL(2,A),\omega)$$

⌟

Proof: To show that $\varphi_f(zg) = \omega(z)\varphi_f(g)$ for $z \in A^*$, notice by(14.4.4.30), $Z(A^\times) = Z(\mathbb{Q}^\times)Z(\mathbb{R}_+^\times)(Z(A)\cap K_0(N))$, and for these elements $\varphi_f(zg) = \lambda(z)\varphi_f$, as ω is trivial on $\prod_{v\notin S_f(N)}\mathcal{O}_v^\times$.

It identifies moderate growth because $A^\times = \mathbb{Q}^\times\mathbb{R}_+^\times\prod_{v\nmid\infty}\mathcal{O}_v^\times$ again.

To show cuspidality, notice $x\mapsto \gamma(\begin{bmatrix}1 & x\\ & 1\end{bmatrix}g)$ is left-invariant under a if $g^{-1}\begin{bmatrix}1 & a\\ & 1\end{bmatrix}g\in K_0(N)$. but such a is open in A, thus contains some open compact subgroup $U_f\subset A_f$. Notice by strong approximation, $A = \mathbb{Q}\times\mathbb{R}\times U_f$, thus there is an isomorphism $\mathbb{R}/M\cong A/FU_f$. Now let $g = \gamma g_\infty k_0$, then

$$\int_{A/F}\varphi_f(\begin{bmatrix}1 & a\\ & 1\end{bmatrix}g) = C\int_{\mathbb{R}/M}\varphi_f(\begin{bmatrix}1 & x\\ & 1\end{bmatrix}g)dx = C\lambda(k_0)\int_0^M f(\gamma^{-1}\begin{bmatrix}1 & x\\ & 1\end{bmatrix}\gamma g_\infty),$$

which vanishes for each g iff f is cuspidal at every cusp. For similar reason, φ_f is of moderate growth iff f is of moderate growth at every cusp. □

Remark (20.5.2.13). Similar isomorphism happens for more general congruence subgroups, for example, we can change $\Gamma_0(N)$ to $\Gamma_1(N)$ and change $K_0(N)$ to

$$U_1(N) = \{\begin{bmatrix}a & b\\ c & d\end{bmatrix}\in \mathrm{GL}(2,\widehat{\mathbb{Z}}) : c\equiv 0(\mathrm{mod}\ \ N), d\equiv 1(\mathrm{mod}\ \ N)\}.$$

⌟

Prop. (20.5.2.14) [Strong Multiplicity One].
- Let f be a cuspidal eigenfunction in $\mathcal{A}_0(\Gamma_0(N)\backslash GL(2,\mathbb{R})^+,\chi)$ of a.e. Hecke operators T_p for $p\nmid N$, then φ_f lies in an irreducible subspace of $L_0^2(GL(2,F)\backslash GL(2,A),\omega)$.
- If f, g are cuspidal eigenfunctions for a.e. Hecke operators in $\mathcal{A}_0(\Gamma_0(N)\backslash GL(2,\mathbb{R})^+,\chi)$ of a.e. Hecke operators T_p for $p\nmid N$, then $f = g$.

In particular, any Hecke eigenform generates a cuspidal representation. ⌟

Proof: 2: By(20.5.2.9), consider the projection of φ_f to any irreducible cuspidal representation π. By(20.5.2.11), φ_f is an eigenform of the Hecke operator T_p. But it is also eigenvalues of the Hecke operator R_p, But $\mathcal{H}_{\mathbb{Q}_p}$ is generated by T_p, R_p, R_p^{-1} by(20.2.2.10), so π_p is spherical with determined eigenvalues. But then π_v is determined by(3.6.4.12). Then π is determined by strong multiplicity one(20.5.3.8).

1 follows from 2 because if π is a component of $L_0^2(GL(2,F)\backslash GL(2,A),\omega)$ that the projection of φ_f is non-zero, then it has the same Hecke eigenvalue as φ_f, so it must be just φ_f by item2.

Cf.[Bump, P344]. □

Remark (20.5.2.15). WARNING: This is in general not true for groups other than $\mathrm{GL}(n)$. This is related to the theory of L-packets and A-packets.? ⌟

Remark (20.5.2.16) [Adelized Maass Forms]. Notice if f comes from a Maass form, then [G-H11] documented the properties of the adelized Maass form φ_f in detail. ⌟

Ramanujan Conjecture

Conj. (20.5.2.17) [Ramanujan]. If ω is unitary and $\rho = \otimes'\rho_v\in \mathrm{Irr}^{\mathrm{cusp}}(\mathrm{GL}(n)/F,\omega)$, then for any $v\in\Sigma_F$, ρ_v is tempered(18.11.6.3). ⌟

Proof: □

Prop. (20.5.2.18). The Ramanujan conjecture(20.5.2.17) implies the Ramanujan-Petersson conjecture(21.3.6.16). ⌟

Proof: The Ramanujan-Petersson conjecture says the eigenvalue λ_p of T_p on f satisfies $|\lambda_p| \leq 2p^{1/2}$. Consider the irreducible cuspidal representation π_f generated by φ_f(20.5.2.14), then T_p is the same as the eigenvalue of the local Hecke algebra T_p on φ_f. But $\pi_{f,p}$ is unramified, thus by(18.11.6.10) it is unitary principal or complementary. But notice if the Satake parameters of $\pi_{f,p}$ are α_i, then $\lambda_p = p^{1/2}(\alpha_1 + \alpha_2)$, Then it suffices to show that $|\alpha_1 + \alpha_2| \leq 2$, which is equivalent to π_p being tempered(18.11.6.10). □

Conj. (20.5.2.19)[Generalized Ramanujan Conjecture]. Let G be a reductive group over a global field F, and $\pi \in \mathrm{Irr}^{\mathrm{cusp},generic}(G/F, \omega)$, then π is tempered. Notice this implies the Ramanujan conjecture, as any $\rho \in \mathrm{Irr}^{\mathrm{cusp}}(\mathrm{GL}(n)/F, \omega)$ is generic(20.5.3.3). ⌟

Proof: □

Remark (20.5.2.20) [Arthur Conjecture]. In fact, Arthur extends this conjecture further, and explains the extent of failure of the Ramanujan conjecture for irreducible representations in the discrete spectrum of $L^2(G(\mathbb{F})\backslash G(\mathbb{A}))$, as well as the multiplicities in the discrete spectrum. ⌟

3 Whittaker Models

Def. (20.5.3.1)[Whittaker Models]. The notion of **Whittaker model** and **Whittaker functional**, genericness the same as in the local case(18.11.3.1). ⌟

Prop. (20.5.3.2)[Global uniqueness of Whittaker Models]. Let (π, V) be an irreducible admissible representation of $GL(2, A)$, then (π, V) has a Whittaker model w.r.t ψ iff each (π_v, V_v)(20.5.1.4) has a Whittaker model $\mathcal{W}(\pi_v, \psi_v)$. If this is the case, then $\mathcal{W}(\pi, \psi)$ is unique and

$$\mathcal{W}(\pi, \psi) = \bigotimes{}' (W_v, W_v^0)$$

where W_v^0 are the unique spherical function(18.11.5.15) of $\mathcal{W}_v$ normalized s.t. $W_v^0(K_v) = 1$. ⌟

Proof: Let $(\pi, V) = \otimes_v'(\pi_v, V_v)$ w.r.t a.e. spherical vectors ξ_v^0 by tensor product theorem(20.5.1.4), and (π_v, V_v) are spherical a.e. v.

Firstly if every (π_v, V_v) has a Whittaker model, the W in the proposition is truly a Whittaker model: functions in $\mathcal{W}(\pi, \psi)$ are clearly smooth and K-finite, and they have moderate growth because each local part is, and for a.e. v, $\mathcal{W}_v(\pi, \psi)$ is compactly supported on $|x|_v \leq 1$. And there is a canonical isomorphism of V onto $\mathcal{W}(\pi, \psi)$ by letting $(W_\xi)_v = W_v^0$ if $\xi_v = \xi_v^0$ and

$$W_\xi(g) = \prod_v W_{v,\xi_v}(g_v).$$

This is definable because $g_v \in K_v$ for a.e. v thus $W_{v,\xi_v}(g_v) = W_v^0(g_v) = 1$ for a.e. v.

Because the local Whittaker models are all rapidly decreasing, and the spherical Whittaker model vanishes for $|\xi_v|_v > 1$, thus W is also rapidly decreasing, and is a Whittaker model for π.

Secondly if $\mathcal{W}$ is a Whittaker model for (π, V), denote $\xi \mapsto W_\xi$ the isomorphism of V onto $\mathcal{W}$. Notice there exists some $\xi \in V$ that $W_\xi(1) \neq 0$: if $W_\xi(g_\infty g_f) \neq 0$, then $W_{\pi(g_f)\xi}(g_\infty) \neq 0$, and argue the same way as in(20.1.3.4). We may assume $\xi^0 = \otimes_v \xi_v^0$ that $W_{\xi^0}(1) = 1$.

Consider the "pullback" of W to $GL(n,F_v)$ via ξ, then they are clearly Whittaker models for (π_v,V_v) thus unique(15.4.1.5)(20.1.3.3), and also $W_{v,\xi_v^0}(1)=1$. So W_v^0 exists a.e. uniquely. Now we prove W is of the form we said above, this will prove uniqueness.

Then we need to prove

$$W_\xi(g)=\prod_v W_{v,\xi_v}(g_v)$$

We only need to prove for one $\xi=\xi^0$, because $\mathcal{W},\mathcal{W}(\pi_v,\psi_v)$ are both irreducible. And also we can assume $g_v=1, a.e.$, because $(W_\xi)_v(g_v)=W_{v,\xi_v}(g_v)=1$, a.e.. Then we are in the finite case and we can multiply by scalars at f.m. v s.t. this equation is true and nonzero for g. □

Thm. (20.5.3.3) [Fourier Expansion and Existence of Whittaker Models, Shalika]. Given $(\pi,V)\in \mathrm{Irr}^{\mathrm{cusp}}(\mathrm{GL}(n)/F,\omega)$, for $\Phi\in V$, define

$$W_\Phi(g)=\int_{\mathrm{Unip}(n,F)\backslash\mathrm{Unip}(n,A)}\Phi(ng)\psi_N(-n)dn,$$

then $GL(n,\mathbf{A}_F)$ acts on these functions, and they form a Whittaker model $\mathcal{W}(\pi,\psi)$. $W_\Phi(g)$ is called the **Fourier-Whittaker coefficients** for Φ.

And we have a Fourier expansion formula:

$$\Phi(g)=\sum_{\gamma\in\mathrm{Unip}(n-1,F)\backslash GL(n-1,F)}W_\Phi(\begin{bmatrix}\gamma&\\&1\end{bmatrix}g),$$

which converges absolutely and uniformly on compact subsets of $GL(n,\mathbf{A}_F)$. ⌟

Remark (20.5.3.4). This is false for some other groups, for the reason that the Fourier inversion may not be true, thus it map happen that all the Fourier coefficients vanish. For example, holomorphic Siegel modular forms on $\mathrm{Sp}(2n)$ don't have Whittaker models. ⌟

Proof: We only prove for $n=2$. For general case, see the beautiful paper[Sha74] of Shlika**?**.

For any $g\in GL(n,A)$, consider $F(n)=\varphi(ng)$ on $N(A)$, then it is a continuous function on $N(F)\backslash N(A)$, and $N(F)\backslash N(A)$ is compact(14.4.4.12), so by Fourier inversion formula(11.10.3.17),

$$F(x)=\sum_{\alpha\in F}C(\alpha)\psi(\alpha x),\quad C(\alpha)=\int_{\mathrm{Unip}(n,F)\backslash\mathrm{Unip}(n,A)}\varphi(\begin{bmatrix}1&x\\&1\end{bmatrix}g)\psi(-\alpha x)dx.$$

Now $C(0)=0$ because φ is cuspidal, and if $\alpha\in F^\times$, as φ is automorphic,

$$\begin{aligned}C(\alpha)&=\int_{\mathrm{Unip}(n,F)\backslash\mathrm{Unip}(n,A)}\varphi(\begin{bmatrix}\alpha&\\&1\end{bmatrix}\begin{bmatrix}1&x\\&1\end{bmatrix}g)\psi(-\alpha x)dx\\&=\int_{A/F}\varphi(\begin{bmatrix}1&\alpha x\\&1\end{bmatrix}\begin{bmatrix}\alpha&\\&1\end{bmatrix}g)\psi(-\alpha x)dx=W_\varphi(\begin{bmatrix}\alpha&\\&1\end{bmatrix}g).\end{aligned}$$

So if we let $x=0$, we get $\Phi(g)=\sum_{\alpha\in F^\times}W_\Phi(\begin{bmatrix}\alpha&\\&1\end{bmatrix}g)$.

Now we show $\{W_\Phi\}$ is Whittaker model: they all satisfies $W_\Phi(ng)=\psi(n)W_\Phi(g)$ by construction, and because $W_{X\varphi}=XW_\varphi$, $\rho(g)W_\varphi=W_{\rho(g)\varphi}$, it is clear that this space is invariant under action of $GL(2,A_f)$ and $(\mathfrak{g}_\infty,K_\infty)$, and also it is of moderate growth in y because φ does(20.5.1.10) and $N(F)\backslash N(A)$ is compact, and it consists of K-finite vectors because V is admissible(20.5.2.10). Finally, the Fourier inversion shows that $\varphi\mapsto W_\varphi$ is non-zero, thus injective. □

Cor. (20.5.3.5) [Cuspidal Forms Decay Rapidly]. Any cuspidal form on $GL(2,\mathbf{A}_F)$ is rapidly decreasing for $|y|\to\infty$.

Moreover, it also decays rapidly when $|y|\to 0$. ⌟

Remark (20.5.3.6). This is proved already in(20.5.1.11). ⌟

Proof: To show it is rapidly decreasing, use the Fourier expansion formula, and the fact the Whittaker model is product of local Whittaker models. Also for $v\in\Sigma_F^{\text{fin}}$, the local Kirillov model is compactly supported(18.11.3.19), and for $v\in\Sigma_F^\infty$, the Whittaker model is rapidly decreasing(20.1.3.3), notice for any $g\in GL(2,A)$, for any C, the number of $a\in K^*$ that $\varphi(\begin{bmatrix}a&\\&1\end{bmatrix}g)\neq 0$ and $|a|_\infty<C$ is bounded by a polynomial of C, thus it is rapidly decreasing.

For $|y|\to 0$, as φ is automorphic, notice

$$\varphi(\begin{bmatrix}y&\\&1\end{bmatrix})=\varphi(w_0\begin{bmatrix}1&\\&y\end{bmatrix}w_0)=\omega(y)(\pi(w_0)\varphi)(\begin{bmatrix}y^{-1}&\\&1\end{bmatrix}).$$

□

Cor. (20.5.3.7). Every local component of a cuspidal representation of $GL(n,A)$ is generic, by(20.5.3.2). ⌟

Prop. (20.5.3.8) [Strong Multiplicity One for $\mathrm{GL}(n)$]. If $(\pi,V),(\pi',V')\in\mathrm{Irr}^{\mathrm{cusp}}(\mathrm{GL}(n)/F)$ satisfy $\pi_v\cong\pi'_v$ a.e. v, then $\pi\cong\pi'$, and $V=V'\subset\mathcal{A}_0(\mathrm{GL}(n,F)\backslash GL(n,\mathbf{A}_F))$. ⌟

Proof: We only prove for $n=2$ and the case π_1,π_2 are isomorphic on Archimedean places**?**. For general n, Cf.[Representations of the Group $GL(n,K)$ where K is a local field, Gelfand-Kazhdan], [Euler Subgroups, in Lie Groups and their Representations, Piatetski-Shapiro(1975)]. For the Archimedean places, Cf.[Base Change for $GL(2)$, Langlands(1980)Lemma3.1]

Firstly if $\pi_v\cong\pi'_v$ for every place v, then their corresponding Whittaker model is the same(multiplied by a scalar) by(20.5.3.2). Then by(20.5.3.3) we have a Fourier expansion formula

$$\varphi(g)=\sum_{\alpha\in F^*}W_\varphi(\begin{bmatrix}\alpha&\\&1\end{bmatrix}g).$$

Thus $V=V'$.

In case that $\pi_v\cong\pi'_v$ only outside a finite set S, we choose functions W_v,W'_v in the local Whittaker model for π_v,π'_v s.t. if $v\notin S$, $W_v=W'_v$ and W_v is the unique spherical function normalized that $W_v(K_v)=1$ a.e. v, and if $v\in S$, they are chosen that

$$F(y)=W_v(\begin{bmatrix}y&\\&1\end{bmatrix})=W'_v(\begin{bmatrix}y&\\&1\end{bmatrix})\in C_c^\infty(F_v^\times),$$

which is possible by(18.11.3.20). And we define

$$\varphi(g)=\sum_{\alpha\in F^*}W(\begin{bmatrix}\alpha&\\&1\end{bmatrix}g),\quad \varphi'(g)=\sum_{\alpha\in F^*}W'(\begin{bmatrix}\alpha&\\&1\end{bmatrix}g),$$
$$W(g)=\prod_v W_v(g_v),\quad W'(g)=\prod_v W'_v(g_v).$$

as in(20.5.3.3).

Then we claim $\varphi=\varphi'$ on $GL(2,A)$: $\varphi\in V,\varphi'\in V'$ are automorphic, thus $\varphi=\varphi'$ on $GL(2,F)GL(2,\mathbf{A}_F^S)$ by continuity, which is just $GL(2,\mathbf{A}_F)$ by weak approximation, so we have a $\varphi\in V\cap V'$, meaning $V=V'$. □

4 Eisenstein Series

References are [Bump, Chap3].

Prop. (20.5.4.1)[Langlands]. For any $\rho \in \mathrm{Irr}^{\mathrm{auto}}(G/F, \omega)$, there exists a parabolic subgroup $P = MN$ and $\sigma \in \mathrm{Irr}^{\mathrm{cusp}}(M/F)$ that π is a subquotient of $I_P(\sigma)$. ⌟

Proof:

□

Remark (20.5.4.2). The pair (M, σ) may not be unique up to conjugacy. It is unique for $GL(n)$, by a theorem of Jacquet-Shalika, but in general it is false. For example, Waldspurger showed for $G = \mathrm{PGSp}(4)$ that there are cuspidal representations π that are abstractly isomorphic to a subquotient of some $I_P(\sigma)$ with σ cuspidal on $M = GL(2)$. These are called **CAP representations**. ⌟

20.6 Overview of the Langlands Program

1 Langlands Program

Main references are [Lan70]. Cf. Arthur's work on stabilization of trance formula, proof of the fundamental lemma by Laumon-Ngo, and inputs from Shin, Morel, Harris-etc..

Def. (20.6.1.1) [Langland Dual Groups]. For any connected reductive group G over a global field F, we want to define a complex analytic group ${}^L G_F$, and for each place $\mathfrak{p}$, a complex analytic group ${}^L G_{F_\mathfrak{p}}$, and complex analytic homomorphisms ${}^L G_{F_\mathfrak{p}} \to {}^L G_F$ defined up to conjugacy. The definition is given in [Lan70]. ⌟

Then for each complex analytic representation σ of ${}^L G_F$ and automorphic representation π of $G_{A(F)}$, we want to define an L-function

$$L(s,\sigma,\pi) = \prod_{\mathfrak{p}} L(s,\sigma_\mathfrak{p},\pi_\mathfrak{p})$$

that is convergent in some right half plane, and

$$L(s,\sigma_\mathfrak{p},\pi_\mathfrak{p}) = \prod_{i=1}^n \frac{1}{1-\alpha_i|\varpi_\mathfrak{p}|^s}$$

for any non-Archimedean plane $\mathfrak{p}$, where $n = \deg(\sigma_\mathfrak{p})$.

Also there is a functional equation

$$L(s,\sigma,\pi) = \varepsilon(s,\sigma,\pi)L(1-s,{}^L\sigma,\pi)$$

with

$$\varepsilon(s,\sigma,\pi) = \prod_{\mathfrak{p}} \varepsilon(s,\sigma_\mathfrak{p},\pi_\mathfrak{p},\psi_{F_\mathfrak{p}})$$

for any non-trivial character ψ of $F\backslash A(F)$, where the product is finite.

Conj. (20.6.1.2). Is it possible to define the local L-functions $L(s,\rho,\pi)$ and the local factors $\varepsilon(s,\rho,\pi,\psi_F)$ at the ramified primes that

$$L(s,\sigma,\pi) = \prod_{\mathfrak{p}} L(s,\sigma_\mathfrak{p},\pi_\mathfrak{p})$$

is meromorphic in the entire complex plane with only a finite number of poles and satisfies the functional equation. ⌟

Conj. (20.6.1.3). Suppose G,G' are reductive groups over the local field F and G is quasi-split and G' is an inner twist of G, then ${}^L G_F = {}^L G'_F$. Is there a correspondence $\mathrm{Irr}(G'_F) \to \mathrm{Irr}(G_F)$ s.t. if $\pi = R(\pi')$, then $L(s,\rho,\pi) = L(s,\rho,\pi')$ for any representation ρ of ${}^L G_F$? ⌟

Conj. (20.6.1.4) [Local Functorial Lifting]. Let G,G' be two quasi-split groups over the local field F. Let G split over K and K' where $F \subset K \subset K'$. Suppose $\varphi : {}^L G'_{K'/F} \to {}^L G_{K/F}$ is a complex analytic homomorphism that makes the diagram

$$\begin{array}{ccc} {}^L G'_{K'/F} & \longrightarrow & G(K'/F) \\ \downarrow{\scriptstyle\varphi} & & \downarrow \\ {}^L G_{K/F} & \longrightarrow & G(K/F) \end{array}$$

commutative, is there a correspondence $r_\varphi : \mathrm{Irr}(G'_F) \to \mathrm{Irr}(G_F)$ that if $\pi = R_\varphi(\pi')$, then for any representation ρ of ${}^L G_F$,

$$L(s,\rho,\pi) = L(s,\rho\circ\varphi,\pi'), \varepsilon(s,\rho,\pi,\psi_F) = \varepsilon(s,\rho\circ\varphi,\pi',\psi_F).$$

Such a correspondence is called a **functorial lifting** of π'. ⌟

Some evidences of(20.6.3.2) is given in[Lan70]P17.

Relation to Artin L-Functions

Let $F \in$ `LField` and $\psi \neq \mathbb{1} \in \chi(F)$. For any representation σ of $W_{K/F}$ we can define a local L-function $L(s,\sigma)$ and local factors $\varepsilon(s,\sigma,\psi_F)$.

If F is a global field and σ is a representation of $W_{K/F}$, then

$$L(s,\sigma) = \prod_{\mathfrak{p}} L(s,\sigma_{\mathfrak{p}}), \quad \varepsilon(s,\sigma) = \prod_{\mathfrak{p}} \varepsilon(s,\sigma_{\mathfrak{p}},\psi_{F_{\mathfrak{p}}})$$

satisfies the functional equation

$$L(s,\sigma) = \varepsilon(s,\sigma)L(1-s,{}^L\sigma).$$

Conj. (20.6.1.5). Suppose G is quasi-split over the local field F and splits over the Galois extension K. Let ${}^L U_K$ be a maximal compact subgroup of ${}^L G_F$. Let K' be a Galois extension of F containing K and let $\varphi : W_{K'/F} \to {}^L U_F$ be a homomorphism that makes the diagram

$$\begin{array}{ccc} W_{K'/F} & \longrightarrow & G(K'/F) \\ \downarrow{\scriptstyle\varphi} & & \downarrow \\ {}^L U_F & \longrightarrow & G(K/F) \end{array}$$

commutative, then there is an irreducible unitary representation $\pi(\varphi)$ of G_F s.t. for any representation σ of ${}^L G_F$, $L(s,\sigma,\pi(\varphi)) = L(s,\sigma\circ\varphi)$, and $\varepsilon(s,\sigma,\pi(\varphi),\psi_F) = \varepsilon(s,\sigma\circ\varphi,\psi_F)$. ⌟

Conj. (20.6.1.6). Suppose G is quasi-split over the local field F and splits over the Galois extension K. Let ${}^L U_K$ be a maximal compact subgroup of ${}^L G_F$. Let K' be a Galois extension of F containing K and let $\varphi : W_{K'/F} \to {}^L U_F$ be a homomorphism that makes the diagram

$$\begin{array}{ccc} W_{K'/F} & \longrightarrow & G(K'/F) \\ \downarrow{\scriptstyle\varphi} & & \downarrow \\ {}^L U_F & \longrightarrow & G(K/F) \end{array}$$

commutative. If $\mathfrak{P}'$ is a prime of K' and $\mathfrak{p} = \mathfrak{P}' \cap F$, then $\varphi_{\mathfrak{p}} = \varphi \circ \alpha_{\mathfrak{p}}$ takes $W_{K'_{\mathfrak{P}'}/F_{\mathfrak{p}}}$ into ${}^L U_{F_{\mathfrak{p}}}$. If $\pi(\varphi) = \otimes_{\mathfrak{p}} \pi(\varphi_{\mathfrak{p}})$, is $\pi(\varphi)$ an automorphic representation? ⌟

Relation to Elliptic Curves

Conj. (20.6.1.7). For $F \in$ `NField` and $E \in \mathcal{E}\mathrm{ll}/F$, for any place $\mathfrak{p}$, there is a representation $\pi(C/F_{\mathfrak{p}})$ of $\mathrm{GL}(2,F_{\mathfrak{p}})$**?**. Is it true that $\pi(C/F) = \otimes_{\mathfrak{p}} \pi(C/F_{\mathfrak{p}})$ is an automorphism representation? ⌟

2 Local Langlands

Archimedean Local Langlands for $\mathrm{GL}(n)$

Cf.[Local Langlands Correspondence, the Archimedean case, Knapp(1994)].

LLC for $\mathrm{GL}(n)$ **over Function Fields**

References are [G. Laumon, M. Rapoport, U. Stuhler: D-elliptic sheaves and the Langlands correspondence]. [V.G. Drinfeld: Elliptic modules, Mat. USSR Sbornik 23, pp. 561−592 (1974)], [V.G. Drinfeld: Elliptic modules II, Mat. USSR Sbornik 31, pp. 159–170 (1977)].

3 Global Langlands Correspondence

Global Langlands Conjectures

Prop. (20.6.3.1) [Langlands L-function]. Let $F \in$ `GField`, and G a reductive algebraic group over F, (π, V) an automorphic cuspidal representation of $G(A)$, $(\pi, V) = \prod'(\pi_v, V_v)$. Let S be a finite set of primes including the Archimedean ones and places that π_v is ramified or the field Ω/F defining ${}^L G$ is unramified. Let $r : {}^L G \to \mathrm{GL}(m, \mathbb{C})$ be a complex homomorphism, for $v \notin S$, let α_v be the semisimple conjugacy class in ${}^L G_v$ parametrizing π_v, then we define

$$L_v(s, \pi_v, r_v) = \frac{1}{\det(I - q_v^{-s} r_v(\alpha_v))}, \quad L_S(s, \pi, r) = \prod_{v \notin S} L_v(s, \pi_v, r_v)$$

called the **Langlands L-functions** attached to π and r. Langlands proved in [Euler Products, 1971] that such a product is convergent and analytic for $\mathrm{Re}(s)$ sufficiently large. ⌟

Conj. (20.6.3.2) [Global Functorial Lifting]. Suppose G, G' are two quasi-split groups over the global field F. Let G split over K and K' where $F \subset K \subset K'$. Suppose $\varphi : {}^L G'_{K'/F} \to {}^L G_{K/F}$ is a complex analytic homomorphism that makes the diagram

$$\begin{array}{ccc} {}^L G'_{K'/F} & \longrightarrow & G(K'/F) \\ \downarrow{\scriptstyle \varphi} & & \downarrow \\ {}^L G_{K/F} & \longrightarrow & G(K/F) \end{array}$$

commutative. If $\mathfrak{P}'$ is a prime of K', $\mathfrak{P} = \mathfrak{P}' \cap K, \mathfrak{p} = \mathfrak{P}' \cap F$, then φ determines a homomorphism $\varphi_{\mathfrak{p}} : {}^L G'_{K'_{\mathfrak{P}'}/F_{\mathfrak{p}}} \to {}^L G_{K_{\mathfrak{P}}/F_{\mathfrak{p}}}$ that makes the diagram

$$\begin{array}{ccc} {}^L G'_{K'_{\mathfrak{P}'}/F_{\mathfrak{p}}} & \longrightarrow & G(K'_{\mathfrak{P}'}/F_{\mathfrak{p}}) \\ \downarrow{\scriptstyle \varphi_{\mathfrak{p}}} & & \downarrow \\ {}^L G_{K_{\mathfrak{P}}/F_{\mathfrak{p}}} & \longrightarrow & G(K_{\mathfrak{P}}/F_{\mathfrak{p}}) \end{array}$$

commutative. If $\pi' = \otimes_{\mathfrak{p}} \pi'_{\mathfrak{p}}$ is an automorphic representation of G'_F, is it true that $\pi = \otimes_{\mathfrak{p}} R_{\varphi_{\mathfrak{p}}}(\pi'_{\mathfrak{p}})$ is an automorphic representation of G_F? Such an automorphic representation is called a **functorial lifting** or π'. ⌟

Remark (20.6.3.3). This conjecture reduces the conjecture about a general group to the case of $GL(n, F)$, which can be handled, such as by [Zeta Functions of Simple Algebras, Godement/Jacquet]. ⌟

Conj. (20.6.3.4). If(20.6.1.3) is true, if G, G' are defined over the global field F and G is quasi-split and G' is an inner twist of G, suppose $\pi' = \otimes_{\mathfrak{p}}\pi'_{\mathfrak{p}}$ is an automorphic representation of G'_F, is it true that $\pi = \otimes_{\mathfrak{p}}R(\pi'_{\mathfrak{p}})$ is an automorphism representation of G_F? ⌟

Conj. (20.6.3.5). ⌟

Def. (20.6.3.6)[L-Packets]. It is possible that two automorphic representations π and π' of $G(A)$ have the same L-function, and for any reductive group H over F and σ an automorphic representation of $H(A)$ and r_1 a complex analytic representation of ${}^LH$,

$$L_S(s, \pi\otimes\sigma, r\otimes r_1) = L_S(s, \pi'\otimes\sigma, r\otimes r_1).$$

In this case, π, π' are called to be in the same **L-packet**. ⌟

Prop. (20.6.3.7). Any L-packet is finite. And it is conjectured that every L-packet contains a generic representation. ⌟

Proof: □

4 Beyond Endoscopy

References are [Problems Beyond Endoscopy, Arthur].

20.7 Automorphic Forms Beyond GL(2)

Prop. (20.7.0.1)[Ramakrishnan, 2000]. Multiplicity one theorem is true for cuspidal representations on $SL(2)$. ⌟

Proof: □

Prop. (20.7.0.2) [Blasius, 1994]. Multiplicity one theorem is false for cuspidal representations on $\mathrm{SL}(n), n \geq 3$. ⌟

Proof: □

1 Automorphic Forms on Unitary Groups

Main references are [Automorphic Forms on Unitary Groups, Eischen].

Unitary groups provide a particularly fruitful setting in which to work. Unitary groups have associated Shimura varieties, which provide convenient structure for studying algebraic aspects of automorphic forms (which, in turn, arise as sections of a vector bundle over Shimura varieties). We have substantial results about Galois representations associated to automorphic forms on unitary groups (e.g. [Ski12, Che04, Che09, CH13, Har10]). In addition, we have convenient representations of the L-functions associated automorphic forms on unitary groups, which are useful both for proving analytic properties and for extracting algebraic information (and even p-adic properties, as seen in [EHLS20]). Working with unitary groups has enabled major developments, including a proof of the main conjecture of Iwasawa Theory for GL2 [SU14] and the rationality of special values of certain automorphic L-functions (including [Shi00, Har97, Har08, Har84, Bou15]), as well as progress toward cases of the Bloch−Kato conjecture (including [SU06, Klo09, Klo15, Wan19]), and the Gan−Gross−Prasad conjecture (many recent developments, including [Xue14, Xue19, Zha14, Liu14, Yun11, JZ20, He17, BP20, BPLZZ21]).

2 Quaternionic Modular Forms

Main references are [Modular Forms on Exceptional Groups, Pollack].

3 Weil Representations

We use notations as in3.

Def. (20.7.3.1) [Heisenberg Group of $O(V)$]. Let F be a local or finite field of characteristic$\neq 2$, (V, B) a quadratic space over F of dimension n, $O(V) = O(V, B)$. Then the **Heisenberg group** H is the group $V \times V \times F$ with the group law

$$(v_1^*, v_1, x_1)(v_2^*, v_2, x_2) = (v_1^* + v_2^*, v_1 + v_2, x_1 + x_2 + B(v_2, v_1^*) - B(v_1, v_2^*)).$$

Let $\psi : F \to \mathbb{C}$ a non-trivial character. We may identify V with V^* via the pairing $(v, v^*) \mapsto \psi(-2B(v, v^*))$. Then the group $A(V)$(11.10.3.20) is $V \times V \times \mathbb{T}$ with multiplication

$$(v_1^*, v_1, t_1)(v_2^*, v_2, t_2) = (v_1^* + v_2^*, v_1 + v_2, t_1 t_2 \psi(-2B(v_1, v_2^*))).$$

Then there is a surjective homomorphism $\tau : H \to A(V) : (v^*, v, x) \mapsto (v^*, v, \psi(x)\psi(-B(v, v^*)))$.

$A(V)$ acts on $L^2(G)$: $(\rho(v^*, v, t)\Phi)(u) = t\psi(-2B(u, v^*))\Phi(u + v)$(11.10.3.21), and this induces an action π of H on $L^2(G)$: $(\rho(v^*, v, x)\Phi)(u) = t\psi(-2B(u, v^*))\Phi(u + v)$.

$SL(2,F)$ acts on H: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}(v_1, v_2, x) = (av_1 + bv_2, cv_1 + dv_2, x)$, and acts on $A(V)$: $\begin{bmatrix} a & b \\ c & d \end{bmatrix}(v_1, v_2, t) = (av_1 + bv_2, cv_1 + dv_2, t\psi(-acB(v_1, v_1) - bdB(v_2, v_2)))$, these two actions are compatible with τ.

$O(V)$ acts on H: $g(v_1, v_2, x) = (gv_1, gv_2, x)$, and a similar action on $A(V)$, compatible with τ.

Recall the Fourier transform on V w.r.t. the pairing $(v, v^*) \mapsto \psi(-2B(v, v^*))$. ⌟

Prop. (20.7.3.2). There exists a unitary projective representation ω_1 of $Sp(2n, B)$ on $L^2(V)$ that for the subgroup $SL(2,F) \subset Sp(2n, B)$,

- For $g \in SL(2,F), h \in H$, $\omega_1(g)\pi(h)\omega_1(g)^{-1} = \pi(g(h))$.
- $(\omega_1(\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix})\Phi)(v) = \psi(xB(v,v))\Phi(v)$.
- $(\omega_1(\begin{bmatrix} a & \\ & a^{-1} \end{bmatrix})\Phi)(v) = |a|^{d/2}\chi(a)\Phi(av)$, where $\chi(a)$ is any element that $|\chi(a)| = 1$.
- $\omega_1(w_1)\Phi = \gamma(B)\widehat{\Phi}$, where $\gamma(B)$ is any element that $|\gamma(B)| = 1$.

and there is a unitary representation ω_2 of $O(V)$ on $L^2(V)$ that

- $\omega_2(k)\pi(h)\omega_2(k)^{-1} = \pi(k(h))$.
- $(\omega_2(k)\Phi)(v) = \Phi(k^{-1}v)$.
- ω_2 commutes with ω_1.

where π is a Schrödinger representation of $A(V)$ on $L^2(V)$(11.10.3.21). ⌟

Proof: Because the action of $Sp(2n, B)$ on $A(V)$ is in $B_0(V)$, thus by(11.10.3.21), there are unitary automorphisms of $L^2(G)$ that

$$\omega_1(g)\pi(h)\omega_1(g)^{-1} = \pi(g(h)).$$

Now to check the properties of ω, it suffices to check this equation for $h = (v, 0, 1)$ or $(0, v, 1)$ because these elements generate $A(V)$, using the fact ρ action on $L^2(V)$ is irreducible(11.10.3.21).**?**

For $O(V)$, just verify directly. □

Prop. (20.7.3.3)[$\dim V$ **Even Case**]**.** If F is a local or finite field of characteristic$\neq 2$, V has dimension $2n$, and if we define $\Delta = (-1)^n \det(B) \in F^*/(F^*)^2$, $\chi : F^* \to \{\pm 1\}$ the quadratic character $a \mapsto (\Delta, a)_F$(14.5.5.8), and $\gamma(B)$ as defined in(14.5.5.9), then the projection representation of $SL(2,F)$ in(20.7.3.2) is a true representation.

It suffices to check the relations(3.1.5.8). Use(14.5.5.14) to show that $\gamma(B)^2 = \chi(-1)$. And it suffices to show that

$$w_1 \begin{bmatrix} a^{-1} & \\ & a \end{bmatrix} \begin{bmatrix} 1 & -a \\ & 1 \end{bmatrix} w_1 \begin{bmatrix} 1 & -a^{-1} \\ & 1 \end{bmatrix} \Phi = \begin{bmatrix} 1 & a \\ & 1 \end{bmatrix} w_1 \Phi$$

The LHS equals $\gamma(B)^2|a|^{-n}\mathcal{F}(\Phi * F_{-a^{-1}B})$, which by(14.5.5.9) and(14.5.5.13) equals $\gamma(B)\mathcal{F}(\Phi)F_{aB}$, which is just the RHS. ⌟

Conj. (20.7.3.4)[**Theta Correspondence(Special Case)**]**.** Let ω be the action of $SL(2,F) \times O(V)$ on $L^2(V)$ as in(20.7.3.3) and(20.7.3.2), then its smooth part $C_c^\infty(V)$ is a smooth representation ω_∞. Let π_1 be an irreducible admissible representation of $SL(2,F)$, π_2 an irreducible admissible representation of $O(V)$, they are said to **correspond** iff there exists a non-zero intertwining operator $\omega_\infty \to \pi_1 \otimes \pi_2$.

Then each π_1 can corresponds to at most one π_2, and vise versa. ⌟

Proof: This is proved for non-Archimedean local fields of odd residue characteristic by Waldspurger(1990). □

Def. (20.7.3.5)[Setup for Dihedral Weil Representation]. Let F be local or finite field, and E be a 2-dimensional commutative semisimple algebra over F, then $E = F \oplus F$ and F embeds diagonally, called the **split case**; or E is the unique quadratic extension of F, called the **anisotropic case**. Let the automorphism of E given by

$$x \mapsto \overline{x} : \begin{cases} \overline{(\xi, \eta)} = (\eta, \xi), & E = F \oplus F \\ \text{The non-trivial Galois automorphism}, & E \text{ is a field} \end{cases}.$$

Let $\mathrm{tr}(x) = x + \overline{x}, N(x) = x\overline{x}$. Let $E_1^* = \{x \in E^* | N(x) = 1\}$.

There is an embedding ι of E into $GO(E) \subset GL(2, F)$: for $E = F \oplus F$, it embeds diagonally, and for E a field, E embeds by left action on itself. Notice $\overline{\iota(x)(\overline{y})} = \iota(\overline{x})(y)$, thus $GO(E) \cong E^* \rtimes \{\}$**?**.

Let ψ be a character of E^* that is non-trivial on E_1^*. ⌟

Prop. (20.7.3.6)[Howe Duality of Dihedral Representations]. Let ψ be a character of E^*, then by(18.1.1.12), ψ extends to a representation of $GO(E)$ iff $\psi(x) = \psi(\overline{x})$, which is equivalent to $\psi(x) = 1$ on E_1^*, by Hilbert's theorem90 or direct inspection. Then by(18.1.1.12), in the other case, $\mathrm{ind}_{E^*}^{GO(E)} \psi$ is an irreducible representation of $GO(E)$, and Howe duality predicts an irreducible smooth representation of $GL(2, F)$. In case E is a field or F is finite, we can construct this representation directly, in(20.7.3.7) and(18.6.10.8). ⌟

Prop. (20.7.3.7) [Dihedral Representations]. Let E/F be a quadratic extension of non-Archimedean local fields, then E is a quadratic space over F by the norm form, and let ξ be a quasi-character of E^* that doesn't factor through the norm map $N : E^* \to F^*$. Let $U_{\xi,\psi}$ be the space of functions $\Phi \in C_c^\infty(E)$ that satisfy

$$\Phi(yv) = \xi(y)^{-1}\Phi(v), \quad \forall y \in E^*, N(y) = 1,$$

and let $\chi : F^* \to \{\pm 1\}$ be the quadratic character attached to the extension E/F(14.6.2.14), and let $GL(2, F)_+$ be the subgroup of $GL(2, F)$ that the determinants are norms from E, which is an open normal subgroup of index2, then there exists an irreducible admissible representation $\omega_{\xi,\psi}$ of $GL(2, F)_+$ on $U_{\xi,\psi}$ s.t.

$$(\omega_{\xi,\psi}(\begin{bmatrix} a & \\ & 1 \end{bmatrix})\Phi)(v) = |a|^{1/2}\xi(b)\Phi(bv), \quad \forall b \in E^*, N(b) = a \in F^*$$

$$(\omega_{\xi,\psi}(\begin{bmatrix} 1 & x \\ & 1 \end{bmatrix})\Phi)(v) = \psi(xN(v))\Phi(v)$$

$$(\omega_{\xi,\psi}(\begin{bmatrix} a & \\ & a^{-1} \end{bmatrix})\Phi)(v) = |a|\chi(a)\Phi(av)$$

$$(\omega_{\xi,\psi}(w_1)\Phi) = \gamma(N)\widehat{\Phi}.$$

Then the representation ω_ξ of $GL(2, F)$ induced from this representation of $GL(2, F)_+$ is irreducible and cuspidal. ⌟

Remark (20.7.3.8). For F with odd residue characteristic, this dihedral representation is the only cuspidal representation of $GL(2,F)$, by Tunnell 1978 or 1979.**?** ⌟

Proof: Notice in this case, the character χ defined in(20.7.3.3) is the same as the quadratic character corresponding to E/F: let $E = F(\sqrt{D})$, then $N_{E/F} = \langle 1, -D\rangle$, thus $(a,D)_F = 1$ iff $\langle a, D, -1\rangle$ is universal iff a is represented by $\langle 1, -D\rangle$, which is equivalent to $a \in N_{E/F}(E^*)$. Then by(20.7.3.3), we have an action of $SL(2,F)$ on $L^2(E)$, and we can extend it to $GL(2,F)_+$ satisfying all these equations(**?** by direct verification). And it can be verified $U_{\xi,\psi}$ is stable under this action.

We show this action is smooth: Every $\varphi \in U_{\xi,\psi}$ is stable under some $K(\mathfrak{p}^n)$ for n large: By(18.11.1.9), it suffices to prove it is stable under $N_-(\mathfrak{p}^n), T(\mathfrak{p}^n)$ and $N(\mathfrak{a})$. By action of w_1, it suffices to show it is stable under the latter two. But this is clear from the equations above.

Similarly, to show it is admissible, it suffices to show for any ideal $\mathfrak{a}$, the space of functions fixed by $N(\mathfrak{a})$ and $N_-(\mathfrak{a})$ is of f.d.: It is clear from equation2 that if φ is fixed by $N(\mathfrak{a})$, then there is a fractional ideal $\mathfrak{a}'$ that $\mathrm{Supp}(\varphi) \subset N^{-1}(\mathfrak{a}')$. Similarly for $\mathcal{F}(\varphi)$. These two conditions means φ has bounded support and fixed by some open subgroup, these functions are f.d..

To show $\omega_{\xi,\psi}$ and ω_ξ are irreducible: Let $B_1(F)_+$ be the subgroup of $B_1(F)$ consisting of matrices $\{\begin{bmatrix} a & b \\ & 1\end{bmatrix} | a \in N_{E/F}(E^*)\}$, let $\mathcal{K}_+$ the restriction of $\omega_{\xi,\psi}$ to $B_1(F)_+$. Define a map

$$\Lambda : C_c^\infty(N(E^*)) \to \mathcal{K}_+ : (\Lambda\varphi)(v) = \xi(v)^{-1}|N(v)|^{-1/2}\varphi(N(v)),$$

then this is an isomorphism, and is $B_1(F)$-invariant, where $B_1(F)$ acts on $C_c^\infty(N(E^*))$ as in(18.11.3.15). Thus by Mackey decomposition(18.1.5.42),

$$\mathrm{res}_{B_1(F)} \mathrm{ind}_{GL(2,F)_+}^{GL(2,F)} \omega_{\xi,\psi} \cong \mathrm{ind}_{B_1(F)_+}^{B_1(F)} \omega_{\xi,\psi} \cong \mathrm{ind}_{N(F)}^{B_1(F)} \psi,$$

which is irreducible by(18.11.3.16). thus ω_ξ is irreducible, thus also does $\omega_{\xi,\psi}$.

A byproduct of the above argument is that ω_ξ is cuspidal. □

4 Gan-Gross-Prasad Conjecture

Main References are [Background on the Gan-Gross-Prasad Conjecture, David Schwein].

20.8 Trace Formulae

Main references are [Introductory notes on the trace formula, Lapid], [Trace formula, Whitehouse] and [Trace Formula, Arthur].

1 Introduction

Remark (20.8.1.1). Delete this subsection. ⌟

The trace formula was introduced by Selberg in his seminal work. Selberg mostly developed the trace formula for quotients of the hyperbolic plane by a Fuchsian group Γ of the first kind (both in the co-compact and the non co-compact case). One of his original motivations and applications was to show the existence of Maass forms with respect to $\Gamma = SL(2, Z)$. It was subsequently vastly generalized by Arthur in the context of adelic quotients $G(F)\backslash G(A)$ of a reductive group G over a number field F. Arthur's main driving force was the functoriality conjectures of Langlands.

Selberg's trace formula is a far-reaching non-commutative generalization of the Poisson summation formula. It underlines a duality between geometric and spectral objects.

2 Trace Formulae

Trace Formula for Compact Quotient

Prop. (20.8.2.1). Consider the right action of G on $L^2(\Gamma\backslash G,\chi)$(20.1.1.17), let $\varphi \in C_c^\infty(G)$, then φ can act on $L^2(\Gamma\backslash G,\chi)$ by(11.8.3.24), and:

- $\rho(\varphi)$ is an integration operator, in particular Hilbert-Schmidt and compact. And $\mathrm{Im}(\rho(\varphi)) \subset C^\infty(\Gamma\backslash G,\chi)$.
- If $\varphi(g^{-1}) = \overline{\varphi(g)}$, then $\rho(\varphi)$ is self-adjoint.
- If $\varphi(k_\theta g) = e^{-tk\theta}\varphi(g)$, then $\mathrm{Im}(\rho(\varphi)) \subset C^\infty(\Gamma\backslash G,\chi,k)$.

Compare with(20.8.2.4). ⌟

Proof: These follows from(20.8.2.4). □

Cor. (20.8.2.2). Let H be a nonzero closed G-subrepresentation of $L^2(\Gamma\backslash G,\chi)$, then H decomposes as $\oplus_k H^k$ w.r.t. action of $SO(2,\mathbb{R})$. And if $H^k \neq 0$, then Δ has a nonzero eigenvector in $H^k \cap C^\infty(\Gamma\backslash G,\chi)$. ⌟

Proof: The decomposition is clear from(11.10.4.3). It's left to show Δ has an eigenvalue in $H_k \cap C^\infty(\Gamma\backslash G,\chi)$. By lemma(18.9.4.1) above, for $f_0 \in H^k$, there is a $\varphi \in C_c^\infty(G)$ s.t. $\rho(\varphi)f_0 \neq 0$, and $\varphi(k_\theta g) = e^{-ik\theta}\varphi(g)$. So(20.8.2.1) shows $\rho(\varphi)$ maps H into $H^k \cap C^\infty(\Gamma\backslash G,\chi)$ and induces a compact self-adjoint operator on H^k. So we can choose a f.d. eigenspace of it. Notice Δ commutes with the action $\rho(\varphi)$, so Δ fixes this eigenspace, thus it has an eigenvalue on $H_k \cap C^\infty(\Gamma\backslash G,\chi)$. □

Prop. (20.8.2.3)[$L^2(\Gamma\backslash G)$ Totally Decomposable]. Let G be a unimodular locally compact topological group and $\Gamma \subset G$ be a discrete subgroup that $\Gamma\backslash G$ is compact, $\chi \in \widehat{\Gamma}$, then the space $L^2(\Gamma\backslash G,\chi)$ decomposes as

$$L^2(\Gamma\backslash G,\chi) = \bigoplus_{\pi\in\widehat{G}} m_\pi V_\pi$$

that each m_π is finite. ⌟

Proof: Let Σ be the set of sums of irreducible invariant subspaces of $L^2(\Gamma\backslash G,\chi)$ that is mutually orthogonal. then choose by Zorn's lemma a maximal one in Σ, and we prove the orthogonal complement $H=0$ otherwise we construct an irreducible subspace of H.

Let $f\neq 0\in H$, choose by(18.9.4.1) and(20.8.2.1) a $\varphi\in C_c(G)$ that $\rho(\varphi)$ is compact self-adjoint and $\rho(\varphi)f\neq 0$. So $\rho(\varphi)$ has a non-zero eigenvalue and the eigenspace L is of f.d..

Let L_0 be a minimal nonzero subspace of L that is an intersection of L with a nonzero closed invariant subspace of $\mathcal{H}$, and let V be the intersection of all closed invariant subspaces W of H that $L_0=L\cap W$. We show V is irreducible, if not, then $V=V_1\cap V_2$, and if $0\neq f_0\in L_0$, then $f_0=f_1+f_2$ and both f_1,f_2 are eigenfunctions of $\rho(\varphi)$ of eigenvalue λ. Now if $f_1\neq 0$, then by minimality, $V_1\cap L=L_0$.

The finiteness of m_π follows from the fact that $\rho(f)$ is Hilbert-Schmidt for every $f\in C_c(G)$(20.8.2.4). □

Prop. (20.8.2.4). If $\Gamma\subset G$ is a discrete subgroup that $\Gamma\backslash G$ is compact, consider the right action of G on $L^2(\Gamma\backslash G)$(11.10.2.9), let $\varphi\in C_c(G)$, then φ can act on $L^2(\Gamma\backslash G,\chi)$ by(11.8.3.24), and:

- $\rho(\varphi)$ is an integration operator, in particular Hilbert-Schmidt and compact.
- If $\varphi(g^{-1})=\overline{\varphi(g)}$, then $\rho(\varphi)$ is self-adjoint.

⌟

Proof: 1:

$$(\rho(\varphi)f)(g)=\int_G f(h)\varphi(g^{-1}h)dh=\int_{\Gamma\backslash G_1}\sum_{\gamma\in\Gamma}f(\gamma h)\varphi(g^{-1}\gamma h)dh=\int_{\Gamma\backslash G_1}f(h)K_\varphi(g,h)dh$$

where

$$K_\varphi(g,h)=\sum_{\gamma\in\Gamma}\varphi(g^{-1}\gamma h).$$

Because φ is compactly supported, this is a smooth function in g and h, in particular square integrable on $\Gamma\backslash G$ compact. And $\rho(\varphi)(f)(g)$ is smooth in g because $f\in L_1(\Gamma\backslash G_1,\chi)$ as $\Gamma\backslash G_1$ is compact, and $K(g,h)$ is smooth in g.

2 is easy. □

Prop. (20.8.2.5) [Trace of $\rho(f)$]. If $\varphi=\varphi_1*\varphi_2$ where $\varphi_i\in C_c(\Gamma\backslash G)$, then $\rho(\varphi)=\rho(\varphi_1)\rho(\varphi_2)$(11.8.3.24) and hence a trace class(11.9.5.7). And its integral kernel is

$$K_\varphi(x,y)=\int_{\Gamma\backslash G}K_{\varphi_1}(x,z)K_{\varphi_2}(z,y)dz.$$

and

$$\operatorname{tr}\rho(f)=\int_{\Gamma\backslash G}K_\varphi(x,x)dx=\int_{\Gamma\backslash G}\int_{\Gamma\backslash G}K_{\varphi_1}(x,y)K_{\varphi_2}(y,x)dxdy.$$

⌟

Proof: This follows from(11.9.5.10). □

Cor. (20.8.2.6) [the Geometric Side of Trace Formula]. If G is unimodular, let $f=f_1*f_2$, $c(\gamma)$ be a representative for the conjugacy classes of Γ, then

$$\operatorname{tr}(\rho(f))=\sum_{\gamma\in c(\Gamma)}\int_{\Gamma_\gamma\backslash G}f(x^{-1}\gamma x)dx.$$

And if G_γ is unimodular for every $\gamma \in \Gamma$, then

$$\operatorname{tr}(\rho(f)) = \sum_{\gamma \in c(\Gamma)} V(\Gamma_\gamma \backslash G_\gamma) \int_{G_\gamma \backslash G} f(x^{-1}\gamma x) dx.$$

┘

Proof:

$$K_f(x,x) = \sum_{\gamma \in \Gamma} f(x^{-1}\gamma x) = \sum_{\gamma \in c(\Gamma)} \sum_{\delta \in \Gamma_\gamma \backslash \Gamma} f(x^{-1}\delta^{-1}\gamma\delta x),$$

so we have

$$\int_{\Gamma \backslash G} K_f(x,x) dx = \int_{\Gamma \backslash G} \sum_{\gamma \in c(\Gamma)} \sum_{\delta \in \Gamma_\gamma \backslash \Gamma} f(x^{-1}\delta^{-1}\gamma\delta x) = \sum_{\gamma \in c(\Gamma)} \int_{\Gamma_\gamma \backslash G} f(x^{-1}\gamma x) dx.$$

□

Cor. (20.8.2.7) [Trace Formula for $\Gamma \backslash G$ Compact]. Let G be a unimodular locally compact topological group and $f = f_1 * f_2$ where $f_i \in C_c(G)$, and Γ be a discrete subgroup of G with $\Gamma \backslash G$ compact and G_γ is unimodular for every $\gamma \in \Gamma$, then $\rho(f)$ is a trace class with

$$\sum_{\pi \in \widehat{G}} m_\pi \operatorname{tr}(\pi(f)) = \operatorname{tr}(\rho(f)) = \sum_{\gamma \in c(\Gamma)} V(\Gamma_\gamma \backslash G_\gamma) \int_{G_\gamma \backslash G} f(x^{-1}\gamma x) dx.$$

┘

Proof: Follows from(20.1.4.2) and(20.8.2.6). □

Lemma (20.8.2.8). Let $G = GL(2,\mathbb{R}), K = SL(2,\mathbb{R})$, $\Gamma \backslash G$ be compact, ρ be the principal series $P(\lambda, 0)$(18.9.4.15) of G, and $s = \frac{1}{2}(s_1 - s_2 + 1), \lambda = s(1-s), \mu = (s_1 + s_2)$, then for any $f \in C_c^\infty(K \backslash G/K)$, $\rho(f) \in V_\rho^K$, which has dimension1, so f is a trace class and

$$\operatorname{tr}(\rho(f)) = \int\int f(\begin{bmatrix} e^{u/2} & x \\ 0 & e^{-u/2} \end{bmatrix}) e^{\frac{us}{2}} du dx.$$

┘

Proof: The trace of $\rho(f)$ is just the scalar by which $\rho(f)$ acts on a non-zero vector of ρ^K. Take $\varphi \in \rho^K \subset H(s_1, s_2, 0)$ normalized that $\varphi(I) = 1$, then

$$(\rho(f)\varphi)(I) = \int_G f(g)\varphi(g) dg = \int_K \int_A \int_N f(ank)\varphi(ank) dA dN d\theta = \int_A \int_N f(an)\varphi(an) dA dN$$

□

20.9 Modular Galois Representations

This section concerns automorphy and modularity of global Galois Representations.

Notation (20.9.0.1).
- Let $(F, \mathcal{O}_F) \in$ `NField`.

⌟

1 Galois Representation attached to Automorphic Forms

Prop. (20.9.1.1) [Representation Associated to a Cusp Form, Eichler-Shimura]. For any newform $f \in S_k(\Gamma_1(N))$, let $\mathcal{O}_f$ be the ring generated by the coefficients of f, then there exists a Galois representation

$$\rho_f : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(2, \mathcal{O}_f).$$

⌟

Proof: □

Automorphic Galois Representations

Def. (20.9.1.2) [Automorphic Galois Representations]. An **automorphic Galois representation** is a Galois representation of $\mathrm{Gal}_{\mathbb{Q}}$ on a p-local field that is attached to an automorphic representation of $\mathrm{GL}(n, \mathbf{A}_F)$ for some $F \in$ `NField` via the global Langlands conjecture. ⌟

Def. (20.9.1.3) [Modular Galois Representations]. A continuous irreducible representation $\mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(2, \overline{\mathbb{F}}_p)$ or $\mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(2, K)$, where $K \in p$-`NField` is called a **modular Galois representation** if it arises from a newform as in(20.9.1.1). ⌟

Def. (20.9.1.4) [Modular Galois Representations]. Let A be a $\mathbb{Z}_p$-algebra and $\rho : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(2, A)$ be a representation, then ρ is called a **modular Galois representation** if there exists some $N > 0$ and a homomorphism $\mathrm{pr} : T'(N) \to A$(where $T'(N) = \mathbb{Z}[T_\ell, \langle d \rangle] \subset \mathrm{End}(S_2(\Gamma_1(N)))$, $\ell \in \mathbf{P} \backslash \{p\}, d \in (\mathbb{Z}/(N))^*$) s.t. ρ is unramified outside Np, and for $\ell \nmid pN$,

$$\mathrm{tr}(\rho(\mathrm{Frob}_\ell)) = \mathrm{pr}(T_\ell), \quad \det(\rho(\mathrm{Frob}_\ell)) = \mathrm{pr}(\langle \ell \rangle)\ell.$$

? ⌟

Conj. (20.9.1.5) [Langlands-Fontaine-Mazur]. Any geometric representation of Gal_F is automorphic(20.9.1.2). ⌟

Remark (20.9.1.6). This is very likely to imply Fontaine-Mazur conjecture(20.9.5.2). ⌟

Level-Lowering

Cor. (20.9.1.7) [Level-Lowering, Ribet]. Let $p, \ell \in \mathbf{P}, N \in \mathbb{Z}_+, \ell \nmid N$, and $f \in S_2^{\mathrm{new}}(\Gamma_0(N\ell))$. Suppose that $\overline{\rho}_{f,p}$ is irreducible and one of the following is true:
- $\overline{\rho}_{f,p}$ is unramified at ℓ,
- $\ell = p$ and $\overline{\rho}_{f,p}$ is flat at p.

Then there exists a $g \in S_2(\Gamma_0(N))$ s.t. $\overline{\rho}_{g,p} \cong \overline{\rho}_{f,p}$. ⌟

Proof: Cf.[Fermat's last theorem, Chap7]. □

Potential Modularity

Remark (20.9.1.8). A potential modularity result is a result that says certain representation of $\mathrm{Gal}_{\mathbb{Q}}$ comes from geometry when restricting to Gal_F for some $F \in \mathtt{NField}$. Cf.[Remarks on a Conjecture of Fontaine and Mazur, Taylor]. ⌟

2 Geometric Galois Representations

Def. (20.9.2.1) [Geometric Representations]. For $F \in \mathtt{NField}, p \in \mathbf{P}$, $(\rho, V) \in \mathrm{Rep}_{\overline{\mathbb{Q}_p}}(\mathrm{Gal}_F)$ is called a **geometric representation** if it satisfies

- For a.e. $v \in \Sigma_F^{\mathrm{fin}}$, ρ_v is unramified.
- For any $v \in S(p)$, the representation ρ_v is deRham(18.4.4.10).

It is called a **genuine geometric representation** if it is isomorphic to the subquotient of some $\mathrm{H}^r_{\text{ét}}(X_{\overline{F}}, \mathbb{Q}_p)(m)$ where $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}/F$ and $m \in \mathbb{Z}$. ⌟

Prop. (20.9.2.2) [Change of Fields]. Let $E/F \in \mathtt{NField}$ be a field extension, then geometric representations are stable under res^L_K and Ind^L_K. ⌟

Proof: □

Compatible Systems

Prop. (20.9.2.3) [Compatible System of adic Representations]. For $E, F \in \mathtt{NField}, n \in \mathbb{Z}_+$, an E-rational n-dimensional **weakly compatible system of Galois representations** of Gal_F is a collection

$$\mathcal{R} = \{R_{\ell,\iota}\}_{\ell \in \mathbf{P}, \iota \in \mathrm{Hom}(E, \overline{\mathbb{Q}_\ell})},$$

where $R_{\ell,\iota}$ are semisimple ℓ-adic Galois representations

$$R_{\ell,\iota} : \mathrm{Gal}_F \to \mathrm{GL}(n, \overline{\mathbb{Q}_\ell}),$$

which satisfy the following conditions:

1. There is a multiset of integers H-T$(\mathcal{R})$ s.t. for any (ℓ, ι), the restriction $R_{\ell,\iota}|_{\mathrm{Gal}_{\mathbb{Q}_\ell}}$ is deRham and H-T$(R_{\ell,\iota}|_{\mathrm{Gal}_{\mathbb{Q}_\ell}}) =$ H-T$(\mathcal{R})$.
2. There exists a finite set $S \subset \Sigma_F^{\mathrm{fin}}$ s.t. if $v \notin S$, then $\mathrm{WD}_v(R_{\ell,\iota})$ is unramified for all (ℓ, ι).
3. For a.e. $v \in \Sigma_F^{\mathrm{fin}}$, there is an F-semisimple WD-representation $\mathrm{WD}_v(\mathcal{R}) \in \mathfrak{wd}^n_E(W_{F_v})$ s.t. for all (ℓ, ι),
$$\mathrm{WD}_v(R_{\ell,\iota})^{F\text{-ss}} \sim \mathrm{WD}_v(\mathcal{R}) \otimes_{E,\iota} \overline{\mathbb{Q}_\ell}.$$

Moreover,

- $\mathcal{R}$ is called a **strongly compatible system of adic representations** if condition3 holds for any $v \in \Sigma_F$.
- $\mathcal{R}$ is called **odd/irreducible/geometric** if each $R_{\ell,\iota}$ is.
- $\mathcal{R}$ is called **pure of weight** $w \in \mathbb{Z}$ if for a.e. $p \in \mathbf{P}$ and eigenvalues α_i of $\mathfrak{wd}_p(\mathcal{R})$, $|\alpha_i| \in \overline{\mathbb{Q}}$, and
$$|\iota(\alpha_i)|^2 = p^w.$$

- $\mathcal{R}$ is called a **genuinely geometric system** if there exists an $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/\mathbb{Q}$ and $i \in \mathbb{N}, j \in \mathbb{Z}$ and a subspace
$$W \subset H_{\text{Betti}}(X, \overline{\mathbb{Q}}(j))$$
s.t. for any (ℓ, ι), $W \otimes_{\overline{\mathbb{Q}},\iota} \overline{\mathbb{Q}}_\ell$ is $\mathrm{Gal}_\mathbb{Q}$-invariant and realizes $R_{\ell,\iota}$.

⌟

Conj. (20.9.2.4).
- If $\rho : \mathrm{Gal}_\mathbb{Q} \to \mathrm{GL}(n, \overline{\mathbb{Q}}_\ell)$ be a continuous semisimple representation unramified at a.e. places and deRham at p, then ρ is a part of a weakly compatible system.
- Any weakly compatible system is strongly compatible.
- Any irreducible strongly compatible system $\mathcal{R}$ is geometric and pure of weight $\frac{2}{\dim \mathcal{R}} \sum_{h \in \text{H-T}(\mathcal{R})} h$.

⌟

3 Modularity Lifting

Thm. (20.9.3.1) [Modularity Lifting, Taylor-Wiles/Khare-Wintenberger]. Assume $p \in \mathbf{P}$ and $\overline{\rho} : \mathrm{Gal}_\mathbb{Q} \to \mathrm{GL}(2, \overline{\mathbb{F}_p})$ is a continuous modular Galois representation, and
- $\mathrm{Im}(\overline{\rho})$ is non-solvable if $p = 2$,
- $\overline{\rho}|_{\mathbb{Q}(\zeta_p)}$ is absolutely irreducible if $p > 2$.

Then ρ is also modular if:
- $(p = 2)$ and ρ is an odd lift of $\overline{\rho}$ to a 2-adic representation that is
  - a.e. unramified,
  - crystalline of weight 2 at 2, or semistable of weight 2 at 2 and $k(\overline{\rho}) = 4$,
- $(p > 2)$ and ρ is a lift of $\overline{\rho}$ to a p-adic representation that is crystalline of weight $k \in [2, p+1]$ at p, or pot.semistable of weight 2 at p,

⌟

Proof: Cf.[Khare-Wintenberger 2].**?** □

4 Serre's Modularity Conjecture

References are [K-W09b], [K-W09c] and [Diamond, F.: The Taylor-Wiles construction and multiplicity one. Invent. Math. 128(2), 379–391 (1997)], [Fujiwara, K.: Deformation rings and Hecke algebras in the totally real case], [Khare, C., Wintenberger, J.-P.: On Serre's conjecture for 2-dimensional mod p representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$], [Kisin, M.: Modularity of 2-adic Barsotti-Tate representations. Invent. Math. (2009)], [Kisin, M.: Moduli of finite flat group schemes, and modularity. Ann. Math], [Edixhoven, Serre's Conjecture, in Fermat's Last Theorem].

Notation (20.9.4.1).
- For $N \in \mathbb{Z}_+$, let $Q(N)$ be a maximal prime factor of N(and $Q(1) = 1$).
- Let $p \in \mathbf{P}, q \in p^{\mathbb{Z}_+}$, and $\overline{\rho} : \mathrm{Gal}_\mathbb{Q} \to \mathrm{GL}(2, \overline{\mathbb{F}_p})$ be a continuous representation.

⌟

Def. (20.9.4.2) [Artin Conductor and Weights of $\overline{\rho}$]. $k(\overline{\rho}), N(\overline{\rho})$. Cf.[Serre, Modular Representations, Section1.2, 2]**?**. ⌟

Thm. (20.9.4.3) [Serre's Modularity Conjecture, Khare-Kisin-Wintenberger]. Any odd smooth absolutely irreducible representation $\overline{\rho}$(such a representation is said to be of **Serre-type**) is modular(20.9.1.3). ⌟

Proof: Cf.[Khare-Wintenberger]Thm9.1**?** □

Lemma (20.9.4.4). Serre's modularity conjecture(20.9.4.3) is true for the following two cases:

- $p \neq 2$ and $2 \nmid N(\overline{\rho})$.
- $p = 2$ and $k(\overline{\rho}) = 2$.

⌟

Proof: (D_0)(20.9.4.8) follows from the truth of (L_r)(20.9.4.7) for each r. Then the assertion follows from(20.9.4.8) and (D_0). □

Lemma (20.9.4.5). Let $\rho : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}(2, \mathcal{O})$ be a continuous odd irreducible representation s.t.

- $\overline{\rho}$ has non-solvable image, and $\overline{\rho}$ is modular.
- ρ is of weight 2, a.e. unramified, and potentially crystalline at p.

Then ρ is modular. ⌟

Proof: Cf.[Khare-Wintenberger]Hypothesis H.**?** □

Def. (20.9.4.6) [Locally Good Dihedral Reoresentations]. $\ell \in \mathbf{P} \backslash \{p\}$ is called a **good dihedral prime** for $\overline{\rho}$ if

- $\overline{\rho}|_{I_\ell}$ is of the form $\begin{bmatrix} \psi & \\ & \psi^\ell \end{bmatrix}$, where $\psi \neq \mathbb{1} \in \chi(I_\ell)$ is of order a power of an odd prime t, s.t. $t | \ell + 1$, and $t > \max(Q(\frac{N(\overline{\rho})}{q^2}), 5, p)$.
- $q \equiv 1 (\mathrm{mod}\ 8)$, and $q \equiv 1 (\mathrm{mod}\ r)$ for any $r \leq \max(Q(\frac{N(\overline{\rho})}{q^2}), p) \in \mathbf{P}$.

If there exists a good dihedral prime q for $\overline{\rho}$, then $\overline{\rho}$ is called **locally good-dihedral** or q-dihedral. ⌟

Lemma (20.9.4.7). For $r \in \mathbb{Z}_+$, consider the following statements:

(L_r) : If $\overline{\rho}$ is of Serre-type(20.9.4.3) and satisfies

- $\overline{\rho}$ is locally good-dihedral(20.9.4.6),
- $k(\overline{\rho}) = 2$ or $p \neq 2$,
- $N(\overline{\rho})$ is odd and divisible by at most r different primes.

Then $\overline{\rho}$ is modular.

(W_r) : If $\overline{\rho}$ is of Serre-type and satisfies

- $\overline{\rho}$ is locally good-dihedral(20.9.4.6),
- $k(\overline{\rho}) = 2$,
- $N(\overline{\rho})$ is odd and divisible by at most r different primes.

Then $\overline{\rho}$ is modular.

Then

- (W_1) is true.
- (Killing ramification in weight 2)(L_r) implies (W_{r+1}).
- (Reduction to weight 2)(W_r) implies (L_r).

In particular, by induction spirally, all $(L_r),(W_r)$ are true. ⌟

Proof: Cf.[Khare-Wintenberger]Thm3.1, 3.2, 3.3.?

2: As L_r clearly implies W_r, it suffices to consider the case $N(\overline{\rho})$ has exactly $r+1$ different primes. Suppose $q\in\mathbf{P},\overline{\rho}$ is q-dihedral, and $s\in\mathbf{P},s|N(\overline{\rho}),s\neq q$. □

Lemma (20.9.4.8) [Level-Rising]. For $r\in\mathbb{N}$, if the following:

(D_r) $\overline{\rho}$ is modular If $\overline{\rho}$ is of Serre-type and satisfies

- $\overline{\rho}$ is locally good-dihedral,
- $p\in\mathbf{P}\setminus\{2\}$,
- $2^{r+1}\nmid N(\overline{\rho})$.

is true, then we have: $\overline{\rho}$ is modular if $\overline{\rho}$ is of Serre-type and satisfies

- $k(\overline{\rho})=2$ or $p\neq 2$ or $r\neq 0$,
- $2^{r+1}\nmid N(\overline{\rho})$,

⌟

Proof: Cf.[Khare-Wintenberger]Thm3.4.? □

Thm. (20.9.4.9) [Compatible Lifting]. Suppose $\overline{\rho}$ is of Serre-type s.t.

- (if $p=2$)$\overline{\rho}$ has non-solvable image,
- (if $p\neq 2$)$k(\overline{\rho})\in[2,p+1]$ and $\overline{\rho}|_{\mathbb{Q}(\mu_p)}$ is absolutely irreducible.

Then $\overline{\rho}$ lifts to an E-rational almost strictly compatible, irreducible, odd Galois representation of $\mathrm{Gal}_{\mathbb{Q}}$ satisfying the following:

-

⌟

<u>**Applications**</u>

5 Conjectures

Prop. (20.9.5.1)[Properties of Étale Cohomologies]. Let $F\in\mathtt{NField}$ and $X\in\mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}^d/F,p\in\mathbf{P}$.

- (E5): If $v\notin\Sigma_F^p$ and X has good reduction at v, then $\mathrm{H}^i_{\text{ét}}(X,\mathbb{Q}_p)|_{\mathrm{Gal}_{F_v}}\in\mathrm{Rep}^{\mathrm{ur}}_{\mathbb{Q}_p}(\mathrm{Gal}_{F_v})$, and
$$P_{v,X}(T)=\det(1-\mathrm{Frob}_v T|\mathrm{H}^i_{\text{ét}}(X,\mathbb{Q}_p))\in\mathbb{Z}[T]$$
is independent of p prime to v. And all roots of $P_{v,X}(T)$ in $\mathbb{C}$ has absolute value $q_v^{-i/2}$.
- (E6): Genuine geometric representations are geometric. And for $v\in\Sigma_F^p$, if X has good reduction at v, $\mathrm{H}^i_{\text{ét}}(X,\mathbb{Q}_p)|_{\mathrm{Gal}_{F_v}}$ is even crystalline.
- (E7): There is a cycle map
$$\eta_\ell:\mathrm{CH}^i(X)\to(\mathrm{H}^{2i}_{\text{ét}}(X,\mathbb{Q}_\ell)(i))^{\mathrm{Gal}_K}.$$
and for $P\in X(K)$, $\eta_\ell(P)\neq 0\in(\mathrm{H}^{2d}_{\text{ét}}(X,\mathbb{Q}_p)(d))^{\mathrm{Gal}_K}$.

And there are some open conjectures:

- (EC1)[Semisimplicity of Frobenius]: Suppose X has good reduction on v,
  - If $v\notin\Sigma_F^p$, then Frob_v acts semi-simply on $H^i(X,\mathbb{Q}_p)$.
  - if $v\in\Sigma_F^p$, then Frob_v acts semi-simply on $D_{\mathrm{crys}}(H^i(X,\mathbb{Q}_p)|_{\mathrm{Gal}_{F_v}})$.

- (EC2)[Grothendieck-Serre]: $H^i(X, \mathbb{Q}_p)$ is a semisimple Gal_F-representation.
- (EC3)[Tate's Conjecture]: η_ℓ is surjective. There are variant of this conjecture:
  There is a decomposition $H^i(X(\mathbb{C}), \overline{\mathbb{Q}}) = \oplus M_j$ as $\overline{\mathbb{Q}}$-vector spaces s.t.
  - For any $\ell \in \mathbf{P}$ and an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \mathbb{Q}_\ell$, $M_j \otimes_{\overline{\mathbb{Q}},\iota} \overline{\mathbb{Q}}_\ell$ is a minimal $\mathrm{Gal}_{G_{\mathbb{Q}_p}}$-stable $\overline{\mathbb{Q}}_\ell$-space.
  - There are Weil-Deligne representations $WD_p(W_j)$ over $\overline{\mathbb{Q}}$ s.t. for any $\ell \in \mathbf{P}$ and an embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \mathbb{Q}_\ell$,
  $$WD_p(M_j) \otimes_{\overline{\mathbb{Q}},\iota} \overline{\mathbb{Q}}_\ell \cong WD_p(M_j \otimes_{\overline{\mathbb{Q}},\iota}, \overline{\mathbb{Q}}_\ell).$$
  - There are motivic weights H-T(M_j) s.t. for any $\ell \in \mathbf{P}$ and $\iota : \mathbb{Q} \hookrightarrow \mathbb{Q}_\ell$,
  $$\text{H-T}(M_j \otimes_{\overline{\mathbb{Q}},\iota} \overline{\mathbb{Q}}_\ell) = \text{H-T}(M_j).$$
  and for any $\iota : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$,
  $$\dim_{\mathbb{C}}(M_j \otimes_{\overline{\mathbb{Q}},\iota} \mathbb{C}) \cap H^{a,i-a}(X(\mathbb{C}), \mathbb{C})$$
  equals the multiplicity of a in H-T(M_j).

⌟

Conj. (20.9.5.2) [Fontaine-Mazur]. For $F \in \texttt{NField}$, any irreducible geometric representation is genuine geometric(20.9.2.1). ⌟

Proof: Emerton and Kisin proved the two-dimensional case, Cf.[The Fontaine-Mazur conjecture for GL(2), Kisin], [Emerton, Local-Global Compatibility in the p-adic Langlands Programme for $\mathrm{GL}(2)_{\mathbb{Q}}$]**?**. □

Remark (20.9.5.3). It follows from proper base change(8.4.3.1) and(8.4.7.36)(17.11.2.1) that any such cohomology group satisfies the requirement.

This conjecture is very strong, for example, the étale cohomology of smooth proper varieties are known to satisfy many good properties, like Weil conjecture, and Fontaine-Mazur conjecture implies that those properties can be derived via linear algebra data.

The local version of this conjecture is known to be false. ⌟

Def. (20.9.5.4) [Algebraic Representations]. $(\rho, V) \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_F)$ is called an **algebraic representation** if
$$P_{v,X}(T) = \det(1 - \mathrm{Frob}_v T | H^i(X, \mathbb{Q}_p)) \in \overline{\mathbb{Q}}[T].$$
And it is moreover called **pure of weight** w if for a.e. $v \in \Sigma_F$, eigenvalues of $\rho(\mathrm{Frob}_v)$ are all Weil integers of weight w. And w is called the **motivic weight** of V. ⌟

Prop. (20.9.5.5). If $F_0 \subset F$ is a subfield, and $V \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_K)$ is pure of weight w, then if $W = \mathrm{Ind}_{\mathrm{Gal}_F}^{\mathrm{Gal}_{F_0}}(V)$, W is also pure of weight w. ⌟

Proof: **?** □

Prop. (20.9.5.6) [Total Hodge-Tate Weights]. For a geometric representation $V \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_F)$, for each $v \in \Sigma_F^v$, there are Hodge-Tate weights associated to v. For $k \in \mathbb{Z}$, define

$$m_k(V) = \sum_{v \in \Sigma_F^p} [F_v : \mathbb{Q}_p] m_k(V|_{\mathrm{Gal}_{F_v}}),$$

called the **total Hodge-Tate weights** of V. Then it satisfies:

- $\sum_{k\in\mathbb{Z}} m_k(V) = [F : \mathbb{Q}] \dim V$.
- For a subfield $F_0 \subset F$, if $W = \mathrm{Ind}_{\mathrm{Gal}_F}^{\mathrm{Gal}_{F_0}}(V)$, then $m_k(V) = m_k(W)$.?
- If V is pure of weight w, then

$$w[F : \mathbb{Q}] \dim V = 2 \sum_{k\in\mathbb{Z}} m_k \cdot k.$$

⌟

Proof: 1 is clear.

2: ?

3: By item2 and(20.9.5.5), it suffices to show for $F = \mathbb{Q}$. Secondly, it suffices to show for $\det V$, it has motivic weight $w \dim V$ and for each $v \in \Sigma_F^p$ the unique Hodge-Tate weights equal to the sum of Hodge-Tate weights of V. Then we may assume it has weight 0 by Tate twist because Hodge-tensoring by $\mathbb{Q}_p(k)$ increases both sides by $-2k$.

Then by Sen's theory, $V|_{\mathrm{Gal}_{\mathbb{Q}_p}}$ is potentially unramified. Let χ be the Hecke character attached to V, then its kernel contains an open subgroup $U_p \subset \mathbb{Z}_p^\times$, and also by small circle argument, it contains an open subgroup $U^p \subset \prod_{\ell\neq p} \mathbb{Z}_\ell^\times$, and it also contains $\mathbb{R}_+^\times$ by(14.6.3.27). But notice $\mathbf{I}_{\mathbb{Q}}^* / \mathbb{Q}^\times U_p U^p \mathbb{R}^\times$ is finite. Thus it is an Artin representation, and has motivic weight 0(20.9.5.4), □

Prop. (20.9.5.7) [Symmetry of Hodge-Tate Weights]. If the Tate conjecture(20.9.5.1) is true, then for any genuine geometric representation V pure of weight w,

- $m_k = m_{w-k}$.
- If $w \in 2\mathbb{Z}$, let $m_{w/2}^{\pm}(V)$ be defined by

$$m_{w/2}^+(V) + m_{w/2}^-(V) = m_{w/2}(V)$$

$$m_{w/2}^+(V) - m_{w/2}^-(V) = (-1)^{w/2}(\dim V^{\mathsf{c}=\mathrm{id}} - \dim V^{\mathsf{c}=-\mathrm{id}}).$$

  Then $m_{w/2}^{\pm}(V) \in \mathbb{N}$.
- For a subfield $F_0 \subset F$, $m_{w/2}^{\pm}(V) = m_{w/2}^{\pm}(\mathrm{Ind}_{\mathrm{Gal}_F}^{\mathrm{Gal}_{F_0}}(V))$.

⌟

Polarized Representations

Def. (20.9.5.8) [Polarized Representations]. V is called a **polarized Galois representation** if $V^\vee \cong V(w)$ for some $w \in \mathbb{Z}$. w is called the weight of the polarization. If V is polarized and pure, then the motivic weight equals the polarization weight, so there will be no confusion. ⌟

Prop. (20.9.5.9). If $F/\mathbb{Q}$ is Galois, and V, V' are two irreducible geometric representation of Gal_F s.t. $L(V; s) = L(V'; s)$, then $V' \cong V$. ⌟

Proof: This is because $L(V;s)$ determines $WD_v(V)$ for all v that is unramified. Thus also determines V by Chebotarev density theorem**?**. □

Example (20.9.5.10) [Polarized Representations].

- Any 1-dimensional representation is polarized.
- $V_p(A)$ of an Abelian variety is polarized of weight 1.
- Representations attached to a classical modular eigenform in $S_{2k}(\Gamma_0(N))$ is polarized of weight $2k-1$.
- For an irreducible polarized representation of $\mathrm{Gal}_{\mathbb{Q}}$ of dimension 2, its weight is odd iff V is odd.

⌟

Proof: **?** □

21 L-Functions

21.1 Eisenstein Series

1 Non-Holomorphic Eisenstein Series

References are [Bump, Chap3] and [Diamond]Chap4.10.

Def. (21.1.1.1)[Non-Holomorphic Eisenstein Series]. The **non-holomorphic Eisenstein series** of weight s is defined to be

$$E^*(z,s)=\frac{1}{2}L_{\mathbb{R}}(2s)\sum_{(m,n)\neq 0\in\mathbb{Z}^2}\frac{(\mathrm{Im}(z))^s}{|mz+n|^{2s}}=L_{\mathbb{R}}(2s)\sum_{\gamma\in\overline{\Gamma_\infty}\backslash\overline{\Gamma(1)}}(\mathrm{Im}(\gamma(z)))^s$$

It is absolutely convergent for $\mathrm{Re}(s)>1$, and is automorphic for $\Gamma(1)$(20.1.1.11). ⌟

Prop. (21.1.1.2)[Fourier Expansion of $E(z,s)$]. The Fourier coefficients of $E(z,s)$ is of the form

$$E^*(z,s)=\sum_{n=-\infty}^{\infty}a_n(y,s)e^{2\pi irx},$$

where

$$a_0(y,s)=\Lambda(2s)y^s+\Lambda(2-2s)y^{1-s}$$

and for $n\neq 0$,

$$a_n(y,s)=2|n|^{-s+1/2}\sigma_{2s-1}(|n|)\sqrt{y}K_{s-1/2}(2\pi|n|y),$$

where $K_{s-1/2}(z)$ is the K-Bessel function(11.6.3.1). In particular,

$$E^*(z,s)=\Lambda(2s)y^s+\Lambda(2-2s)y^{1-s}+4\sqrt{y}\sum_{n\in\mathbb{Z}_+}n^{\frac{1}{2}-s}\sigma_{2s-1}(n)K_{s-\frac{1}{2}}(2\pi ny)\cos(2\pi nx)$$

⌟

Proof:

$$a_r(y,s)=\int_0^1 E^*(x+iy,s)e^{-2\pi irx}dx=\int_0^1\frac{1}{2}\pi^{-s}\Gamma(s)\sum_{(m,n)\neq 0\in\mathbb{Z}^2}\frac{y^s}{|mz+n|^{2s}}e^{-2\pi irx}dx.$$

The term with $m=0$ only contributes to a_0, and equals $\pi^{-s}\Gamma(s)\zeta(2s)y^s$. For the rest we may assume $m>0$ by symmetry, then they contributes to

$$\pi^{-s}\Gamma(s)y^s\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}\int_0^1[(mx+n)^2+m^2y^2]^{-s}e^{-2\pi irx}dx$$

$$= \pi^{-s}\Gamma(s)y^s \sum_{m=1}^{\infty} \sum_{n \mod m} \int_{-\infty}^{\infty} [(mx+n)^2 + m^2y^2]^{-s} e^{-2\pi i r x} dx$$
$$= \pi^{-s}\Gamma(s)y^s \sum_{m=1}^{\infty} m^{-2s} \sum_{n \mod m} e^{2\pi i r n/m} \int_{-\infty}^{\infty} (x^2+y^2)^{-s} e^{-2\pi i r x} dx$$

Notice $\sum_{n \mod m} e^{2\pi i r n/m} = \begin{cases} m & m|r \\ 0 & \text{otherwise} \end{cases}$, thus the calculation reduces to(11.6.3.5). □

Prop. (21.1.1.3) [Functional Equation]. $E^*(z,s)$ has meromorphic continuation to all $s \in \mathbb{C}$, and it is analytic except at $s=1$ or $s=0$, where the residue at $s=1$ is $1/2$ for any z, and it satisfies the functional equation

$$E^*(z,s) = E^*(z,1-s).$$

and $E(x+\mathrm{i}\,y,s) = O(y^\sigma)$ for $y \to \infty$, where $\sigma = \max(\mathrm{Re}(s), 1-\mathrm{Re}(s))$. ⌟

Proof: This follows from the Fourier expansion of $E^*(z,s)$(21.1.1.2). Each term $a_r(y,s)$ has analytic extension to all s, except that a_0 has simple poles at $s=0$ and $s=1$ by(21.4.2.5)(the pole at $s=1/2$ was neutralized). And the functional equation and the convergence is clear from the properties of K-Bessel functions(11.6.3.2). For the residue, it suffices to show the residue of $\pi^{-s/2}\Gamma(s/2)\zeta(s)$ at 0 is -1(21.4.2.5). □

Prop. (21.1.1.4) [Kronecker's First Limit Formula].

$$2E^*(z,s) = \frac{1}{s-1} + \gamma_0 - \log(4\pi y|\eta(z)|^4) + O(s-1).$$

And a similar formula is true for $s=0$, by the functional equation(21.1.1.3). ⌟

Proof: Cf.[Kronecker's First Limit Formula, Revisited]. □

Prop. (21.1.1.5) [Eisenstein Series of Mixed Type]. The **Eisenstein series of mixed type** is defined to be

$$E_{k,s}(z) = \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{y^s}{(mz+n)^k|mz+n|^{2s}}, k \in \mathbb{Z}, s \in \mathbb{C}.$$

Then

$$R_k(y^{k/2}E_{k,s}(z)) = (k+s)y^{(k+2)/2}E_{k+2,s}(z).$$

and $y^{k/2}E_{k,s}(z)$ is a Maass form in (z) of weight k. Its better to consult the paper https://arxiv.org/abs/1803.08210 for the Fourier expansion of $E_{k,s}$. ⌟

Proof:

$$((z-\bar{z})\frac{\partial}{\partial z} + k/2)[\frac{(\frac{z-\bar{z}}{2i})^{s+k/2}}{(mz+n)^{s+k}(m\bar{z}+n)^s}]$$
$$= (z-\bar{z})(\frac{\frac{s+k/2}{2i}(\frac{z-\bar{z}}{2i})^{s-1+k/2}(mz+n)^{s+k} - (\frac{z-\bar{z}}{2i})^{s+k/2}m(s+k)(mz+n)^{s+k-1}}{(m\bar{z}+n)^s(mz+n)^{2s+2k}}) + \frac{k}{2}\frac{(\frac{z-\bar{z}}{2i})^{s+k/2}}{(mz+n)^{s+k}(m\bar{z}+n)^s}$$
$$= \frac{(\frac{z-\bar{z}}{2i})^{s+k/2}}{(mz+n)^{s+k+1}(m\bar{z}+n)^s}[(s+k/2)(mz+n) - (z-\bar{z})m(s+k) + \frac{k}{2}(mz+n)]$$

$$= (k+s)\frac{(\frac{z-\bar{z}}{2i})^{s-1+(k+2)/2}}{(mz+n)^{s+k+1}(m\bar{z}+n)^{s-1}}$$
$$= (k+s)y^{(k+2)/2}E_{k+2,s-1}(z)$$

□

Prop. (21.1.1.6) [Rankin-Selberg]. Let $\varphi \in C^\infty(\Gamma(1)\backslash\mathscr{H})$ be decreasing rapidly along $y \to \infty$ and $\varphi(z) = \sum_{n\in\mathbb{Z}} \varphi_n(y)e^{2\pi inx}$ be its Fourier expansion. Call φ_0 the constant term of φ. Consider the Mellin transform

$$M(s,\varphi_0) = \int_0^\infty \varphi_0(y)y^s\frac{dy}{y}(11.11.2.16), \quad \Lambda(s,\varphi_0) = \Lambda(2s)M(s-1,\varphi_0).$$

As $\varphi(s,\varphi_0)$ is bounded as a function on y and decay rapidly, $M(s,\varphi)$ is absolutely convergent for $\mathrm{Re}(s) > 0$.

Then

$$\Lambda(s,\varphi_0) = \int_{\Gamma(1)\backslash\mathscr{H}} E^*(z,s)\varphi(z)\frac{dxdy}{y^2}$$

and thus has a meromorphic continuation to all s and satisfies a functional equation, with at most simple poles at $s = 0$ or 1,

$$\mathrm{Res}_{s=1}\Lambda(s,\varphi_0) = \frac{1}{2}\int_{\Gamma(1)\backslash\mathscr{H}} \varphi(z)\frac{dxdy}{y^2}.$$

⌟

Proof: Using(21.1.1.1),

$$\begin{aligned}\int_{\Gamma(1)\backslash\mathcal{H}} \varphi(z)\frac{dxdy}{y^2} &= \Lambda(2s)\sum_{\gamma\in\overline{\Gamma_\infty}\backslash\overline{\Gamma(1)}}\int_{\overline{\Gamma(1)}\backslash\mathcal{H}}(\mathrm{Im}(\gamma(z)))^s\varphi(\gamma(z))\frac{dxdy}{y^2}\\ &= \Lambda(2s)\int_{\Gamma_\infty\backslash\mathcal{H}}\mathrm{Im}(z)^s\varphi(z)\frac{dxdy}{y^2}\\ &= \Lambda(2s)\int_0^\infty y^{s-1}\int_0^1\varphi(x+\mathrm{i}\,y)dx\frac{dy}{y}\\ &= \Lambda(2s)\int_0^\infty \varphi_0(y)y^{s-1}\frac{dy}{y}\\ &= \Lambda(s,\varphi_0)\end{aligned}$$

The assertion about the meromorphic continuation and the residue follows from the equation above and(21.1.1.3). □

21.2 L-Functions Attached to Motives

Main references are [Conjectures in Arithmetic Algebraic Geometry, Hulsbergen, 1992], [Galois Representations, ICM, Taylor].

Notation (21.2.0.1).

- Use notations defined in .

⌟

Remark (21.2.0.2). In short, nineteenth century number theory showed that much, if not all, of number theory is reflected by properties of L-functions. ⌟

1 Artin L-Functions

References are [On the Functional Equation of the Artin L-Functions, Langlands], [On Artin L-Functions, Cogdell], [Deligne's 1973 Paper]. [Neu99].

Weil Representations

Thm. (21.2.1.1) [Weil L-Factors]. For any local field K and a non-trivial additive character ψ of K, there exists a group homomorphism

$$\varepsilon(\cdot,\psi):K_0(\mathfrak{wd}(W_K))\to\mathbb{C}^\times$$

that satisfy

- For a quasi-character χ, $\varepsilon(\chi,\psi)$ agrees with local factor given by Tate thesis.
- If E/F is a finite extension, and ρ is a representation of W_E, then

$$\varepsilon(\operatorname{ind}_{W_E}^{W_F}\rho,\psi_F)=\lambda(E/F,\psi_F)^{\dim\rho}\varepsilon(\rho,\psi_F\circ\operatorname{tr}_{E/F}).$$

⌟

Proof: Cf.[Functional Equation for Artin L-Functions, Langlands] and [Tate, Number Theoretical Background]. □

Def. (21.2.1.2) [Weil-Deligne L-Factors]. Let $K\in p\text{-}\mathtt{NField}$ and $\rho=(\rho_0,N)\in\mathfrak{wd}(W_K)$, we define

- the conductor $\mathfrak{f}(\rho)=\mathfrak{f}(\rho_0)+\dim(V^{I_K}/\ker(N)^{I_K})$, where $\mathfrak{f}(\rho_0)$ is the Artin conductor(18.3.2.16).
- the local L-factor

$$L(\rho,s)=\det(1-q^{-s}\operatorname{Frob}_\kappa\,|\ker(N)^{I_K})^{-1}.$$

- the local ε-factor

$$\varepsilon(\rho,s,\psi)=q^{-(c(\rho)+n(\psi)\dim V)s}\det(-\varphi|V^{I_K}/\ker(N)^{I_K})\varepsilon(\rho',\psi).$$

⌟

Prop. (21.2.1.3). $\varepsilon(\rho\otimes\omega_s,\psi)=q^{-(c(\rho)+n(\psi)\dim V)s}\varepsilon(\rho,\psi)$. ⌟

Proof: □

Artin L-Functions

Def. (21.2.1.4) [Local Artin L-Factors]. For a Galois extension $L/F \in$ NField and $\rho \in \mathrm{Rep}(\mathrm{Gal}(L/F))$, the local L-factors(21.2.1.2) are:

$$L_v(F,\rho;s) = \begin{cases} (\det(1-||v||^{-s}\rho(\varphi_{\mathfrak{P}/\mathfrak{p}})|V^{I_{\mathfrak{P}}}))^{-1} & , v\in\Sigma_F^{\mathrm{fin}} \\ L_{\mathbb{C}}(s)^{\chi(1)} & , v\in\Sigma_F^{\mathbb{C}} \\ L_{\mathbb{R}}(s)^{n_+}\cdot L_{\mathbb{R}}(s+1)^{n_-} & , v\in\Sigma_F^{\mathbb{R}}\text{(21.3.3.1)} \end{cases}$$

where in the case $v\in\Sigma_F^{\mathrm{fin}}$, $\mathfrak{P}$ is a prime over $\mathfrak{p}=\mathfrak{p}_v$, and in the case $v\in\Sigma_F^{\mathbb{R}}$, let $\mathfrak{p}=\mathfrak{p}_v,\mathfrak{P}$ be any place of L over $\mathfrak{p}$, and let $\mathfrak{c}_{\mathfrak{P}}$ be the generator of $\mathrm{Gal}(L_{\mathfrak{P}}/F_{\mathfrak{p}})$, then

$$n_+ = \frac{\chi(1)+\chi(\mathfrak{c}_{\mathfrak{P}})}{2},\quad n_- = \frac{\chi(1)-\chi(\mathfrak{c}_{\mathfrak{P}})}{2}.$$

⌟

Prop. (21.2.1.5)[Functoriality of Artin L-Factors]. For a Galois extension of global fields L/F and $(\rho,V)\in\mathrm{Rep}(\mathrm{Gal}(L/F)), v=v_{\mathfrak{p}}\in\Sigma_F$, The Artin L-factors(21.2.1.4) satisfy the following functorial properties:

- $L_v(F,\mathbb{1};s) = L_v(\mathbb{1};s)$**?**.
- For $\rho,\rho'\in\mathrm{Rep}(\mathrm{Gal}(L/F))$, $L_v(F,\rho\oplus\rho';s) = L_v(F,\rho;s)L_v(F,\rho';s)$.
- For Galois extensions $L'/L/K$ and $\rho\in\mathrm{Rep}(\mathrm{Gal}(L/F))$, $L(L'/F,\rho;s) = L(L/F,\rho;s)$.
- If $F\subset M\subset L$, $\rho\in\mathrm{Rep}(\mathrm{Gal}(L/M))$, then $L_{\mathfrak{p}}(F,\mathrm{Ind}_{\mathrm{Gal}(L/F)}^{\mathrm{Gal}(L/M)}(\rho);s) = \prod_{\mathfrak{q}|\mathfrak{p}} L_{\mathfrak{q}}(M,\rho;s)$.

⌟

Proof: **?**

1, 2, 3 are clear.

For 4: Let $G=\mathrm{Gal}(L/F), H=\mathrm{Gal}(L/M)$, for any $\mathfrak{p}\in\Sigma_F^{\mathrm{fin}}$, let $\{\mathfrak{q}_1,\ldots,\mathfrak{q}_r\}=S(\mathfrak{p})\subset\Sigma_M^{\mathrm{fin}}$, and take $\mathfrak{P}_i\in\Sigma_L^{\mathrm{fin}}$ over $\mathfrak{q}_i$. Let G_i, I_i be the decomposition and inertia groups of $\mathfrak{P}_i/\mathfrak{p}$, then $H_i=G_i\cap H, I_i'=I_i\cap H$ are the decomposition and inertia groups of $\mathfrak{P}_i/\mathfrak{q}_i$. Denote f_i the inertia degree of $\mathfrak{q}_i/\mathfrak{p}$. Let $(\rho,W)\in\mathrm{Rep}(\mathrm{Gal}(L/M)), (\rho',V)=\mathrm{Ind}_{\mathrm{Gal}(L/F)}^{\mathrm{Gal}(L/M)}(\rho)\in\mathrm{Rep}(\mathrm{Gal}(L/F))$, then it suffices to show that

$$\det(1-\varphi_{\mathfrak{P}_1/\mathfrak{p}}T|V^{I_1}) = \prod_{i=1}^r \det(1-\varphi_{\mathfrak{P}_i/\mathfrak{p}}^{f_i}T^{f_i}|W^{I_i'}).$$

If $\mathfrak{P}_i=\tau_i^{-1}(\mathfrak{P}_1)$, then we can take $\varphi_{\mathfrak{P}_i/\mathfrak{p}}=\tau_i^{-1}\varphi_{\mathfrak{P}/\mathfrak{p}}\tau_i, I_i=\tau_i^{-1}I\tau_i$, then

$$\det(1-\varphi_{\mathfrak{P}_i/\mathfrak{p}}^{f_i}T^{f_i}|W^{I_i'}) = \det(1-\varphi_{\mathfrak{P}_1/\mathfrak{p}}^{f_i}T^{f_i}|W^{I_1\cap\tau_i H\tau_i^{-1}}),$$

and $f_i=(G_i:H_iI_i)=(G_1:(G_1\cap\tau_iH\tau_i^{-1})I_1)$.

Let σ_{ij} be a representative of $G_1/(G_1\cap\tau_iH\tau_i^{-1})$, then because $G/H=\cup_i G_i/H_i$, $\{\sigma_{ij}\tau_i\}_{ij}$ is a representative of G/H. Then

$$V=\oplus_i(\bigoplus_j \sigma_{ij}\tau_i W),$$

and $V_i=\bigoplus_j\sigma_{ij}\tau_iW=\mathrm{Ind}_{G_1\cap\tau_iH\tau_i^{-1}}^{G_1}(\tau_iW)$ is a G_1-module. So

$$\det(1-\varphi_{\mathfrak{P}_1/\mathfrak{p}}T|V^{I_1}) = \prod_{i=1}^r\det(1-\varphi_{\mathfrak{P}_1/\mathfrak{p}}T|V_i^{I_1})$$

Then it suffices to prove for each i,

$$\det(1-\varphi_{\mathfrak{P}_1/\mathfrak{p}}T|V_i^{I_1})=\det(1-\varphi_{\mathfrak{P}_i/\mathfrak{p}}^{f_i}T^{f_i}|W^{I_i'}).$$

Notice

$$V_i^{I_1}=\Big(\mathrm{Ind}_{G_1\cap\tau_iH\tau_i^{-1}}^{G_1}(\tau_iW)\Big)^{I_1}=\mathrm{Ind}_{H_i}^{G_i}W^{I_i'}(18.1.5.40)=\bigoplus_{i=0}^{f_i-1}\varphi_{\mathfrak{P}_i/\mathfrak{p}}^{i}W^{I_i'},$$

so the assertion follow easily from this. □

Def. (21.2.1.6) [Artin L-Functions]. Let $L/F\in$ `GField` be Galois, and $(\rho,V)\in\mathrm{Rep}(\mathrm{Gal}(L/F))$, the **Artin L-function** of ρ is defined to be the Euler product of local L-factors(21.2.1.4)

$$L(F,\rho;s)=\prod_{v\in\Sigma_F^{\mathrm{fin}}}L_v(F,\rho;s).$$

This L-function also only depends on F but not L, as we will see in(21.2.1.7).

And also define the **completed Artin L-function** as the function

$$\Lambda(F,\rho;s)=\prod_{v\in\Sigma_F}L_v(F,\rho;s).$$

⌟

Prop. (21.2.1.7) [Functoriality of Artin L-Functions]. Let $L/F\in$ `GField` be Galois and $(\rho,V)\in\mathrm{Rep}(\mathrm{Gal}(L/F))$, The L-functions satisfy the following functorial properties:

- $L(F,\mathbb{1};s)=\zeta(F;s)$(21.4.3.1).
- For $\rho,\rho'\in\mathrm{Rep}(\mathrm{Gal}(L/F))$, $L(F,\rho\oplus\rho';s)=L(F,\rho;s)L(F,\rho';s)$.
- For Galois extensions $L'/L/K$ and $\rho\in\mathrm{Rep}(\mathrm{Gal}(L/F))$, $L(L'/F,\rho;s)=L(L/F,\rho;s)$.
- If $F\subset M\subset L$, $\rho\in\mathrm{Rep}(\mathrm{Gal}(L/M))$, then $L(F,\mathrm{Ind}_{\mathrm{Gal}_M}^{\mathrm{Gal}_F}(\rho);s)=L(M,\rho;s)$.

⌟

Proof: These follow from(21.2.1.5). □

Cor. (21.2.1.8). For a finite Galois extension L/F,

$$\zeta(L;s)=\zeta(F;s)\cdot\Big(\prod_{\rho\neq\mathbb{1}\in\mathrm{Irr}(\mathrm{Gal}(L/F))}L(F,\rho;s)^{\chi_\rho(1)}\Big)$$

⌟

Prop. (21.2.1.9) [Artin L-Functions and Weber L-Functions]. Let $L/F\in$ `GField` be Abelian and Galois with conductor $\mathfrak{f}$, and $\chi\in\chi(\mathrm{Gal}(L/F))$, composing with the Artin symbols(14.6.4.26), we get a character $\widetilde{\chi}:C_F/C^{\mathfrak{f}}\cong J^{\mathfrak{f}}/P^{\mathfrak{f}}\to\mathrm{Gal}(L/F)\xrightarrow{\chi}\mathbb{C}^\times$, which is a Dirichlet character. Then we have

$$L(F,\chi;s)=\prod_{\mathfrak{p}\in S}\frac{1}{1-\chi(\varphi_{\mathfrak{P}/\mathfrak{p}})(N\mathfrak{p})^{-s}}L(F,\widetilde{\chi};s)(21.4.2.3),$$

where $S=\{\mathfrak{p}\in S_f(\mathfrak{f})|\chi(I_{\mathfrak{P}})=1\}$. Moreover, if χ is injective, then $S=\varnothing$. ⌟

Proof: S are the primes that are ramified in L/F and $\mathbb{C}(\chi)^{I_{\mathfrak{P}}}\neq 0$. □

Functional Equations

Prop. (21.2.1.10) [Functional Equations, Brauer]. By Brauer theorem(18.1.3.33) and(18.1.3.33), the Artin L-functions can be written as products and inverses of Weber L-functions(21.4.2.3) and f.m. L-factors. In particular, they can be extended meromorphically to all $s \in \mathbb{C}$ and satisfies a functional equation(21.4.2.5). But the ε-factor remains mysterious**?**.

More explicitly, for a Galois extension of global fields L/F and $(\rho, V) \in \mathrm{Rep}(\mathrm{Gal}(L/F))$, the completed Artin L-function satisfies a functional equation

$$\Lambda(F, \rho; s) = \varepsilon(\rho; s)\Lambda(\rho^\vee; 1 - s),$$

where

$$\varepsilon(\rho) = w(\rho)\Big(|d_F|^{\chi_\rho(1)}||\mathfrak{f}(F, \rho)||\Big)^{1/2-s} \text{(18.3.2.16)}$$

and $w(\rho)$ is a root number, which satisfies $|w(\rho)| = 1$. ⌟

Proof: Cf.[Algebraic Number Theory, Neukirch].**?** □

Conj. (21.2.1.11)[Artin]. If $F \in \texttt{GField}$ and $(\rho, V) \in \mathrm{Rep}^{\mathrm{fd}}(\mathrm{Gal}_F)$ satisfies $V^{\mathrm{Gal}_F} = 0$, then $L(F, \rho; s)$ is an entire function w.r.t. $s \in \mathbb{C}$. ⌟

Proof: □

Remark (21.2.1.12). The Artin conjecture is true if $\mathrm{Im}(\rho)$ is solvable, as we can reduce to Abelian case, and use(21.2.1.9) and(21.4.2.5). ⌟

Thm& Conj.Cor. (21.2.1.13) [Langlands-Tunnell]. ⌟

Artin-Weil L-Functions

Cf.[On the Functional Equation of the Artin L-Functions, Langlands].

2 Galois L-Functions

Def. (21.2.2.1) [L-Functions]. Given an isomorphism $\iota : \overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$, for any $V \in \mathrm{Rep}_{\mathbb{Q}_p}(\mathrm{Gal}_F)$, define the global L-function as

$$L(\iota V; s) = \prod_{v \in \Sigma_F^{\mathrm{fin}}} L(\iota\, \mathrm{WD}_p(V); s) \text{(21.2.1.2)}.$$

⌟

Prop. (21.2.2.2). By Chebotarev density theorem, $L(\iota V; s)$ determines $\mathrm{WD}_p(V)$ and thus V up to F-semisimplification. ⌟

Proof: **?** □

Prop. (21.2.2.3). Situation as in(21.2.2.1),

- $L(V(n); s) = L(V; s + n)$.
- If $F_0 \subset F$ is a subfield, $W = \mathrm{Ind}_{\mathrm{Gal}_K}^{\mathrm{Gal}_{K_0}}(V)$, then $L(V; s) = L(W; s)$.
- If V is S-pure of weight w, then $L_S(V; s)$ converges absolutely for $\mathrm{Re}\, s > w/2 + 1$.

- If V is pure of weight w, then $L(V;s)$ is meromorphic for $\mathrm{Re}\, s > w/2+1$ and has no zeros there.

⌟

Proof: 1 is easy.
2: ?
3: Compare with the Dedekind zeta function(21.3.2.1).
4: clear. □

Conj. (21.2.2.4) [Holomorphy]. Situation as in(21.2.2.1), if V is geometric and pure of weight w, then it is totally pure. In particular, it is holomorphic for $\mathrm{Re}\, s > w/2+1$. ⌟

Proof: ?. This should be a consequence of Fontaine-Mazur conjecture and Tate's conjecture. □

Conj. (21.2.2.5) [Meromorphic Extension]. If V is geometric and pure of weight w, then
- $L(V;s)$ admits a meromorphic continuation to all $s\in\mathbb{C}$, and essentially bounded on vertical strips.
- $L(V;s)\neq 0$ for $\mathrm{Re}(s) > w/2+1$.
- If V is irreducible, then $L(V;s)$ has no poles, expect when $V\cong \mathbb{Q}_p(n)$, then it has a simple pole at $s=-n+1$.
- $L(V;w/2+1)\neq 0$.

⌟

Proof: □

Remark (21.2.2.6). This is true when V is automorphic, by Jacquet-Shalika method. ⌟

Conj. (21.2.2.7) [Grand RH Hypothesis]. If V is geometric and pure of weight w, then $L(V;s)$ has no zeros on $\mathrm{Re}\, s > (w+1)/2$. ⌟

Proof: □

Def. (21.2.2.8) [Completed L-Functions]. If V is geometric and pure of weight w, define

$$L_\infty(V;s) = \Gamma_{\mathbb{R}}(s-w/2)^{m^+_{w/2}}.\Gamma_{\mathbb{R}}(s-w/2+1)^{m^-_{w/2}}.\prod_{k\in\mathbb{Z},k<w/2}\Gamma_{\mathbb{C}}(s-k)^{m_k}.$$

and define the **root number at** ∞

$$w_\infty(\rho) = \mathrm{i}^{m^-_{w/2}}.\Big(\prod_{k<w/2}\mathrm{i}^{m_k}\Big)^{2w+1}$$

and the Artin conductor $\mathfrak{f}(\rho)$(18.3.2.16), and the completed L-function

$$\Lambda(V;s) = L(\iota V;s)L_\infty(V;s).$$

and the **root number**

$$w(\iota\rho) = w_\infty(\rho)\prod_{p\in\mathbf{P}} w(\mathrm{WD}_p(\rho);\psi_p)$$

where $\iota\psi_p(x) = e^{-2\pi\,\mathrm{i}\,x}$. ⌟

Prop. (21.2.2.9). If $V \in \mathrm{Rep}_{\overline{\mathbb{Q}}_\ell}(\mathrm{Gal}_\mathbb{Q})$ is geometric and pure of weight w, then

- $L_\infty(V(n); s) = L_\infty(V; s+n)$.
- $L_\infty(V(n); s)$ has a pole of order $\sum_{0\leq k<w/2} m_k + m^+_{w/2}$ at $s = 0$.
- If Tate's conjecture(20.9.5.1) holds, then $m^\pm_{w/2} \geq 0$, so $L_\infty(V(n); s)$ has no zeros.

⌟

Proof: Only 1 deserves a proof: It suffices to prove for $n = 1$. If $w \notin 2\mathbb{Z}$ this is clear. If $w \in 2\mathbb{Z}$, notice Tate twists change weights by 2, so it is also odd, and $(-1)w'/2 = -(-1)^{w/2}$. But also the twist changes the action of c by -1 in(20.9.5.7), so the assertion follows. □

Conj. (21.2.2.10) [Functional Equations]. If V is geometric and pure of weight w, then

$$\Lambda(V; s) = w(V)N(V)^{(w+1)/2-s}\Lambda(V^\vee; 1-s).$$

where $N(V)$ is the conductor of V**?**. ⌟

Proof: □

Remark (21.2.2.11). This is true for V automorphic, by Jacquet-Shalika method.**?** ⌟

Conj.Cor. (21.2.2.12). For a geometric representation polarized of weight w(20.9.5.8), there should be a functional equation

$$\Lambda(V; 1+w-s) = \varepsilon(V; s)\Lambda(V; s).$$

⌟

Proof: □

3 Hasse-Weil L-Functions

References are [Zeta Functions in Algebraic Geometry, Mustata].

Zeta-Functions over Finite Fields

Def. (21.2.3.1) [Zeta-Functions]. Let $p \in \mathbf{P}, q \in p^{\mathbb{Z}_+}$, and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}}/\mathbb{F}_q$, then its **zeta-function** is defined to be the power series

$$Z(X; T) = \exp(\sum_{n\geq 1} \#X(\mathbb{F}_{q^n})\frac{T^n}{n}) \in \mathbb{Q}[[T]].$$

Notice that we can get the information of number of rational points of X by the formula

$$\#X(\mathbb{F}_{q^n}) = \frac{1}{(n-1)!}\frac{d^n}{dT^n}\log Z(X; T)|_{T=0}.$$

⌟

Prop. (21.2.3.2) [Euler Product]. there is an Euler product formula for $Z(X; T)$ by(17.2.2.2)(17.2.2.3):

$$Z(X; T) = \prod_{x \text{ closed in } X} \frac{1}{1 - T^{\deg(x)}}.$$

⌟

Thm. (21.2.3.3) [Rationality of Zeta Functions, Dwork]. Let $p \in \mathbf{P}, q \in p^{\mathbb{Z}_+}$, and $X \in \mathcal{S}\mathrm{ch}^{\mathrm{ft}}/\mathbb{F}_q$, then $Z(X;T) \in \mathbb{Q}(T)$. ⌟

Proof: Cf.[Zeta Functions in Algebraic Geometry, Mustata]**?**. Does this follows from Weil conjecture? □

Thm. (21.2.3.4) [Weil Conjecture1949, Weil/Deligne1974/Laumon]. Let $p \in \mathbf{P}, q \in p^{\mathbb{Z}_+}$, and $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}\mathcal{V}\mathrm{ar}^n/\mathbb{F}_q$, then

1. (Riemann Hypothesis): $Z(X;T)$ is of the form
$$Z(X;T) = \frac{P_1(X;T)P_3(X;T)\dots P_{2n-1}(X;T)}{P_0(X;T)P_2(X;T)\dots P_{2n}(X;T)}$$
s.t.
   - $P_0(X;T) = 1-T$,
   - $P_{2n}(X;T) = 1-q^nT$,
   - For $0 \le i \le 2n$, $P_i(X;T) \in \mathbb{Z}[T]$,
   - For $0 \le i \le 2n$, $P_i(X;T) = \prod_{j\le k}(1-\alpha_{ij}T)$, where each $\alpha_{ij} \in \mathrm{Weil}(q^{i/2})$ is a q-Weil number of weight i(14.4.1.13).
   - $\deg(P_i(X;T))$ is called the **i-th Betti number** of X, and $\deg P_i(X;T) = \deg P_{2n-i}(X;T)$.
2. (Functional Equation):
$$Z(X;\frac{1}{q^nT}) = \pm q^{n\chi/2}T^\chi Z(X;T),$$
where χ is a Euler character $\Delta\cdot\Delta = \sum_{i=0}^{2n}(-1)^i\deg P_i(X;T)$. Notice that $n\chi/2 \in \mathbb{Z}$.
3. If $R \subset \mathbb{C}$ is a f.g. $\mathbb{Z}$-algebra, $\mathfrak{p} \in \mathrm{Spec}(R)$ s.t. $R/\mathfrak{p} \cong \mathbb{F}_q$, and there exists $\mathcal{X} \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}/R$ s.t. $\mathcal{X}_{\kappa(\mathfrak{p})} \cong X$, then $\deg(P_i(X;T))$ equals the i-th Betti number of $\mathcal{X}_{\mathbb{C}}^{\mathrm{an}}$.
4. $\chi(X) = \Delta_X \cdot \Delta_X$.

⌟

Proof: 1: It follows from trace formula(17.2.2.6) that
$$Z(X;T) = \frac{P_1(X;T)P_3(X;T)\dots P_{2n-1}(X;T)}{P_0(X;T)P_2(X;T)\dots P_{2n}(X;T)} = \frac{P(T)}{Q(T)},$$
where the roots α_{ij} of $P_i(X;T)$ are algebraic integers satisfying $|\iota(\alpha_{ij}^{-1})| = q^{-i/2}$ by Deligne's purity theorem(17.2.6.5). Thus $P_i(X;T) \in \mathbb{Q}[T]$ because it is in $\overline{\mathbb{Q}}[T]$ and also it is stable under $\mathrm{Gal}_{\mathbb{Q}}$, as their roots are distinguished by their ι-values.

Moreover, by Euler product(21.2.3.2), $Z(X;T) \in \mathbb{Z}[[T]]$, so it follows from(9.5.1.16) that $P(T), Q(T) \in \mathbb{Z}[T]$.

Notice by Poincaré duality(8.4.7.51), $\mathrm{H}^{2n}_{\text{ét}}(X;\mathbb{Q}_\ell(n)) \cong \mathrm{H}^0_{\text{ét}}(X;\mathbb{Q}_\ell)^\vee$, thus F_X^* acts on $\mathrm{H}^0_{\text{ét}}(X;\mathbb{Q}_\ell)$ by id and acts on $\mathrm{H}^{2n}_{\text{ét}}(X,\mathbb{Q}_\ell)$ by q^n. Thus $P_0(X;T) = 1-T$, $P_{2n}(X;T) = 1-q^nT$.

2: Apply(3.5.14.1) to $H^i = \mathrm{H}^i_{\text{ét}}(X;\mathbb{Q}_\ell)$, trace map and perfect pairing given by Poincaré duality(8.4.7.51) and $\varphi_i = q^{-i/2}F_X^*$. Notice $\varphi_{2n} = \mathrm{id}$ by item2. Now(3.5.14.1) says $\varphi_i^{-1} = \varphi_{2d-i}^t$. Then
$$\{\frac{q^{i/2}}{\alpha_{ij}}\}_j = \{\frac{\alpha_{2n-i,j}}{q^{(2n-i)/2}}\}_j$$

where we are counting multiplicity. Thus for $i\neq d$, we can assume $\alpha_{ij}\alpha_{2n-i,j}=q^n$, and for $i=d$, suppose there are $N_\pm$ many $\alpha_{d,j}=\pm q^{n/2}$, and the other $\alpha_{d,j}$ comes in pair: $\alpha_{d,j}\alpha_{d,b_d-j}=0$. Then

$$Z(X;\frac{1}{q^nT})=\prod_i(1-\alpha_{ij}/(q^nT))^{(-1)^{i+1}}=\prod_i(1-\frac{1}{\alpha_{2n-i,j}T})^{(-1)^{i+1}}=Z(X;T)\cdot q^{n\chi/2}(-1)^{N_+}.$$

Moreover, if n is odd, then $b_i=b_{d-i}$, and χ is even, so $d\chi/2\in\mathbb{Z}$.
3: These follow from the trace formula(17.2.2.6) and(8.4.7.35).
4: By(8.10.2.2),

$$\Delta_X\cdot\Delta_X=(\mathrm{cyl}_{X\times X}(\Delta_X),\mathrm{cyl}_{X\times X}(\Delta_X))=\sum_{i=0}^{2d}\mathrm{tr}(\mathrm{id}\,|\mathrm{H}^i_{\text{ét}}(X))=\chi(X).$$

□

Cor. (21.2.3.5) [Invariance of Characteristic Polynomial with ℓ]. It follows from the proof above that P_i is determined by X, and it is also the characteristic polynomial of $\mathrm{Fr}_{\overline{X}}$ on $\mathrm{H}^i_{\text{ét}}(X,\mathbb{Q}_\ell)$ for any $\ell\in\mathbf{P}\backslash\,\mathrm{char}\,k$, so the latter is independent of ℓ chosen. ⌟

Points Counting

Thm. (21.2.3.6) [Deligne's Estimate]. ⌟

Proof: □

Cor. (21.2.3.7) [Weil Bound]. For $X\in\mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}\mathcal{V}\mathrm{ar}^1/\mathbb{F}_q$, by Weil conjecture(21.2.3.4),

$$|\#X(\mathbb{F}_{q^n})-q^n-1|=|\sum_j\alpha_{1j}|\leq 2g(X)q^{n/2}.$$

⌟

Thm. (21.2.3.8) [Ihara/Drinfeld-Vladut]. For $p\in\mathbf{P},q\in 2^{\mathbb{Z}_+}$, let $A(q)=\overline{\lim}_{g(X)\to\infty}\frac{\#X(\mathbb{F}_q)}{g(X)}$, where the limit is taken over all smooth proper curves over $\mathbb{F}_q$. Then $A(q)\leq\sqrt{q}-1$.
And if $q\in 2^{\mathbb{Z}_+}$, then $A(q)=\sqrt{q}-1$. ⌟

Proof: Let α_{1j} as in(21.2.3.4), $\omega_i=\alpha_{1i}q^{-1/2}$, then $|\omega_i|=1$ and inversion induces an automorphism of $\{\omega_i\}$. Then by(21.2.3.7), for any $r\in\mathbb{Z}_+$,

$$N=\#X(\mathbb{F}_q)\leq\#X(\mathbb{F}_{q^r})=q^r+1-q^{r/2}\sum_i\omega_i^r.$$

And notice

$$0\leq|1+\omega_i+\ldots+\omega_i^r|^2=(r+1)+\sum_{j=1}^r(r+1-j)(\omega_i^j+\omega_i^{-j}),$$

So

$$\begin{aligned}2g(X)(r+1)&\geq-\sum_i\sum_{j=1}^r(r+1-j)(\omega_i^j+\omega_i^{-j})=-2\sum_{j=1}^r(r+1-j)(\sum_i\omega_i^j)\\&\geq N\sum_{j=1}^r(r+1-j)q^{-j/2}-\sum_{j=1}^r(r+1-j)(\alpha^j+\alpha^{-j})\end{aligned}$$

Thus

$$\frac{N}{g(X)} \le (\sum_{j=1}^{r} \frac{r+1-j}{r+1} q^{-j/2})^{-1} \cdot (1 + \frac{1}{g} \sum_{j=1}^{r} \frac{r+1-j}{r+1} (\alpha^j + \alpha^{-j}))$$

Taking limit $g \to \infty$,

$$\frac{N}{g(X)} \le (\sum_{j=1}^{r} \frac{r+1-j}{r+1} q^{-j/2})^{-1}.$$

And taking limit $r \to \infty$ gives

$$\frac{N}{g(X)} \le (\sum_{j=1}^{r} q^{-j/2})^{-1} = \sqrt{q} - 1.$$

For the last assertion, See[Ihara].**?** □

Thm. (21.2.3.9) [Lang-Weil Estimate]. Cf.[Zeta function in algebraic geometry, Mustata]. ⌟

Proof: □

Hasse-Weil L-Functions

Prop. (21.2.3.10) [Hasse-Weil L-Functions]. Let $F \in \texttt{GField}$ and $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}\mathcal{V}\mathrm{ar}/F$, the **Hasse-Weil L-function** of X is defined to be

$$L(X, s) = \prod_{v \in \Sigma_F^0} Z(\mathcal{X}_v, q^{-s}),$$

where for v s.t. $\mathcal{X}_v$ has good reduction, $Z(\mathcal{X}_v, T) = Z(\mathcal{X}_{k_v}, T)$ in(21.2.3.1), and for bad places v, it needs to be defined otherwise.**?** ⌟

Prop. (21.2.3.11). Let $l_1, \ldots, l_N$ be linear forms in r-variables with rational coefficients, then

$$\sum_{x \in \mathbb{Z}^r} \frac{1}{l_1(x) \ldots l_N(x)} \in \mathbb{Q}\pi^N$$

if it is convergent. ⌟

Proof: □

Def. (21.2.3.12) [Hasse-Weil L-Functions]. For $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}\mathcal{V}\mathrm{ar}/\mathbb{Q}, \ell \in \mathbf{P}$, there is some $N \in \mathbb{Z}_+, \ell | N$ s.t. X has a model $\mathcal{X}/\mathbb{Z}[\frac{1}{N}]$. Choose an embedding Then we can define a a partial zeta function

$$\zeta_N(X; s) = \prod_{p \nmid N} \Big(\prod_{x \in |X_p|_0} (1 - p^{-s \deg(x)})^{-1} \Big),$$

then by Grothendieck-Lefschetz formula,

$$\zeta_N(X; s) = \prod_{i=0}^{2 \dim X} L_N(\iota H^i(X, \overline{\mathbb{Q}}_\ell); s)^{(-1)^i}.$$

Thus it is natural to define the **Hasse-Weil L-function**

$$\zeta(X;s) = \prod_{i=0}^{2\dim X} L(\iota H^i(X,\overline{\mathbb{Q}}_\ell);s)^{(-1)^i}.$$

and the completed L-function

$$\Lambda(X;s) = \prod_{i=0}^{2\dim X} \Lambda(\iota H^i(X,\overline{\mathbb{Q}}_\ell)l;s)^{(-1)^i}.$$

┘

Example (21.2.3.13).
- $L(\operatorname{Spec}\mathbb{Q};s) = \zeta(s)$.
- For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$,
$$L(E;s) = \frac{\zeta(s)\zeta(s-1)}{L(h^1E;s)}(21.2.6.2).$$

┘

Conj. (21.2.3.14) [Functional Equations]. Motivated by Poincaré duality and(21.2.2.10), situation as in(21.2.3.12), $\zeta(X;s)$ should have a meromorphic extension to the whole plane, and satisfies a functional equation of the form

$$\Lambda(X;s) = \varepsilon(s)\Lambda(X, 1+\dim X - s).$$

┘

Proof: □

Remark (21.2.3.15). This is true for elliptic curves, by [BCDT]. ┘

4 Motivic L-Functions

Main references are [Del79] and [Zag94].

Def. (21.2.4.1) [Motivic L-Functions]. Use the fact the Grothendieck motives over a finite field is a Tannakian category**?**, we can define L-functions for any motives over a number field. Such an L-function is called a **motivic L-function**. ┘

Conj. (21.2.4.2) [Properties]. The motivic L-functions are conjectured to satisfy the following properties:

Algebraicity: There are Dirichlet series expansions: $L(s) = \sum_{n\geq 1} a_n n^{-s}$ for $\mathrm{Re}(s)$ large, where $\{a_n\} \in F$ for some number field F.

Euler Product: There are Euler product expansions: $L(s) = \prod_{p\in\mathbf{P}} \Phi_p(p^{-s})$ where $\max_{p\in\mathbf{P}}\{\deg\Phi_p\} < \infty$. In particular, $n \mapsto a_n$ is multiplicative.

Functional Equation: There is a γ-factor

$$\gamma(s) = A^s \cdot \prod_i \Gamma(\frac{1}{2}(s+m_i))$$

where $A \in \mathbb{C}^*, m_i \in \mathbb{Z}$, s.t. $\zeta(s) = \gamma(s)L(s)$ satisfies a functional equation

$$\zeta(s) = w\zeta(h-s)$$

where $w = \pm 1$ called the **sign of functional equation** and $h \in \mathbb{Z}_+$. And in this way, $L(s)$ extends to a meromorphic function on $\mathbb{C}$ with only f.m. poles.

Local Riemann Hypothesis: The zeros of $\Phi_p(p^{-s})$ lie on the line $\mathrm{Re}(s) = \frac{k-1}{2}$.

Riemann Hypothesis: The zeros of $L(s)$ are either integers or lie on the line $\mathrm{Re}(s) = \frac{k-1}{2}$.

Special Values: A **critical point for** $L(s)$ is an integer $m \in \mathbb{Z}$ s.t. neither m nor $h - m$ is a pole of $L(s)$. Then for a critical point m for $L(s)$, the **critical value** $L(m) = A(m)\Omega(m)$, where $A(m)$ is a reasonable algebraic number and $\Omega(m) \in \mathbb{P}$ is a reasonable period number.

Central Special Values: If $h = 2m, m \in \mathbb{Z}$, then m is called a **central value** of $L(s)$, and in this case, $A(m)$ is a square times a simple factor.

More...

⌟

Proof: □

Conj. (21.2.4.3) [Big Automorphy Conjecture]. Every motivic L-function comes from a automorphism representation. ⌟

Proof: □

5 0-Dimensional Motives

6 Abelian Motives

Elliptic Curves

Def. (21.2.6.1) [L-Factors]. ⌟

Def. (21.2.6.2) [Motivic L-Function of Elliptic Curves]. Let F be a global field F and $E \in \mathcal{E}\mathrm{ll}/F$, the motivic h^1 L-function is defined to be

$$L(h^1E, s) = \prod_{v \in \Sigma_F^0} L(h^1E_v, s)$$

where $L(E_v, s)$ is defined to be

- $L(E_v, s) = (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}$ as in(21.2.6.1), where $a_v = q_v + 1 - \#\widetilde{E}_v(\kappa_v)$, if E has good reduction at v.
- $(1 - q_v^{-s})^{-1}$ if E has split multiplicative reduction at v.
- $(1 + q_v^{-s})^{-1}$ if E has non-split multiplicative reduction at v.
- 1 if E has additive reduction at v.

Notice that in all cases we have $L(E_v, 1) = q_v/\#\widetilde{E}_{\mathrm{sm}}(\kappa_v)$. ⌟

Prop. (21.2.6.3) [Tate-Faltings]. If $E, E' \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ s.t. $L_E(s) = L_{E'}(s)$, then E, E' are isogenous. ⌟

Proof: Cf.[Milne, Elliptic Curves, Thm5.4.1]. □

Thm. (21.2.6.4) [Analytic Continuation]. For $F \in \texttt{NField}$ and $E \in \mathcal{E}\mathrm{ll}/F$, according to(21.2.3.14), the L-function $L(E,s)$(21.2.6.2) should have an analytic continuation an entire function on $s \in \mathbb{C}$, and satisfies a functional equation relating its value at s and $2-s$.

If $F = \mathbb{Q}$, let

$$\Lambda(E,s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$$

be the completed L-function, where $N_{E/\mathbb{Q}}$ is the conductor, then it satisfies the functional equation:

$$\Lambda(E,s) = w_E\Lambda(E,2-s)$$

where $w_E = \pm 1$ is called the **sign of functional equation of** E. ⌟

Proof: By modularity theorem(19.4.2.6), $L(E;s) = L(f;s)$ for some normalized Hecke eigenform $f \in S_2(\Gamma_0(N_E))$. So the assertion follows from(21.3.6.21). Notice $g = f[w_N]_k = -w_E f$(19.4.2.8). □

7 Zeta Functions of Shimura Varieties

8 Tamagawa Number Conjecture(Bloch-Kato)

References are [A note on Height Pairings, Tamagawa Numbers and the Birch and Swinnerton-Dyer Conjecture, Bloch].

Conj. (21.2.8.1) [Tamagawa Number Conjecture]. Let $F \in \texttt{NField}$ and $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/F$, suppose that $G(F)$ is discrete in $G(\mathbf{A}_F)$, then

$$\tau(G) = \frac{\#\operatorname{Pic}(G)_{\mathrm{tor}}}{\#\text{Ш}(G)}.$$

Moreover, $\operatorname{ord}_{s=1} L(s) \le 0$, and $r = 0$ iff $\operatorname{Vol}(G(A_F)/G(F)) < \infty$. ⌟

Proof: □

Thm. (21.2.8.2) [Bloch]. The Tamagawa number conjecture(21.2.8.1) implies that BSDT conjecture. ⌟

Proof: [Bloch, Height Pairing and]. □

Equivariant Tamagawa Number Conjecture

9 Others

Invariants of Moduli Spaces

Prop. (21.2.9.1). Volumes and Euler characteristics of moduli spaces are often expressible by special values of ζ-functions. ⌟

Proof: □

Def. (21.2.9.2)[Witten ζ-Functions]. Because of the appearance in physics(Verlinde formula), people are interested in certain moduli spaces of vector bundles on curves.

Witten gave a formula expressing the volume of these moduli spaces in terms of special values of **Witten ζ-functions**:

Let $\mathfrak{g}$ be a semisimple f.d. Lie algebra, define

$$\zeta_g(s) = \sum_{\rho \in \mathrm{Rep}(\mathfrak{g})} \frac{\dim(\rho)^s}{}?$$

⌟

Prop. (21.2.9.3). A consequence of Witten's formula(21.2.9.2) is:

$$\zeta_{\mathfrak{g}}(2m) \in \mathbb{Q}\pi^{2rm}, m \in \mathbb{Z}_+$$

where r is the number of positive roots of $\mathfrak{g}$. ⌟

Multiple ζ-Values

Cf.[Zag94].

21.3 L-Functions Attached to Automorphic Representations

Main references are [Bum98], [Cog00] and [Gelbart-Shahidi, Analytic Properties of Automorphic L-Functions].

Notation (21.3.0.1).

- Use notations defined in Adelic Automorphic Representations.
- Use notations defined in Archimedean L-Factors.
- Fix a global field F.
- Fix an additive character $\psi = \otimes' \psi_v : \mathbf{A}_F / F \to \mathbb{C}^\times$.
- Fix a linear algebraic group $G \in \mathcal{A}\mathrm{lg}\mathcal{G}\mathrm{rp}/F$ with center Z, and let $\mathcal{K} \subset G(\mathbf{A}_F)$ be a hyperspecial compact subgroup(15.4.3.2).
- Fix a central character $\omega : Z(\mathbf{A}_F)/Z(F) \to \mathbb{C}^\times$. Notice if $G = \mathrm{GL}(2)$, ω is just a Hecke character.

┘

1 Introduction

Remark (21.3.1.1) [Delete]. According to https://mathoverflow.net/questions/44657/principal-l-functions-on-gln, there are several ways to attach L-functions to a cusp form on $\mathrm{GL}(n)$ with functional equations:

1. Godement-Jacquet: In the spirit of Tate's thesis, take a cusp form f on $G = \mathrm{GL}(n)$ (and f' in the dual representation) and a Schwartz-Bruhat function Φ on $\mathrm{Mat}(n, \mathbf{A}_F)$ and integrate
$$\int_{Z(\mathbf{A}_F)G(F)\backslash G(\mathbf{A}_F)} \langle \pi(g)f, f'\rangle \Phi(g) |\det(g)|^s dg.$$
For this, Cf.[G-H11]Chap11.
2. Rankin-Selberg: Take a cusp form f on $G = \mathrm{PGL}(n)$ (and f' in the dual representation) and a specific Eisenstein series on $\mathrm{PGL}(n^2)$ and integrate
$$\int_{Z(\mathbf{A}_F)(G\times G)(F)\backslash (G\times G)(\mathbf{A}_F)} E(g_1, g_2) f(g_1) f'(g_2) \mathrm{d}g_1 \mathrm{d}g_2,$$
where Z is the center of $\mathrm{PGL}(n^2)$. For this, Cf.[Bum98] and [Goldfeld].
3. Explicit Eulerian integral(Jacquet-Shapiro-Shalika): Take a cusp form f on $\mathrm{GL}(n)$ and f' on $\mathrm{GL}(m)$ with $n > m$, integrate
$$\int_{GL(m,F)\backslash GL(m,\mathbf{A}_F)} Pf(g) f'(g) |\det(g)|^{s-1/2} \mathrm{d}g.$$
where P is the projection operator brilliantly designed s.t. this integral resolves to the product of Whittaker models for f and f'. For this, Cf.[Cog00] and [Analytic Theory of L-functions for $GL(n)$].
4. Eisenstein series(Langlands-Shahidi):

┘

L-Functions for $\mathrm{GL}(n)$

Prop. (21.3.1.2). To $\pi \in \mathrm{Irr}^{\mathrm{adm}}(\mathrm{GL}(n)/\mathbb{Q})$, we can associate:

-

⌟

2 Tate's thesis(Godement-Jacquet for $\mathrm{GL}(1)$)

Main references are [Poo15], [R-V99] and [Tat65].

Lemma (21.3.2.1) [Dedekind Zeta Function]. For a global field F, the **Dedekind zeta function** is defined by

$$\zeta(F;s) = \prod_{\mathfrak{p}\in\Sigma_F^{\mathrm{fin}}} \frac{1}{1-||\mathfrak{p}||^{-s}}.$$

It converges absolutely for $\mathrm{Re}(s) > 1$. Notice if $F \in \mathtt{FField}$, then

$$\zeta(F;s) = \sum_{\mathfrak{a}\in\mathrm{Ideal}(\mathcal{O}_F)} \frac{1}{||\mathfrak{a}||^s}$$

⌟

Proof: It suffices to show $\prod_{\mathfrak{p}\in\Sigma_F^{\mathrm{fin}}} \frac{1}{1-||\mathfrak{p}||^{-\sigma}} < +\infty$ for $\sigma > 1$.

If F is a number field, let $d = [F:\mathbb{Q}]$, this is bounded by

$$\prod_p (1-p^{-\sigma})^{-d} = (\sum_{n\geq 1} n^{-\sigma})^d < \infty.$$

If F is a function field, let the number of irreducible polynomial modulo p be N_n, then use the same method, it suffices to prove the convergence of

$$\prod_{\mathfrak{p}\in\Sigma_F^{\mathrm{fin}}} \frac{1}{1-\frac{1}{(N\mathfrak{p})^\sigma}} = \prod_{n\geq 1}(\frac{1}{1-q^{-n\sigma}})^{N_n}.$$

This is convergent iff $\sum_{n\geq 1} N_n q^{-n\sigma}$ is convergent(11.4.3.8), but the latter is bounded by

$$\sum_{n\geq 1} q^n q^{-n\sigma} = \sum_{n\geq 1} q^{-n(\sigma-1)} < \infty.$$

□

Def. (21.3.2.2) [Zeta Functions]. If $\Phi \in \mathcal{S}(F)$ and χ is a Hecke character of F, $s \in \mathbb{C}$, the **global zeta function** is defined to be

$$\zeta(\chi,\Phi;s) = \int_{\mathbf{I}_F} \Phi(\mathfrak{a})\chi(\mathfrak{a})|\mathfrak{a}|^s d^\times \mathfrak{a}.$$

When $\Phi = \otimes_v \Phi_v$ is a pure tensor,

$$\zeta(\chi,\Phi;s) = \prod_{v\in\Sigma_F} \zeta_v(s,\chi_v,\Phi_v) = \prod_{v\in\Sigma_F} \int_{F_v^\times} \Phi_v(x)\chi_v(x)|x|_v^s d^\times x$$

Where the **local zeta functions** $\zeta_v(\chi_v,\Phi_v;s)$ converge to a holomorphic function for $\mathrm{Re}(s) > 0$ and the integral is absolutely convergent for $\mathrm{Re}(s) > 1$. ⌟

Proof: For the local zeta function: Φ_v is rapidly decreasing, thus it suffices to integrate the part where $|x|_v < 1$. Then Φ_v is bounded on this compact region, thus it suffices to evaluate $\int_{|x|_v\leq 1} |x|_v^s \mathrm{d}^\times x < \infty$ for $\mathrm{Re}(s) > 0$, which can be done case by case.

To show the global integral converges, notice the local integrals is the same as the local L-factors for a.e. $v \in \Sigma_F$ by(21.3.2.3), so we can use Fubini and notice that $\prod_v L(\chi_v; s)$ converges by comparison with the Dedekind zeta function(21.3.2.1). □

Prop. (21.3.2.3) [Unramified Factors]. For any place v that unramified in the sense of(14.4.5.19) and $\Phi_v = \mathbb{1}_{\mathcal{O}_v}$,

$$\zeta_v(\chi_v, \Phi_v; s) = L(\chi_v; s) = (1 - \chi_v(\varpi)||\mathfrak{p}||^{-s})^{-1}\text{(21.3.3.1)}.$$

⌟

Proof: Notice the a.e. $v \in \Sigma_F$ satisfies v that unramified in the sense of(14.4.5.19) and $\Phi_v = \mathbb{1}_{\mathcal{O}_v}$, and for such a v,

$$\zeta_v(\chi_v, \Phi_v; s) = \sum_{k\in\mathbb{N}} \int_{v(x)=k} \chi_v(x)|x|_v^s d^\times x = \sum_{k\in\mathbb{N}} (\chi_v(\varpi_v)||v||^{-s})^k = (1 - \chi_v(\varpi)||v||^{-s})^{-1}.$$

□

Prop. (21.3.2.4) [Global Functional Equation]. The global zeta function(21.3.2.2) can be extended to a meromorphic function for all s, and it has poles iff $\chi(x) = |x|^\lambda$ for some $\lambda \in \mathrm{i}\,\mathbb{R}$. In which case, it only has poles at

$$s = \begin{cases} -\lambda, 1-\lambda & , F \in \texttt{NField} \\ -\lambda + \frac{2\pi n\,\mathrm{i}}{\log(\# F_0)}, 1 - \lambda + \frac{2\pi n\,\mathrm{i}}{\log(\# F_0)} & , F \in \texttt{FField} \end{cases}$$

with respectively residue $-kf(0)$ and $kf^\vee(0)$, where $k = V(\mathbf{I}_F^1/F^\times)$(14.4.5.20), and essentially bounded on the vertical strips away from the poles. And we have functional equations

$$\zeta(\chi, \Phi; s) = \zeta(\chi^{-1}, \Phi^\vee; 1-s).$$

⌟

Proof: Consider the exact sequence

$$1 \to \mathbf{I}_F^1 \to \mathbf{I}_F \to |\,\mathbf{I}_F\,| \to 1.$$

Let $\mathbf{I}_F^t$ be the inverse image of $t \in |\,\mathbf{I}_F\,|$, where $|\,\mathbf{I}_F\,| = \mathbb{R}_+$ or $q^{\mathbb{Z}}$, with Haar measure dt/t or $\log q$ times the counting measure(also denoted dt/t), and choose Haar measure $d^\times x$ on each I_F^t compatible with $d^\times \mathfrak{a}$ and dt/t. In particular, if $|a_t| = t$,

$$\int_{|I_F|} \int_{I_F^1} \Phi(a_t x)\chi(a_t x) t^s d^\times x \frac{dt}{t} = \int_{I_F} \Phi(\mathfrak{a})\chi(\mathfrak{a})|\mathfrak{a}|^s d^\times \mathfrak{a}.$$

Then the measure $d^\times x$ and the counting measure on $F^\times$ induces a measure $d^\times x$ on $I_F^1/F^\times$, in particular, for any $f \in C(C_F)$, we have

$$\int_{I_F^t/F^\times} f(x) d^\times x = \int_{I_F^1/F^\times} f(a_t x) d^\times x = \int_{I_F^1/F^\times} f(\frac{a_t}{x}) d^\times x = \int_{I_F^{1/t}/F^\times} f(\frac{1}{x}) d^\times x. \qquad (\star)$$

Denote $\zeta_t(\chi,\Phi;s)=\int_{I_F^t}\Phi(x)\chi(x)|x|^s d^\times x$, then

$$\zeta(\chi,\Phi;s)=\int_0^1\zeta_t(\chi,\Phi;s)\frac{dt}{t}+\int_1^\infty\zeta_t(\chi,\Phi;s)\frac{dt}{t}=J+I$$

where if $|I_F|=q^{\mathbb{Z}}$ the value at 1 is counted half-half at this two part. Now for the I-part, if $\mathrm{Re}(s)$ is smaller, it is smaller, thus I extends to a holomorphic function to all $s\in\mathbb{C}$. For the J-part, by lemmas(21.3.2.6)(21.3.2.5),

$$\begin{aligned}J&=\int_0^1\zeta_{1/t}(\widehat{\Phi},\chi^{-1};1-s)\frac{dt}{t}+[\int_0^1(k\widehat{\Phi}(0)(\frac{1}{t})^{1-s}-k\Phi(0)t^s)\frac{dt}{t}]\delta_{c,|\cdot|}\\&=\int_1^\infty\zeta_t(\widehat{\Phi},\chi^{-1};1-s)\frac{dt}{t}+[\int_0^1(k\widehat{\Phi}(0)t^{s-1}-k\Phi(0)t^s)\frac{dt}{t}]\delta_{c,|\cdot|}\\&=I(\chi,\Phi;s)+I(\chi^{-1},\widehat{\Phi};1-s)+k\delta_{c,|\cdot|}[\int_0^1(\widehat{\Phi}(0)t^{s-1}-\Phi(0)t^s)\frac{dt}{t}]\end{aligned}$$

So it can be extended, and the final part is

$$\frac{k\widehat{f}(0)}{s-1}-\frac{kf(0)}{s}$$

when F is number field, and when F is function field, it equals

$$k\log q[\widehat{f}(0)(-\frac{1}{2}+\sum_{n=0}^\infty(q^{-n})^{s-1})-f(0)(-\frac{1}{2}+\sum_{n=0}^\infty(q^{-n})^s)]=\frac{k\log q}{2}(\widehat{f}(0)\frac{1+q^{1-s}}{1-q^{1-s}}+f(0)\frac{1+q^s}{1-q^s}).$$

Now clearly $\zeta(\chi,\Phi;s)=\zeta(\chi^{-1},\widehat{\Phi};1-s)$, and it has the desired residues at 1 and $|\cdot|$. □

Lemma (21.3.2.5). $\int_{\mathbf{I}_F^t/F^\times}\chi(x)|x|^s d^\times x=kt^s$ if $\chi=\mathbb{1}$ and 0 otherwise. ⌟

Proof: $\int_{\mathbf{I}_F^t/F^\times}\chi(x)|x|^s d^\times x=\chi(a_t)t^s\int_{\mathbf{I}_F^1/F^\times}\chi(x)d^\times x$, $\mathbf{I}_F^t/F^\times$ is compact(14.4.4.21) and χ is trivial on $\mathbf{I}_F^1/F^\times$ iff $\chi=\mathbb{1}$, thus we can use(11.10.1.14). □

Lemma (21.3.2.6). $\zeta_t(\chi,\Phi;s)+\Phi(0)\int_{\mathbf{I}_F^t/F^\times}\chi(x)|x|^s d^\times x=\zeta_{1/t}(\widehat{\Phi},\chi^{-1};1-s)+\widehat{\Phi}(0)\int_{I_F^{1/t}/F^\times}\chi(x)|x|^s d^\times x$. ⌟

Proof:

$$\begin{aligned}\zeta_t(\chi,\Phi;s)+\Phi(0)\int_{I_F^t/F^\times}\chi(x)|x|^s d^\times x&=\int_{\mathbf{I}_F^t/F^\times}(\sum_{a\in F^\times}\Phi(ax))\chi(ax)|ax|^s d^*x+\int_{\mathbf{I}_F^t/F^\times}\Phi(0)\chi(x)|x|^s d^\times x\\&=\int_{\mathbf{I}_F^t/F^\times}(\sum_{a\in F}\Phi(ax))\chi(x)|x|^s d^*x\\(14.4.5.22)&=\int_{\mathbf{I}_F^t/K^\times}\frac{1}{|x|}(\sum_{a\in K}\widehat{\Phi}(a/x))\chi(x)|x|^s d^*x\\(\text{by }\star)&=\int_{\mathbf{I}_F^{1/t}/F^\times}(\sum_{a\in F}\widehat{\Phi}(ay))|y|\chi^{-1}(y)|y|^{-s}d^*y\\&=\zeta_{1/t}(\widehat{\Phi},\chi^{-1};1-s)+\widehat{f}(0)\int_{\mathbf{I}_F^{1/t}/F^\times}\chi(x)|x|^s d^\times x\end{aligned}$$

□

Local Functional Equations

Lemma (21.3.2.7). For any $\Phi_v, \Psi_v \in \mathcal{S}(F_v)$, $\chi_v \in (F_v^\times)^\vee$, $s \in \mathbb{C}$,

$$\frac{\zeta_v(\chi_v, \Phi_v; s)}{\zeta_v(\chi_v^{-1}, \widehat{\Phi}_v; 1-s)} = \frac{\zeta_v(\chi_v, \Psi_v; s)}{\zeta_v(\chi_v^{-1}, \widehat{\Psi}_v; 1-s)}.$$

⌟

Proof: ?

$$\zeta(f,c)\zeta(\widehat{g},\overline{c}) = \int_{K^\times} f(\alpha)c(\alpha)\int_{K^\times} \widehat{g}(\beta)c^{-1}(\beta)|\beta|d\beta = \int\int f(\alpha)\widehat{g}(\beta)c(\alpha\beta^{-1})|\beta|d\alpha d\beta$$

by Fubini.

$$= \int\int f(\alpha)\widehat{g}(\alpha\beta)c(\beta^{-1})|\alpha\beta|d\alpha d\beta = \int(\int f(\alpha)\widehat{g}(\alpha\beta)|\alpha|d\alpha)|\beta|c(\beta^{-1})d\beta$$

And notice

$$\int_{K^\times} f(\alpha)\widehat{g}(\alpha\beta)|\alpha|d\alpha = C\cdot\int_{K^+\setminus\{0\}} f(\xi)\widehat{g}(\xi\beta)d\xi = C\cdot\int_{K^+}\int_{K^+} f(\xi)g(\eta)e^{-2\pi i\Lambda(\xi\beta\eta)}d\eta d\xi$$

which is clearly symmetric in f and g. So the conclusion follows. □

Prop. (21.3.2.8) [Local Functional Equations]. For any $\Phi_v \in \mathcal{S}(F_v), \chi_v \in (F_v^\times)^\vee$, the local zeta function $\zeta_v(\chi_v, \Phi_v; s)$(21.3.2.2) can be extended to a meromorphic function to all $s \in \mathbb{C}$ that is analytic for $\mathrm{Re}(s) > 0$, and there is a function $\gamma_v(\chi_v, \psi_v; s)$, meromorphic for s and independent of f, such that

$$\zeta_v(\chi_v^{-1}, \widehat{\Phi}_v; 1-s) = \gamma_v(\chi_v, \psi_s; s)\zeta_v(\chi_v, \Phi_v; s).$$

⌟

Proof: By(21.3.2.2), both $\zeta_v(\chi_v^{-1}, \widehat{\Phi}_v; 1-s)$ and $\zeta_v(\chi_v, \Phi_v; s)$ are holomorphic in $0 < \mathrm{Re}(s) < 1$, so we define $\gamma(\chi_v, \psi_s; s)$ in this region, and try to extend it. Now(21.3.2.7) shows this is invariant of Φ_v, so we can take any Φ_v we want. Notice if $\Phi_v = 0$ on a nbhd of 0, then $\zeta_v(\chi, \Phi_v; s)$ is entire. Then because Fourier transform preserves $\mathcal{S}(F_v)$(14.4.5.11), we can take Φ_v to be 0 around 0 or $\widehat{\Phi}_v$ to be 0 around 0, then $\gamma_v(\chi_v, \psi_v; s)$ is analytic on both $\mathrm{Re}(s) > 0$ and $\mathrm{Re}(s) < 1$. □

Prop. (21.3.2.9). Let $v \in \Sigma_F^{\mathrm{fin}}$ and $\mathrm{Re}(s) < 1$, then for $N \in \mathbb{Z}_+$ sufficiently large,

$$\gamma_v(s, \chi_v, \psi_v) = \int_{\mathfrak{p}^{-N}} |x|^{-s}\chi_v^{-1}(x)\psi_v(x)dx.$$

⌟

Proof: In(21.3.2.8), take $\Phi_v = \mathbb{1}_{1+\mathfrak{p}^N}$, then $\widehat{\Phi}_v = \mathbb{1}_{\mathfrak{p}^{-N}} \cdot \psi_v$. □

Prop. (21.3.2.10).

- $\gamma(1-s, \chi^{-1}, \psi) = \chi(-1)/\gamma(s, \chi, \psi)$.
- $\rho(\overline{c}) = c(-1)\overline{\rho(c)}$

⌟

Proof: 1:

$$\zeta(f,c)=\rho(c)\zeta(\widehat{f},\widehat{c})=\rho(c)\rho(\widehat{c})\zeta(\widehat{\widehat{f}},c)=\rho(c)\rho(\widehat{c})c(-1)\zeta(f,c)$$

2:

$$\zeta(f,c)=\rho(c)\zeta(\widehat{f},\widehat{c}),\quad \overline{\zeta(f,c)}=\zeta(\overline{f},\overline{c})=\rho(\overline{c})\zeta(\widehat{\overline{f}},\widehat{\overline{c}})$$

And

$$\widehat{\overline{f}}(\xi)=\int\overline{f}(\eta)e^{-2\pi i\Lambda(\xi\eta)}d\eta=\overline{\int f(\eta)e^{2\pi i\Lambda(\xi\eta)}d\eta}=\overline{\widehat{f}}(-\xi)$$

so

$$\rho(\overline{c})\zeta(\widehat{\overline{f}},\widehat{\overline{c}})=\rho(\overline{c})c(-1)\zeta(\overline{\widehat{f}},\overline{\widehat{c}})=\rho(\overline{c})c(-1)\overline{\zeta(\widehat{f},\widehat{c})}$$

Thus $\rho(\overline{c})=c(-1)\overline{\rho(c)}$. □

Cor. (21.3.2.11). Because when $\sigma(c)=\frac{1}{2}$, $\widehat{c}=\overline{c}$**??**, we have $|\rho(c)|=1$ in this case. ⌟

3 Weber L-Functions(GL(1) Case)

Def. (21.3.3.1) [Local L-Factors]. Given a Hecke character χ, for $v\in\Sigma_F$, the local L-factor for $v\in\Sigma_F$ and $s\in\mathbb{C}$ is defined to be

$$L(\chi_v;s)=\begin{cases}(1-\chi_v(\varpi)||\mathfrak{p}||^{-s})^{-1} & v\in\Sigma_F^{\text{fin}},\chi_v\text{ unramified}\\ 1 & v\in\Sigma_F^{\text{fin}},\chi_v\text{ ramified}\\ L_{\mathbb{R}}(s+\nu+\varepsilon)(11.6.1.13) & v\in\Sigma_F^{\mathbb{R}},\chi_v(x)=|x|^\nu\operatorname{sgn}(x)^\varepsilon,\nu\in\mathrm{i}\,\mathbb{R},\varepsilon\in\{0,1\}\\ L_{\mathbb{C}}(s+\nu+\frac{|k|}{2})(11.6.1.13) & v\in\Sigma_F^{\mathbb{C}},\chi_v(x)=|x|^\nu e^{\mathrm{i}\,k\arg(x)},\nu\in\mathrm{i}\,\mathbb{R},k\in\mathbb{Z}\end{cases}$$

⌟

Prop. (21.3.3.2)[Local L-Factors are the Common Divisors]. Situation as in(21.3.2.8), $\frac{\zeta_v(\chi_v,\Phi_v;s)}{L(\chi_v;s)}$ is entire for any $\Phi_v\in\mathcal{S}(F_v)$, and if $v\in\Sigma_F^{\text{fin}}$, it is a rational function of $||v||^{-s}$.

Moreover, if we take

$$\Phi_v(x)=\begin{cases}\mathbb{1}_{1+\mathfrak{c}(\chi_v)} & ,v\in\Sigma_F^{\text{fin}}\\ x^\varepsilon e^{-\pi x^2} & ,v\in\Sigma_F^{\mathbb{R}},\chi_v(x)=|x|^\nu\operatorname{sgn}(x)^\varepsilon,\nu\in\mathrm{i}\,\mathbb{R},\varepsilon\in\{0,1\}\\ \pi^{-1}\overline{x}^k e^{-2\pi|x|_v} & ,v\in\Sigma_F^{\mathbb{C}},\chi_v(x)=|x|^\nu e^{\mathrm{i}\,k\arg(x)},\nu\in\mathrm{i}\,\mathbb{R},k\in\mathbb{N}\\ \pi^{-1}x^{-k}e^{-2\pi|x|_v} & ,v\in\Sigma_F^{\mathbb{C}},\chi_v(x)=|x|^\nu e^{\mathrm{i}\,k\arg(x)},\nu\in\mathrm{i}\,\mathbb{R},k\in\mathbb{Z}_-.\end{cases}$$

then

$$\frac{\zeta_v(\chi_v,\Phi_v;s)}{L(\chi_v;s)}=\begin{cases}d^\times\alpha_v(\mathcal{O}^*) & ,v\in\Sigma_F^{\text{fin}},\chi_v\text{ unramified}\\ d^\times\alpha_v(1+\mathfrak{c}(\chi_v)) & ,v\in\Sigma_F^{\text{fin}},\chi_v\text{ ramified}\\ 1 & ,v\in\Sigma_F^\infty\end{cases}$$

In particular, they can all be non-zero constants. ⌟

Proof: For $v\in\Sigma_F^{\text{fin}}$,

$$\zeta_v(\chi_v,\Phi_v;s)=\sum_{k\in\mathbb{Z}}||v||^{ks}\int_{v(x)=-k}\Phi_v(x)\chi_v(x)d^\times x$$

As $\Phi_v\in C_c^\infty(F_v)$, the summand is 0 for k large. And for k small, $\Phi_v(x)$ is constant. If χ_v is ramified, then these terms are 0, thus it is a polynomial in $||\mathfrak{p}||^{-s}$, and for χ_v unramified, the these terms are a geometric series, which is easily seen to be a rational function of $||\mathfrak{p}||^{-s}$, and has the same pole as $L(\chi_v;s)$(21.3.3.1).

For $v\in\Sigma_F^{\mathbb{R}}$, the poles of $\zeta_v(\chi_v,\Phi_v;s)$ are the same as poles of $\int_{|x|\leq 1}\Phi_v(x)\chi_v(x)|x|^s dx$, because $\int_{|x|\geq 1}\Phi_v(x)\chi_v(x)|x|^s dx$ is convergent for any $s\in\mathbb{C}$. For the former, we can write Φ_v as a sum of an odd function and an even function. Only the part with the same parity of χ_v will be non-zero, and for that part, by(11.4.3.5), its poles are all simple and are poles of $L(\chi_v;s)$(21.3.3.1).

For $v\in\Sigma_F^{\mathbb{C}}$, if $\chi_v(x)=|x|^\nu e^{\mathrm{i}\,k\arg(x)},\nu\in\mathrm{i}\,\mathbb{R},k\in\mathbb{Z}$,

$$\zeta_v(\chi_v,\Phi_v;s)=\frac{1}{2\pi}\int_0^\infty\int_0^{2\pi}r^{2v+2s}e^{ik\theta}\Phi_v(re^{i\theta})d\theta\frac{dr}{r}=\int_0^\infty r^{2v+2s}\varphi(r)\frac{dr}{r},$$

where

$$\varphi(r)=\frac{1}{2\pi}\int_0^{2\pi}e^{ik\theta}\Phi_v(re^{i\theta})d\theta.$$

Suppose $\Phi_v(x)=\sum_{n,m\in\mathbb{N}}a(n,m)x^n\overline{x}^m$, then $\varphi(r)=\sum_{m-n=k}a(n,m)r^{m+n}$. Thus by(11.4.3.5), its pole are $\{s|2s+2v-(|k|+2l)\}$, which are all simple and are poles of $L(\chi_v;s)$(21.3.3.1).

For the last assertion, we need direct calculations, Cf.[Tate's Thesis]P320**?**. □

Prop. (21.3.3.3)[Local ε-Factors]. Situation as in(21.3.2.8), there exists a non-vanishing holomorphic function $\varepsilon_v(\chi_v,\psi_v)$ that

$$\frac{\zeta_v(\chi_v^{-1},\widehat{\Phi}_v;1-s)}{L(\chi_v^{-1};1-s)}=\varepsilon_v(\chi_v,\psi_v;s)\frac{\zeta_v(\chi_v,\Phi_v;s)}{L(\chi_v;s)}.$$

and $\frac{\zeta_v(\chi_v,\Phi_v)}{L_v(\chi_v;s)}$ is holomorphic. Moreover, $\varepsilon_v(\chi_v,\psi_v;s)$ is of the form ab^s for $a\in\mathbb{C}^*,b\in\mathbb{R}$. And $\varepsilon(\chi_v,\psi_v)=1$ if v is unramified in the sense of(14.4.5.19). ⌟

Proof: Such an $\varepsilon_v(\chi_v,\psi_v;s)$ exists by(21.3.2.8). It is holomorphic and non-vanishing by(21.3.3.2) as both $\frac{\zeta_v(\chi_v^{-1},\widehat{\Phi}_v;1-s)}{L(\chi_v^{-1};1-s)}$ and $\frac{\zeta_v(\chi_v,\Phi_v;s)}{L(\chi_v;s)}$ are holomorphic and for any $s_0\in\mathbb{C}$, Φ_v can be chosen to make either one of them non-vanishing at s_0.

To show it is of the form ab^s: If $v\in\Sigma_F^{\mathrm{fin}}$, it is a rational function in $||\mathfrak{p}||^{-s}$ with no zeros or poles, so it must be of the form ab^s. And if v is unramified, then we can take $\Phi_v=\mathbb{1}_{\mathcal{O}_{F,v}},\Phi_v^\vee=\mathbb{1}_{\mathcal{O}_{F,v}}$ by(14.4.5.5), and both sides are 1 by(21.3.2.3).

If $v\in\Sigma_F^\infty$, then we can take Φ_v defined in(21.3.3.2) to do the calculation to show it directly(**?**Cf.[Tate's Thesis]):

$$\Phi_v^\vee(x)=\begin{cases}||\mathfrak{c}(\psi_v)^{-1}\mathfrak{c}(\chi_v)||.d\mu_v(\mathcal{O}_{F_v}).\mathbb{1}_{\mathfrak{c}(\psi_v)\mathfrak{c}(\chi_v)^{-1}}.\psi_v^{-1} & ,v\in\Sigma_F^{\mathrm{fin}}\\ \mathrm{i}^\varepsilon\cdot x^\varepsilon e^{-\pi x^2} & ,v\in\Sigma_F^{\mathbb{R}},\chi_v(x)=\mathrm{sgn}(x)^\varepsilon,\varepsilon\in\{0,1\}\\ \mathrm{i}^k\cdot\pi^{-1}x^k e^{-2\pi|x|_v} & ,v\in\Sigma_F^{\mathbb{C}},\chi_v(x)=|x|^\nu e^{\mathrm{i}\,k\arg(x)},\nu\in\mathrm{i}\,\mathbb{R},k\in\mathbb{N}\\ \mathrm{i}^{-k}\cdot\pi^{-1}\overline{x}^{-k}e^{-2\pi|x|_v} & ,v\in\Sigma_F^{\mathbb{C}},\chi_v(x)=|x|^\nu e^{\mathrm{i}\,k\arg(x)},\nu\in\mathrm{i}\,\mathbb{R},k\in\mathbb{Z}_-.\end{cases}$$

So it follows from(21.3.3.2) that

$$\varepsilon_v(\chi_v,\psi_v;s)=\begin{cases}\text{Cf.[Tate's Thesis]}\,\mathbf{?} & ,v\in\Sigma_F^{\mathrm{fin}}\\ \mathrm{i}^\varepsilon & ,v\in\Sigma_F^{\mathbb{R}}\\ \mathrm{i}^{|n|} & ,v\in\Sigma_F^{C}\end{cases}$$

□

Remark (21.3.3.4). The local ε-factor is calculable using the special function Φ_v, theoretically. ⌟

Prop. (21.3.3.5) [Global Hecke L-Functions]. For a Hecke character $\chi = \prod_v \chi_v$ on F and $s \in \mathbb{C}$, we define the **global Hecke L-function** and **completed Hecke L-function** as

$$L(\chi; s) = \prod_{v \in \Sigma_F^{\text{fin}}} L(\chi_v; s), \quad \Lambda(\chi; s) = \prod_v L(\chi_v; s)(21.3.3.1)$$

which converges for $\operatorname{Re} s > 1$ and has a meromorphic continuation to all $s \in \mathbb{C}$.

Also, we can define the **global ε-factor** for χ as

$$\varepsilon(\chi; s) = \prod_v \varepsilon_v(\chi_v, \psi_v; s).$$

All but f.m. of the product equals 1 by(21.3.3.3), and they are of the form ab^s, so $\varepsilon(s, \chi)$ is also of the form ab^s, where $a \in \mathbb{C}^*, b \in \mathbb{R}_+$. In particular, it is holomorphic and non-vanishing. The fact $\varepsilon(s, \chi)$ is independent of ψ can be seen from(21.3.3.6). ⌟

Prop. (21.3.3.6) [Meromorphic Extension of Hecke L-Functions]. For a Hecke character χ,

- $L(\chi; s)$ has meromorphic continuation to all s, and there is a functional equation

  $$\Lambda(\chi; s) = \varepsilon(\chi; s)\Lambda(\chi^{-1}; 1 - s),$$

  where $\varepsilon(\chi; s)$ is of the form $ab^s, a \in \mathbb{C}^\times, b \in \mathbb{R}_+$.
- $L(\chi; s)$ has poles iff $\chi(x) = |x|^\lambda$ for some $\lambda \in \mathrm{i}\,\mathbb{R}$. In this case,
  - If $F \in \mathtt{NField}$, then it only has simple poles at $s = 1 - \lambda$, with residue $-k||\mathfrak{d}_F||^{1/2}$.
  - If $F \in \mathtt{FField}$, it has poles at $s = -\lambda + \frac{2\pi n\,\mathrm{i}}{\log(\#F_0)}, 1 - \lambda + \frac{2\pi n\,\mathrm{i}}{\log(\#F_0)}$, with respectively residue $-k||\mathfrak{d}_F||^{1/2}$ and k, where $k = V(\mathbf{I}_F^1/F^\times)$(14.4.5.20),
- $L(\chi; s)$ is essentially bounded on the vertical strips away from the poles.
- If $F \in \mathtt{NField}$, then $L(\mathbb{1}; s)$ has a zero of order $r_1 + r_2 - 1$ at $s = 0$.

⌟

Proof: The functional equation follows from the definition of local ε-factors(21.3.3.3) and(21.3.2.4). To show it is essentially bounded on vertical strips, use

$$\frac{\Lambda(\chi; s)}{\zeta(\chi, \Phi; s)} = \prod_{v \in \Sigma_F} \frac{L(\chi_v; s)}{\zeta_v(\chi_v, \Phi_v; s)}$$

where we can take Φ_v s.t. each fraction is of the form ab^s, and a.e. term is 1, by(21.3.3.3). Then $L(\chi; s)$ is essentially bounded on vertical strips because $\zeta(\chi, \Phi; s)$ does(21.3.2.4).

To find the poles and residues, choose Φ_v as in (21.3.3.2), then $\zeta(\chi, \Phi; s)$ is a constant multiple of $\Lambda(\chi; s)$, and the poles and residues of can be read from that of $\zeta(\chi, \Phi; s)$. Then we use(21.3.2.4), the assertion about poles follows.

Then it suffices to calculate for $\chi = 1$: we use the standard character on $\mathbf{A}_F$, then we calculate $\Phi_v(0) = \pi^{-r_2}$ and $\Phi_v^\vee(0) = ||\mathfrak{d}_v||^{-1/2}\pi^{-r_2}$, by(21.3.3.3) and(14.4.5.5). Thus we can use properties of the infinite L-factors(11.6.1.13). □

Def. (21.3.3.7) [Root Number]. The number $w(\chi) = \varepsilon(\chi; \frac{1}{2})$ is called the **root number** of χ. Then it satisfies $|w(\chi)| = 1$, and $w(\chi) \in \{\pm 1\}$ if χ is real. ⌟

4 Godement-Jacquet Theory

Main references are [G-J72].

5 Rankin-Selberg Methods on GL(2) × GL(2)

References are [Automorphic Forms on GL(2), Jacquet, 1972].

Def. (21.3.5.1) [Intro, Rankin-Selberg Method]. Delete this**?**. Converse theorems like(21.3.6.18), shows that a possible method of proving the existence of an automorphic form is to prove by any method the functional equations of sufficiently many of the the L-series attached to it. One of the most powerful methods of doing this is the **Rankin-Selberg method**, which seeks to represent an L-function as an integral of one or more automorphic forms against an Eisenstein series, itself a type of automorphic form. ⌟

Conj. (21.3.5.2) [Rankin-Selberg L-function]. For a global field F, assume the Langlands functoriality, for any $\pi_1 \in \mathrm{Irr}^{\mathrm{auto}}(\mathrm{GL}(n)/F)$ and $\pi_2 \in \mathrm{Irr}^{\mathrm{auto}}(\mathrm{GL}(m)/F)$, their product $\pi_1 \times \pi_2 \in \mathrm{Irr}^{\mathrm{auto}}(\mathrm{GL}(n)\times\mathrm{GL}(m)/F)$, and there is a tensor product map $\otimes : \mathrm{GL}(n)\times\mathrm{GL}(m) \to \mathrm{GL}(mn)$, which by functorial lifting(20.6.3.2) gives us an automorphic representation $\pi_1 \boxtimes \pi_2 \in \mathrm{Irr}^{\mathrm{auto}}(\mathrm{GL}(mn)/F)$, whose L-function is denoted by $L(s, \pi \times \pi')$ And for a finite set S of places of F large enough,

$$L_S(s, \pi_1 \times \pi_2) = \prod_{v\notin S}\prod_{i=1}^{n}\prod_{j=1}^{m}\frac{1}{1-\alpha_i(\pi_{1,v})\beta(\pi_{2,v})q_v^{-s}}$$

called the (partial)**Rankin-Selberg L-function** of π_1, π_2. Here are some examples:

- $\pi_1 = \pi, \pi_2 = \widehat{\pi}$, then for some S, then

$$L_S(s, \pi \times \widehat{\pi}) = \prod_{v\notin S}\prod_{1\le i,j\le n}\frac{1}{1-\alpha_i(\pi_v)\alpha_j^{-1}(\pi_v)q_v^{-s}}.$$

  In this case, this is the functorial lifting of

$$\mathrm{GL}(n) \to \mathrm{GL}(n)\times\mathrm{GL}(n) \to \mathrm{GL}(2n) : g \mapsto (g, g^{-t}) \mapsto g\otimes g^{-t}$$

  by(20.5.2.7), which is isomorphic to the conjugation action of $\mathrm{GL}(n)$ on $\mathrm{Mat}(n)$. This action decomposes as a trivial action and a n^2-1-dimensional representation Ad^0. Thus there should be a decomposition

$$L_S(s, \pi \times \widehat{\pi}) = \zeta_{F,S}(s)L_S(s, \pi, \mathrm{Ad}^0)$$

  where $\zeta_{F,S}(s)$ is the partial zeta function on F.

- $\pi_1 = \pi = \pi_2$, then for some S, then

$$L_S(s, \pi \times \widehat{\pi}) = \prod_{v\notin S}\prod_{1\le i,j\le n}\frac{1}{1-\alpha_i(\pi_v)\alpha_j(\pi_v)q_v^{-s}}.$$

  In this case, this is the functorial lifting of

$$GL(n) \to GL(n)\times GL(n) \to GL(2n) : g \mapsto (g, g) \mapsto g\otimes g$$

by(20.5.2.7), which decomposes as a $\frac{1}{2}n(n+1)$-dimensional symmetric square representation Sym^2, and a $\frac{1}{2}n(n-1)$-dimensional exterior square representation $\wedge^2$. Thus there should be a decomposition

$$L_S(s,\pi\times\widehat{\pi}) = L_S(s,\mathrm{Sym}^2\pi)L_S(s,\wedge^2\pi),$$

where $L_S(s,\mathrm{Sym}^2\pi)$ and $L_S(s,\wedge^2\pi)$ are called the **symmetric square L-functions** and **exterior square L-functions** of π.

There are two Rankin-Selberg constructions of exterior square L-functions, which can be found in [Jacquet, H. and J. Shalika, Exterior square L-functions, in Automorphic Forms, Shimura Varieties and L-functions II, 1990] and [Bump, D. and S. Friedberg, The "exterior square" automorphic L-functions on GL(n), 47-65 in part 2 of Gelbart, Howe and Sarnak (1990)]. The construction of symmetric square L-functions can be found in [Bump, D. and D. Ginzburg, Symmetric square L-functions on GL(r), Annals of Math. 136 (1992)]. ⌟

Prop. (21.3.5.3). For $\pi_1\in\mathrm{Irr}^{\mathrm{auto}}(\mathrm{GL}(2)/F,\omega_1),\pi_2\in\mathrm{Irr}^{\mathrm{auto}}(\mathrm{GL}(2)/F,\omega_2)$, by tensor product theorem(20.5.1.4), we can fix a finite set $\Sigma_F^\infty\subset S\subset\Sigma_F$ that any $v\notin S$ is unramified for both π_1,π_2 in the sense of(21.3.6.1). Let $\alpha_i(v),\beta_i(v)$ be the Stake parameters of $\pi_{1,v},\pi_{2,v}$, then $\pi_1\cong\widehat{\pi}_2$ iff the Rankin-Selberg L-function(21.3.5.2)

$$L_S(s,\pi_1\times\pi_2)=\prod_{v\notin S}\prod_{1\le i,j\le 2}\frac{1}{1-\alpha_i(v)\beta_i(v)}$$

has a pole at $s=1$. ⌟

Proof: Cf.[Bump, Chap3.8]. □

Rankin-Selberg for Modular Forms

Notation (21.3.5.4).

- Use notations on Eisenstein series as in Eisenstein Series.

⌟

Prop. (21.3.5.5)[Convolution of Cusp Forms]. If $f(z)=\sum A(n)q^n\in S_k(\Gamma(1))$, $g(z)=\sum B(n)q^n\in M_k(\Gamma(1))$, define

$$L(f\times g;s)=\zeta(2s-2k+2)\sum A(n)B(n)n^{-s},\quad \Lambda(f\times g;s)=(2\pi)^{-2s}\Gamma(s)\Gamma(s-k+1)L(f\times g;s),$$

then $L(s,f\times g)$ is absolutely convergent for s large, $\Lambda(s,f\times g)$ has a meromorphic continuation to all s, analytic except for at most simple poles at $s=k$ or $s=k-1$, and it satisfies a functional equation

$$\Lambda(s,f\times g)=\Lambda(2k-1-s,f\times g).$$

and the residue of Λ at $s=k$ is $\frac{1}{2}\pi^{1-k}(f,g)$(20.2.1.20).

Moreover, if f,g are Hecke eigenforms, let

$$1-A(p)X+p^{k-1}X^2=(1-\alpha_1(p)X)(1-\alpha_2(p)X),$$
$$1-B(p)X+p^{k-1}X^2=(1-\beta_1(p)X)(1-\beta_2(p)X),$$

then $L(s,f\times g)$ has an Euler product formula

$$L(s,f\times g)=\prod_p\prod_{i=1}^2\prod_{j=1}^2\frac{1}{1-\alpha_i(p)\beta_j(p)p^{-s}}.$$

⌟

Proof: We may assume f, g are Hecke eigenforms(20.2.2.12), so $A(n), B(n)$ are real. Let $\varphi(z) = f(z)\overline{g(z)}y^k$, then φ satisfies the condition of the Rankin-Selberg method(21.1.1.6), thus we calculate

$$\varphi_0(y) = \int_0^1 f(x+iy)\overline{g(x+iy)}y^k dx = \sum_{n=0}^{\infty}\int_{m=0}^{\infty}\int_0^1 A(n)B(n)e^{2\pi i(n-m)x}e^{-2\pi(n+m)y}y^k dx$$
$$= \sum_{n=0}^{\infty} A(n)B(n)e^{-4\pi ny}y^k$$

and

$$M(s,\varphi_0) = \sum_{n=0}^{\infty} A(n)B(n)\int_0^{\infty} e^{-4\pi ny}y^{s+k}\frac{dy}{y} = (4\pi)^{-s-k}\Gamma(s+k)\sum_{n=0}^{\infty} A(n)B(n)n^{-s-k}$$

and

$$\Lambda(s,\varphi_0) = 4^{-s-k+1}\pi^{-2s-k+1}\Gamma(s)\Gamma(s+k-1)\zeta(2s)\sum_{n=1}^{\infty} A(n)B(n)n^{-s-k+1}.$$

Thus

$$\Lambda(s-k+1,\varphi_0) = \pi^{k-1}\Lambda(s, f\times g),$$

and the assertion follows from(21.1.1.6). The residue is also clear.

The Euler product formula follows from(9.5.2.3) applied to $z = p^{-s}$ for all $p \in \mathbf{P}$. □

Remark (21.3.5.6) [Averaged Ramanujan Conjecture]. By the Ramanujan conjecture(21.3.6.16), for any cuspidal form $f = \sum a(n)q^n$, $L(s,f) = \sum a_n n^{-s}$ is convergent for $\mathrm{Re}(s) > \frac{k+1}{2}$. But we can prove this directly: as $\sum a_n^2 n^{-s}$ is convergent for $\mathrm{Re}(s) > k$, and $|a(n)| \leq \max(n^{\frac{k-1}{2}}, n^{-\frac{k-1}{2}}|a(n)|^2)$. ⌟

Waldspurger's Theorem

Cf.[Explicit application of Waldspurger's theorem].

Thm. (21.3.5.7) [Waldspurger]. Let χ be a character, $k \in 2\mathbb{Z}$ and $\varphi \in S_{k-1}(N,\chi^2)$, then there exists a function A_φ on $\mathbb{N}^{sc}$ s.t. for $t \in \mathbb{N}^{sc}$,

$$A_\varphi(t)^2 = L(\varphi\otimes\chi_0^{-1}\chi_t, \frac{k-1}{2})\varepsilon(\chi_0^{-1}\chi_t, \frac{1}{2}).$$

⌟

Proof: Cf.[Explicit application of Waldspurger's theorem]. □

6 Eulerian Integrals on GL(2) × GL(1)

Main references are [Cog00] and[Bum98].

Def. (21.3.6.1) [Unramified Places]. Let (π, V) be an irreducible cuspidal representation, given a pure cuspidal form $\varphi \in V$ and a Hecke character ξ of F, we call a place v of F **unramified** iff $v \in \Sigma_F^{\mathrm{fin}}$, the conductor of ψ_v is $\mathcal{O}_v$ and the conductor of ξ_v is $\mathcal{O}_v^*$, π_v is a spherical principal series.

This condition is true for a.e. v by(20.5.3.2) and(20.5.3.3). ⌟

Def. (21.3.6.2) [Zeta Functions for $\mathrm{GL}(2)\times\mathrm{GL}(1)$]. Given $(\pi, V)\in \mathrm{Irr}^{\mathrm{auto}}(\mathrm{GL}(2)/F,\omega)$, ξ a Hecke character, for any $\Phi\in V$, consider the zeta integral

$$\zeta(\Phi,\xi;s)=\int_{C_F}\Phi(\begin{bmatrix} y & \\ & 1\end{bmatrix})|y|^{s-1/2}\xi(y)d^\times y$$

It is absolutely convergent by(20.5.3.5) and(14.4.4.21).

If $\Phi=\otimes\Phi_v$ is a pure tensor, the zeta integral equals

$$\int_{I_F}W_\Phi(\begin{bmatrix} y & \\ & 1\end{bmatrix})|y|^{s-1/2}\xi(y)d^\times y=\prod_v\int_{F_v^\times}W_{v,\Phi_v}(\begin{bmatrix} y_v & \\ & 1\end{bmatrix})|y_v|^{s-1/2}\xi_v(y_v)d^\times y_v=\prod_v\zeta_v(\Phi_v,\xi_v;s)$$

where each **local zeta functions** $\zeta_v(s,\Phi_v,\xi_v)$ converges absolutely to a holomorphic function for $\mathrm{Re}(s)>1/2$, and the integral is absolutely convergent when $\mathrm{Re}(s)>3/2$, using(11.10.1.38). ⌟

Proof: We analyze the integrand for the local zeta integrals:

For non-Archimedean case, the integrand is compactly supported on(18.11.3.19), and because π_v is unitary, use(18.11.4.23) and(18.11.6.10) to analyze the Kirillov model of π_v, we see the integral converges absolutely for $\mathrm{Re}(s)>1/2$.

For Archimedean case, the W_φ decays rapidly for $|y|\to\infty$, and for $|y|\to 0$, by(20.1.3.2), it is bounded by $|y|^{-1/2}$, thus it also converges absolutely for $\mathrm{Re}(s)>1/2$.

By(21.3.6.3), the local factor is the same as the local L-factor a.e. v, and $|\alpha_i|<||v||^{1/2}$ by(18.11.6.10), thus it converges for $\mathrm{Re}(s)>3/2$ by comparison with the Dedekind Zeta function(21.3.2.1). □

Prop. (21.3.6.3) [Unramified Factors]. If v is unramified in the sense of(21.3.6.1) and Φ_v is the spherical function in π_v normalized s.t. $W_{v,\Phi_v}(1)=1$, then for $\mathrm{Re}(s)>1/2$(thus all, as they are both meromorphic),

$$\zeta_v(\Phi_v,\xi_v;s)=L(\pi_v,\xi_v;s)(21.3.6.10).$$

⌟

Proof: With the unramified hypothesis, there is an explicit formula for W_v in terms of the Satake parameters α_1,α_2(18.11.5.15): if $\mathrm{ord}_v(y)=m$, then

$$W_v(\begin{bmatrix} y & \\ & 1\end{bmatrix})=\begin{cases}||v||^{-m/2}\frac{\alpha_1^{m+1}-\alpha_2^{m+1}}{\alpha_1-\alpha_2} & m\geq 0\\ 0 & \text{otherwise}\end{cases}.$$

$$\begin{aligned}\zeta_v(W_v,\xi_v;s)&=\sum_{m=0}^\infty||v||^{-m/2}\frac{\alpha_1^{m+1}-\alpha_2^{m+1}}{\alpha_1-\alpha_2}||v||^{m/2-ms}\xi(\varpi_v)^m\\&=\frac{1}{(1-\alpha_1\xi(\varpi_v)||v||^{-s})(1-\alpha_2\xi(\varpi_v)||v||^{-s})}=L(\pi_v,\chi_v;s)\end{aligned}$$

□

Prop. (21.3.6.4) [Global Functional Equation]. In spite of the convergence problem of the product of local zeta integrals, the global zeta integral is absolutely convergent for any s as W_Φ decay rapidly**?**. Moreover, because Φ is automorphic, we have

$$\zeta(\Phi,\xi;s)=\int_{C(F)}\Phi(w_1\begin{bmatrix} y & \\ & 1\end{bmatrix})|y|^{s-1/2}\xi(y)d^\times y$$

$$
\begin{aligned}
&= \int_{C(F)} \Phi(\begin{bmatrix} 1 & \\ & y \end{bmatrix} w_1)|y|^{s-1/2}\xi(y)d^\times y \\
&= \int_{C(F)} (\pi(w_1)\Phi)(\begin{bmatrix} y & \\ & 1 \end{bmatrix})|y|^{-s+1/2}(\xi\omega)^{-1}(y)d^\times y \\
&= \zeta(\pi(w_1)\Phi, \xi^{-1}\omega^{-1}; 1-s)
\end{aligned}
$$

⌟

Local Functional Equation

Prop. (21.3.6.5) [Local Zeta Function]. Let K be a p-adic local field and $(\pi, V) \in \mathrm{Irr}^{\mathrm{adm},generic}(\mathrm{GL}(2,K))$, if we identify V with its Kirillov model, then for any $\varphi \in V$, quasi-character ξ of $K^\times$, the local Zeta integral $\zeta(\Phi,\xi;s)$(21.3.6.2) is absolutely convergent for $\mathrm{Re}(s)$ sufficiently large, and defines a holomorphic function there. And it has a meromorphic continuation to all s. In fact,

$$\zeta(\Phi,\xi;s) = p_{\varphi,\xi}(q^{-s})L(\pi,\xi;s), \quad p_{\Phi,\xi} \in \mathbb{C}[X,X^{-1}].$$

Moreover, Φ can be chosen s.t. $p_{\Phi,\xi} = 1$. ⌟

Proof: This is by direct calculation: If V is cuspidal, then $V = C_c^\infty(K^\times)$ by(18.11.3.20). If V is not cuspidal, then by(18.11.4.20) it is $\pi(\chi_1,\chi_2)$ or $\sigma(\chi_1,\chi_2)$, whose elements are known(18.11.4.22)(18.11.4.23). For $\mathrm{Re}(s)$ sufficiently large, the $|t| > \mathfrak{q}^{-k}$ part can contribute to any $p(q^{-s})$ for $p \in \mathbb{C}[q^s, q^{-s}]$ with degree$\leq k-1$, and the $|t| \leq q^{-k}$ part is of the form

$$\int_{\mathfrak{p}^k\setminus\{0\}} (\chi_i\xi)(y)|y|^s d^\times y = \sum_{n\geq k}((\chi\xi)(\varpi)q^{-s})^n \int_{\mathcal{O}^*}(\chi_i\xi)(y)d^\times y = C\frac{\alpha_i^k q^{-ks}}{1-\alpha_i q^{-s}},$$

where $C \neq 0$ iff $\chi_i\xi$ is unramified, or of the form

$$\int_{\mathfrak{p}^k\setminus\{0\}} v(y)(\chi_i\xi)(y)|y|^s d^\times y = \sum_{n\geq k} n((\chi\xi)(\varpi)q^{-s})^n \int_{\mathcal{O}^*}(\chi_i\xi)(y)d^\times y = C\frac{\alpha_i^k q^{-ks}}{(1-\alpha_i q^{-s})^2},$$

where $C \neq 0$ iff $\chi_i\xi$ is unramified.

Clearly $p_{\varphi,\xi}$ can be chosen to be 1 if we choose the compactly supported part of φ suitably. □

Prop. (21.3.6.6) [Local Functional Equations]. The local zeta integral $\zeta_v(\Phi_v,\xi_v;s)$, defined in(21.3.6.2) has a meromorphic continuation to all s, and there exists a meromorphic function $\gamma_v(x,\pi_v,\xi_v,\psi_v)$ s.t.

$$\zeta_v(\pi_v(w_1)\Phi_v, \xi_v^{-1}\omega_v^{-1}; 1-s) = \gamma_v(\pi_v,\xi_v,\psi_v;s)\zeta_v(\Phi_v,\xi_v;s).$$

⌟

Proof: This follows by similar method as the proof of(21.3.2.8) and by evaluating $\gamma_v(\pi_v,\xi_v,\psi_v;s)$ explicitly, using methods of Weil representation parallel to the proof of(21.3.6.8), Cf.[Jacquet-Langlands(1970), P37].?

There are easier way to prove this when $v \in \Sigma_F^{\mathrm{fin}}$: We show that both sides are linear functionals on $\Phi \in V$ that satisfies

$$L(\pi(\begin{bmatrix} y & \\ & 1 \end{bmatrix})\varphi) = \xi^{-1}(y)|y|^{-s+1/2}L(\varphi).$$

This is true for RHS by a change of variable and analytic continuation(21.3.6.5), and then also true for LHS.

Thus for general s, (18.11.3.22) shows two sides differ by a scalar $\gamma(s,\pi,\xi,\psi)$. By(21.3.6.5), for general s, both sides can be non-zero, thus $\gamma(s,\pi,\xi,\psi)$ is non-zero, and thus a meromorphic function of s. □

Prop. (21.3.6.7) [Gamma Factor Determines Representations]. For $(\pi_1,V_1),(\pi_2,V_2) \in \mathrm{Irr}^{\mathrm{adm},generic}(GL(2,K))$, if $\gamma(s,\pi_1,\xi,\psi)=\gamma(s,\pi_2,\xi,\psi)$ for any quasi-character ξ of $K^\times$, then $\pi_1\cong\pi_2$. ⌟

Proof: Identify V_i with their Kirillov models, and let $V_0=V_1\cap V_2$. Then it suffices to show that $\pi_1(w_1),\pi_2(w_1)$ acts the same on V_0: This is because V_0 contains $C_c^\infty(K^*)$, and $B(K)$ action on V_1,V_2 are the same by(18.11.3.15), and $GL(2,F)$ is generated by $B(F)$ and w_1. Then $V_0=V_1=V_2$ as they are irreducible representations.

For $\varphi\in V$, let $\varphi_i=\pi_i(w_1)\varphi$, then it suffices to show $\varphi_1(1)=\varphi_2(1)$: For other a,

$$\varphi_i(a)=(\pi_i(\begin{bmatrix}a&\\&1\end{bmatrix}\begin{bmatrix}&1\\-1&\end{bmatrix})\varphi)(1)=(\pi_i(\begin{bmatrix}&1\\-1&\end{bmatrix}\begin{bmatrix}1&\\&a\end{bmatrix})\varphi)(1)$$

and $\pi_1(\begin{bmatrix}1&\\&a\end{bmatrix})\varphi=\pi_2(\begin{bmatrix}1&\\&a\end{bmatrix})\varphi$.

For $n\in\mathbb{Z}$, let

$$F_\xi(n)=\int_{\mathfrak{q}^{-n}\backslash\mathfrak{q}^{-n+1}}(\varphi_1(y)-\varphi_2(y))\xi(y)d^\times y,$$

then $F_\xi(0)$ only depends on the restriction of ξ to $\mathcal{O}^*$, and $F_\xi(0)=0$ for all but f.m. characters ξ of $\mathcal{O}^*$: $\varphi_1-\varphi_2$ is a locally constant function that is fixed by $U\subset\mathcal{O}^*$, so in order $F_\xi(0)\neq 0$, at least ξ should be trivial on U, and there are f.m. such characters. Thus the hypothesis of Fourier transform on $\mathcal{O}^*$ is satisfied(11.10.3.24) and

$$\varphi_1(1)-\varphi_2(1)=\sum_{\xi\in(\mathcal{O}^*)^\wedge}F_\xi(0).$$

The hypothesis and the functional equation(21.3.6.6) shows $Z(s,\varphi_1,\xi)=Z(s,\varphi_2,\xi)$ for any quasi-character ξ of F^*, so

$$\sum_n F_\xi(n)q^{-sn}=Z(s,\varphi_1,\xi)-Z(s,\varphi_2,\xi)=0$$

and $F_\xi(n)=0$ for n sufficiently small, thus $F_\xi(n)=0$ for all n. In particular, $F_\xi(0)=0$, for any ξ. □

Prop. (21.3.6.8) [Gamma Factor Commutes with Parabolic Induction]. If $(\pi,V)=\mathcal{B}(\chi_1,\chi_2)$ is irreducible, then

$$\gamma(s,\mathcal{B}(\chi_1,\chi_2),\xi,\psi)=\gamma(s,\xi\chi_1,\psi)\gamma(s,\xi\chi_2,\psi).$$

⌟

Remark (21.3.6.9). For the compatibility of the gamma factor with parabolic inductions in the GL(n) case, Cf.[Jacquet, H., I. Piatetski-Shapiro and J. Shalika, Rankin-Selberg Convolutions, Am. J. Math., 105 (1981b), 367-464.] or [Jacquet, H. and J. Shalika, Rankin-Selberg Convolutions: Archimedean Theory]. ⌟

Proof: Cf.[Bump, P548].**?** This uses the concrete realization of the Whittaker model of $\mathcal{B}(\chi_1,\chi_2)$ as a quotient of the Weil representation in the split case. □

Jacquet-Langlands L-Functions($\mathrm{GL}(2)\times\mathrm{GL}(1)$ **Case)**

Def. (21.3.6.10) [Local L-Factors for $\mathrm{GL}(2)$**].** Given $\pi\in\mathrm{Irr}^{\mathrm{auto}}(\mathrm{GL}(2)/F,\omega)$, for $v\in\Sigma_F^{\mathrm{fin}}$, the local L-factor is defined to be

$$L(\pi_v;s)=\begin{cases}1 & ,v\in S_{\mathrm{cusp}}(\pi)\\ \frac{1}{(1-\alpha_1q^{-s})(1-\alpha_2q^{-s})}\text{(18.11.5.2)} & ,\pi_v=\pi(\chi_1,\chi_2)\\ \frac{1}{1-\alpha_2q^{-s}} & ,\pi_v=\sigma(\chi_1,\chi_2),\quad \chi_1\chi_2^{-1}=|\cdot|^{-1}\end{cases}$$

It follows from(18.11.4.20) and(18.11.4.2) that any irreducible representation of $GL(2,F_v)$ is one of the form above. Also when ξ is a quasi-character of $F^\times$, define

$$L(\pi_v,\xi_v;s)=L(\pi_v(\xi_v);s).$$

⌟

Prop. (21.3.6.11) [L-Factors as the Common Divisors]. Situation as in(21.3.6.6), $\frac{\zeta_v(\Phi_v,\xi_v;s)}{L_v(\pi_v,\xi_v;s)}$ is entire for any Φ_v,ξ_v, and if $v\in\Sigma_F^{\mathrm{fin}}$, then it is a rational function of $||v||^{-s}$.

Moreover, for each (π_v,V_v), we can take specific $\Phi_v\in V_v$**?** s.t. $\frac{\zeta_v(\Phi_v,\xi_v;s)}{L_v(\pi_v,\xi_v;s)}$ is of the form ab^s for $a\in\mathbb{C}^\times,b\in\mathbb{R}_+$. ⌟

Proof: Cf.[Jacquet-Langlads, GL(2)]. □

Prop. (21.3.6.12) [Local ε-Factors]. Situation as in(21.3.6.6), there exists a non-vanishing holomorphic function $\varepsilon_v(\pi_v,\xi_v,\psi_v;s)$ s.t.

$$\frac{\zeta(\pi(w_1)\Phi_v,\xi_v^{-1};1-s)}{L_v(\widehat{\pi_v},\xi_v^{-1};s)}=\varepsilon_v(\pi_v,\xi_v,\psi_v;s)\frac{\zeta(\Phi_v,\xi_v;s)}{L_v(\pi_v,\xi_v;s)},$$

and $\frac{Z(s,\Phi,\xi)}{L_v(s,\pi_v,\xi_v)}$ is holomorphic. Moreover, $\varepsilon_v(s,\pi_v,\xi_v,\psi_v)$ is of the form ab^s for $a\in\mathbb{C}^*,b\in\mathbb{R}$. And $\varepsilon_v(s,\pi_v,\xi_v,\psi_v)=1$ if v is unramified in the sense of(21.3.6.1). ⌟

Proof: Such a meromorphic $\varepsilon_v(\pi_v,\xi_v,\psi_v;s)$ exists by(21.3.6.6). It is holomorphic and non-vanishing by the same reason as in(21.3.3.3) as both $\frac{\zeta(\Phi_v,\xi_v;s)}{L_v(\pi_v,\xi_v;s)}$ and $\frac{\zeta(\pi(w_1)\Phi_v,\xi_v^{-1};1-s)}{L_v(\widehat{\pi_v},\xi_v^{-1};s)}$ are holomorphic by(21.3.6.11) and for any $s_0\in\mathbb{C}$, Φ_v can be chosen to make either one of them non-vanishing at s_0. To show it is of the form ab^s: If $v\in\Sigma_F^{\mathrm{fin}}$, it is a rational function in $||v||^{-s}$ with no zeros or poles, so it must be of the form ab^s. And if v is unramified, then we can let Φ_v be the spherical function in π_v normalized s.t. $W_{v,\varphi_v}(1)=1$, then $\pi(w_1)\Phi_v$ is the normalized spherical function of $\widehat{\pi}_v$. Then by(14.4.5.5), both sides are 1 by(21.3.6.3).

If $v\in\Sigma_F^\infty$, then we can take Φ_v as in(21.3.6.11) to do the calculation to show it directly, Cf.[Jacquet-Langlads, GL(2)].**?**. □

Prop. (21.3.6.13) [Global L-Functions for $\mathrm{GL}(2)\times\mathrm{GL}(1)$**].** Define

$$L(\pi,\xi;s)=\prod_{v\in\Sigma^{\mathrm{fin}}}L_v(\pi_v,\xi_v;s),\quad \Lambda(\pi,\xi;s)=\prod_v L_v(\pi_v,\xi_v;s)\quad \varepsilon(\pi,\xi;s)=\prod_v\varepsilon_v(\pi_v,\xi_v,\psi_v;s)$$

Then $\varepsilon(\pi,\xi;s)$ is independent of ψ, and $L(s,\pi,\xi)$ satisfies a functional equation

$$\Lambda(\pi,\xi;s)=\varepsilon(\pi,\xi;s)\Lambda(\widehat{\pi},\xi^{-1};s)$$

⌟

Proof: This follows from(21.3.6.12) and(21.3.6.4). □

Prop. (21.3.6.14) [Non-Vanishing on $\mathrm{Re}(s)=1$**].** For $\pi\in\mathrm{Irr}^{\mathrm{cusp}}(\mathrm{GL}(n)/F)$, $L(\pi;s)\neq 0$ on the line $\mathrm{Re}(s)=1$. ⌟

Proof: Cf.[A Non-Vanishing Theorem for Zeta Functions of $\mathrm{GL}(n)$, Jacquet-Shalika(1976)]. □

Modular Forms

Prop. (21.3.6.15) [Trivial Bound]. If $f\in S_k(\Gamma(N))$, suppose $f(z)=\sum_{n\geq 0}a_n e^{2\pi inz/N}$, then $|a_n|=O(n^{k/2})$. ⌟

Proof: $a_n=\int_0^N f(x+iy)e^{-2\pi in(x+iy)/N}dx$ for any y, so let $y=N/n$, then $a_n=\int_0^N f(x+iN/n)e^{-2\pi inx/N}dx$. As f is a cusp modular form, $(\mathrm{Im}(z))^{k/2}|f(z)|$ is cuspidal automorphic function, thus bounded on $\mathcal{H}$, thus $|a_n|\leq C(N/n)^{\frac{k}{2}}$. □

Thm. (21.3.6.16) [Ramanujan-Petersson Conjecture]. Let f be a cuspidal Hecke eigenform of weight k for $\Gamma(1)$, then for any prime p, $|a_p(f)|\leq 2p^{(k-1)/2}$. ⌟

Proof: By(20.2.2.12) this means the eigenvalue λ_p of f w.r.t. T_p satisfies $|\lambda_p|\leq 2p^{1/2}$. This is a consequence of Weil conjecture and modularity**?**. □

Def. (21.3.6.17) [L-functions associated to Modular Forms]. Each $f\in M_k(\Gamma_1(N))$ has an associated L-functions: if $f=\sum_{n=0}^\infty a_n q^n$, define

$$L(s,f)=\sum_{n=1}^\infty a_n n^{-s}.$$

⌟

Prop. (21.3.6.18) [Functional Equations of Modular Forms, Hecke]. Let $a_0,a_1,\ldots$ be a sequence of complex numbers s.t. $a_n=O(n^M)$ for some integer M. Given $\lambda>0,k>0,C=\pm 1$, write

$$\varphi(s)=\sum_{n=1}^\infty a_n n^{-s},\quad \Phi(s)=(\frac{2\pi}{\lambda})^{-s}\Gamma(s)\varphi(s),\quad f(z)=\sum_{n=0}^\infty a_n e^{2\pi inz/\lambda}.$$

Then the following conditions are equivalent:

- The function $\Lambda(s)=\Phi(s)+\frac{a_0}{s}+\frac{Ca_0}{k-s}$ can be analytically continued to a holomorphic function of the whole plane which is bounded on vertical strips, and it satisfies the functional equation
$$\Phi(s)=C\Phi(k-s).$$
- In the upper half plane, f satisfies the functional equation
$$f(-1/z)=C(z/i)^k f(z).$$

⌟

Proof: Notice first

$$\int_0^\infty e^{-2\pi nt/\lambda}t^s\frac{dt}{t}=(\frac{2\pi}{n\lambda})^{-s}\int_0^\infty e^{-t}t^s\frac{dt}{t}=(\frac{2\pi}{n\lambda})^{-s}\Gamma(s).$$

Thus for $\mathrm{Re}(s)$ large,

$$\Phi(s)=\int_0^\infty(f(it)-a_0)t^s\frac{dt}{t}=\int_1^\infty(f(it)-a_0)t^s\frac{dt}{t}+\int_1^\infty(f(\frac{i}{t})-a_0)t^{-s}\frac{dt}{t}.$$

If 2 holds, then $f(\frac{i}{t})=Ct^kf(it)$, and

$$\begin{aligned}\Phi(s)&=\int_1^\infty(f(it)-a_0)t^s\frac{dt}{t}+\int_1^\infty(Ct^kf(it)-a_0)t^{-s}\frac{dt}{t}\\&=\int_1^\infty(f(it)-a_0)t^s\frac{dt}{t}+C\int_1^\infty(f(it)-a_0)t^{k-s}\frac{dt}{t}+\int_1^\infty(Ct^{k-s}a_0-t^{-s}a_0)\frac{dt}{t}.\end{aligned}$$

The first two integral is absolutely convergent for any s and then can be extended to an analytic function of the whole plane, and the final term equals

$$-(\frac{a_0}{s}+\frac{Ca_0}{k-s})$$

when $\mathrm{Re}(s)$ is large, so it can be extended to a meromorphic function on the whole plane. And $\Phi(s)=\Phi(k-s)$ follows easily from the equation above. Also it is bounded on vertical strips because it attain maximum at the real axis.

Conversely, first notice it suffices to prove for real $y>0$,

$$f(\frac{\mathrm{i}}{y})=Cy^kf(\mathrm{i}\,y)$$

because this implies these two holomorphic functions on $\mathcal{H}$ coincide on the imaginary axis, so they must be equal. Notice

$$\int_0^\infty(f(iy)-a_0)y^s\frac{dy}{y}=\Phi(s)$$

converges absolutely for $\mathrm{Re}(s)$ sufficiently large, so for $\sigma>0$ sufficiently large, Mellin inversion formula(11.11.2.16) shows

$$\begin{aligned}f(iy)-a_0&=\frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty}\Phi(s)y^{-s}ds=\frac{C}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty}\Phi(k-s)y^{-s}ds\\&=\frac{C}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty}(\Lambda(k-s)-\frac{Ca_0}{s}-\frac{a_0}{k-s})y^{-s}ds\end{aligned}$$

Notice $\Phi(\sigma+it)$ decays exponentially for fixed $\sigma=\alpha$ sufficiently large, because of the Stirling formula(11.6.1.12), and for $\sigma=\beta$ sufficiently small, $\Phi(s)=C\Phi(k-s)$ also shows $\Phi(\sigma+it)$ decays exponentially. And also $\frac{Ca_0}{\sigma+it}+\frac{a_0}{k-\sigma-it}=O(t^{-1})$ for $\sigma=\alpha$ or β, so $\Lambda(\sigma+it)=O(t^{-1})$ for σ large or small, and also the hypothesis shows Λ is bounded on the strip $\alpha<\mathrm{Re}(z)<\beta$, thus by(11.4.5.7), $\Lambda(\sigma+it)\to 0$ for $t\to 0$ and σ in any compact set. So we can move the integration of $\Lambda(s)$ to the left or to the right. Then

$$f(iy)-a_0=\frac{C}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty}(\Lambda(k-s)-\frac{Ca_0}{s}-\frac{a_0}{k-s})y^{-s}ds$$

$$
\begin{aligned}
&= \frac{C}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} y^{-k}\Lambda(s)y^s ds - \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty}(\frac{a_0}{s}+\frac{Ca_0}{k-s})y^{-s}ds\\
&= \frac{Cy^{-k}}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty}\Phi(s)y^s ds + \frac{Cy^{-k}}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty}(\frac{a_0}{s}+\frac{Ca_0}{k-s})y^s ds + \frac{1}{2\pi i}\int_{k-\sigma+i\infty}^{k-\sigma-i\infty}(\frac{a_0}{k-s}+\frac{Ca_0}{s})y^{s-k}ds\\
&= Cy^{-k}(f(\frac{i}{y})-a_0)+\frac{y^{-k}}{2\pi i}\int_\gamma(\frac{Ca_0}{s}+\frac{a_0}{k-s})y^s ds\\
&= Cy^{-k}f(\frac{i}{y}) - Ca_0y^{-k}+y^{-k}(Ca_0-a_0y^k) = Cy^{-k}f(\frac{i}{y})-a_0
\end{aligned}
$$

So we are done. □

Def. (21.3.6.19)[L-Functions associated to $S_k(1)$]. Let $a_1, a_2, \ldots$ be a sequence of complex numbers such that $a_n = O(n^M)$ for some $M > 0$. Let

$$L(s) = \sum a_n n^{-s}, \quad \Lambda(s) = L_{\mathbb{C}}(s)L(s), \quad f(z) = \sum a_n e^{-2\pi i nz}.$$

More generally, let $m > 0$ and χ a primitive character mod m, then we define **twisted L-function** as

$$L(f,\chi;s) = \sum a_n\chi(n)n^{-s}, \quad \Lambda(f,\chi;s) = L_{\mathbb{C}}(s)L(f,\chi;s)$$

Notice if $f(x) \in S_k(\Gamma(1))$, and $\pi_f \in \mathrm{Irr}^{\mathrm{auto}}(\mathrm{GL}(2)/\mathbb{Q})$ corresponding to f via(20.5.2.12), then

$$L(f,\chi;s) = L(\pi_f,\chi;s).$$

⌟

Prop. (21.3.6.20) [Converse Theorem(Correspondence for $\Gamma(1)$)]. If $f \neq 0 \in S_k(\Gamma(1))$(so $2|k$), then $\Lambda(f;s)$(21.3.6.19) has analytic continuation to all $s \in \mathbb{C}$, is bounded on vertical strips, and satisfies a functional equation

$$\Lambda(s,f) = (-1)^{k/2}\Lambda(k-s,f).$$

Conversely, let $a_0, a_1, \ldots$ be a sequence of complex numbers that $a_n = O(n^M)$ for some $M > 0$. Let $f(s), L(s), \Lambda(s)$ be defined in(21.3.6.19) and $\Lambda(f;s)$ has analytic continuation to all s and satisfies the above functional equation, then $f(z) \in S_k(\Gamma(1))$.

Moreover, in this case, f is a normalized Hecke eigenform(20.2.2.12) iff $L(s,f)$ has as Euler product formula

$$L(s) = \prod_p (1 - a_p p^{-s} + p^{k-1-2s})^{-1}$$

for s sufficiently large, where $1 - a_s X + p^{k-1}X^2 = (1-aX)(1-\overline{a}X)$, where $|a| = p^{\frac{k-1}{2}}$. ⌟

Proof: The first part is a direct consequence of(21.3.6.18). Notice a_n is bounded by polynomials in n by(21.3.6.15).

When s is large, the Euler product is absolutely convergent, thus it suffices to compare the coefficients. By(20.2.2.12) and(20.2.2.10), f being a normalized Hecke eigenform is equivalent to

$$\begin{cases} c_m c_n = c_{mn}, & (m,n) = 1\\ c_p c_{p^n} = c_{p^{n+1}} + p^{2k-1}c_{p^{k-1}} \end{cases}$$

which is equivalent to

$$(1 - a_p X + p^{k-1}X^2)(\sum_{r=0}^\infty a_{p^r}X^r) = 1.$$

□

Prop. (21.3.6.21) [Functional Equation associated to $S_k(N,\psi)$]. Notation as in(21.3.6.19). If $f(z)\in S_k(N,\psi)$(20.2.1.16). Let w_N be the Fricke involution(20.2.1.4), and notice $\psi(a_\gamma)=\overline{\psi(d_\gamma)}$, so

$$f[w_N]_k[\gamma]_k=f[w_N\gamma w_N^{-1}]_k[w_N]_k=\overline{\psi(d)}f[w_N].$$

Thus $g=f[w_N]_k\in S_k(N,\overline{\psi})$.

Now if

$$f(z)=\sum a_n e^{2\pi\mathrm{i}nz/N},g(z)=\sum b_n e^{2\pi\mathrm{i}nz/N},$$

and χ is a primitive character mod D, define $L(s,f,\chi),L(s,g,\overline{\chi}),\Lambda(s,f,\chi),\Lambda(s,g,\overline{\chi})$ as in(21.3.6.19), then $\Lambda(s,f,\chi)$ extends to an analytic function for all $s\in\mathbb{C}$, and there are functional equations

$$\Lambda(f,\chi;s)=\mathrm{i}^k\,\chi(N)\psi(D)\frac{\tau(\chi)^2}{D}(D^2N)^{-s+k/2}\Lambda(g,\overline{\chi};k-s),\tag{21.1}$$

where $\tau(\chi)$ is the Gauss sum of χ(17.3.3.3).

In particular, if $D=1$(and thus $\chi=\mathbb{1}$), then

$$\Lambda(f;s)=\mathrm{i}^k\,N^{-s+k/2}\Lambda(g;k-s).\tag{21.2}$$

⌟

Proof: Let

$$f_\chi(z)=\sum\chi(n)a_nq^n,\quad g_{\overline{\chi}}(z)=\sum\overline{\chi(n)}b_nq^n.$$

Use(17.3.3.7) on $f_\chi(z)$, we get

$$f_\chi=\frac{\chi(-1)\tau(\chi)}{D}\sum_{m\in(\mathbb{Z}/D\mathbb{Z})^*}\overline{\chi(m)}f[\begin{bmatrix}D&m\\&D\end{bmatrix}]_k$$

Now

$$\begin{aligned}f_\chi[\begin{bmatrix}&-1\\D^2N&\end{bmatrix}]_k=f_\chi[\begin{bmatrix}&-1/DN\\D&\end{bmatrix}]_k&=\frac{\chi(-1)\tau(\chi)}{D}\sum_{m\in(\mathbb{Z}/D\mathbb{Z})^*}\overline{\chi(m)}g[w_N^{-1}]_k[\begin{bmatrix}D&m\\&D\end{bmatrix}]_k[\begin{bmatrix}&-1/DN\\D&\end{bmatrix}]_k\\&=\frac{\chi(-1)\tau(\chi)}{D}\sum_{m\in(\mathbb{Z}/D\mathbb{Z})^*}\overline{\chi(m)}g[\begin{bmatrix}D&-r\\-Nm&s\end{bmatrix}\begin{bmatrix}D&r\\&D\end{bmatrix}]_k\end{aligned}$$

where (r,s) are integers chosen that $Ds-rNm=1$. Thus $\overline{\chi(m)}=\chi(-N)\chi(r)$, and because $g\in M_k(N,\overline{\psi})$,

$$f_\chi[\begin{bmatrix}&-1\\D^2N&\end{bmatrix}]_k=\frac{\chi(N)\tau(\chi)}{D}\sum_{r\in(\mathbb{Z}/D\mathbb{Z})^*}\chi(r)\psi(D)g[\begin{bmatrix}D&r\\&D\end{bmatrix}]_k.$$

Compare this with the formula

$$g_{\overline{\chi}}=\frac{\chi(-1)\tau(\overline{\chi})}{D}\sum_{m\in(\mathbb{Z}/D\mathbb{Z})^*}\chi(m)g[\begin{bmatrix}D&m\\&D\end{bmatrix}]_k,$$

we get

$$f_\chi[\begin{bmatrix}&-1\\D^2N&\end{bmatrix}]_k=\chi(-N)\psi(D)\frac{\tau(\chi)}{\tau(\overline{\chi})}g_{\overline{\chi}}=\chi(N)\psi(D)\frac{\tau(\chi)^2}{D}g_{\overline{\chi}}\text{(17.3.3.4)(17.3.3.6)}.\tag{21.3}$$

Now similar to the proof of(21.3.6.18),

$$\Lambda(s,f,\chi)=\int_0^\infty f_\chi(iy)y^s\frac{dy}{y}.$$

So when $\mathrm{Re}(s)$ is large,

$$\begin{aligned}\chi(N)\psi(D)\frac{\tau(\chi)^2}{D}\Lambda(s,g,\overline{\chi})&=\chi(N)\psi(D)\frac{\tau(\chi)^2}{D}\int_0^\infty g_{\overline{\chi}}(iy)y^s\frac{dy}{y}\\&=\int_0^{D\sqrt{N}}(D^2N)^{-k/2}(iy)^{-k}f_\chi(\frac{1}{-D^2Niy})y^s\frac{dy}{y}+\chi(N)\psi(D)\frac{\tau(\chi)^2}{D}\int_{D\sqrt{N}}^\infty g_{\overline{\chi}}(iy)y^s\frac{dy}{y}\\&=\int_{D\sqrt{N}}^\infty(D^2N)^{k/2}t^ki^{-k}f_\chi(it)(D^2Nt)^{-s}\frac{dt}{t}+\chi(N)\psi(D)\frac{\tau(\chi)^2}{D}\int_{D\sqrt{N}}^\infty g_{\overline{\chi}}(iy)y^s\frac{dy}{y}\\&=i^{-k}(D^2N)^{k/2-s}\int_{D\sqrt{N}}^\infty f_\chi(it)t^{k-s}\frac{dt}{t}+\chi(N)\psi(D)\frac{\tau(\chi)^2}{D}\int_{D\sqrt{N}}^\infty g_{\overline{\chi}}(iy)y^s\frac{dy}{y}\end{aligned}$$

Both integral are absolutely convergent for any s. And similarly when $\mathrm{Re}(s)$ is small,

$$\begin{aligned}i^{-k}(D^2N)^{k/2-s}\Lambda(k-s,f,\chi)&=i^{-k}(D^2N)^{k/2-s}\int_0^\infty f_\chi(it)t^{k-s}\frac{dt}{t}\\&=i^{-k}(D^2N)^{k/2-s}\int_{D\sqrt{N}}^\infty f_\chi(it)t^{k-s}\frac{dt}{t}+\chi(N)\psi(D)\frac{\tau(\chi)^2}{D}\int_{D\sqrt{N}}^\infty g_{\overline{\chi}}(iy)y^s\frac{dy}{y}\end{aligned}$$

Thus we get the desired result. □

Cor. (21.3.6.22). As $f[w_N^2]_k=(-1)^kf$, if $f\in S_k(\Gamma_1(N))$ satisfies $f[w_N]_k=cf$, $c=\varepsilon i^k$, $\varepsilon=\pm1$, then

$$N^{s/2}\Lambda(s,f)=\varepsilon(-1)^kN^{(k-s)/2}\Lambda(k-s,f).$$

so $\mathrm{ord}_{1/2}(L(s,f))$ is even if $\varepsilon=(-1)^k$ and odd if $\varepsilon=(-1)^{k+1}$.

In particular, if $N=1$ and $k\equiv 2 \mod 4$, $L(1/2,f)=0$.

It is conjectured that $L(1/2,f)\neq 0$ if $4|k$, Cf.[Modular Forms, Ribet] P148.**?** ⌟

Prop. (21.3.6.23) [Converse Theorem, Weil]. Let $N>0$ and ψ a character mod N. Suppose a_n,b_n are two sequence of complex numbers that $|a_n|,|b_n|=O(n^M)$ for some positive integer M. If $(D,N)=1$ and χ is a primitive character mod D, let

$$L_1(s,\chi)=\sum\chi(n)a_nn^{-s},\quad L_2(s,\overline{\chi})=\sum\overline{\chi(n)}b_nn^{-s}.$$

and $\Lambda_i(s,\chi_i)=L_\mathbb{C}(s)L_i(s,\chi_i)$.

Now if for D equals to a.e. p and any primitive character mod D, $\Lambda_i(s,\chi)$ has analytic continuation to all s, are bounded on vertical strips, and satisfy the functional equation

$$\Lambda_1(s,\chi)=\mathrm{i}^k\,\chi(N)\psi(D)\frac{\tau(\chi)^2}{D}(D^2N)^{-s+k/2}\Lambda_2(k-s,\overline{\chi}),$$

where $\tau(\chi)$ is the Gauss sum of χ(17.3.3.3), then $f(z)=\sum a_ne^{2\pi\mathrm{i}nz}\in M_k(N,\psi)$. ⌟

Proof: Let
$$f_\chi(z) = \sum \chi(n)a_n q^n, \quad g_{\overline{\chi}}(z) = \sum \overline{\chi(n)} b_n q^n.$$
We first show equation21.3 holds. As in the proof of(21.3.6.18), it suffices to show the functional equation it is true on the positive imaginary axis. If $\sigma = \mathrm{Re}(s)$ is sufficiently large, then
$$\int_0^\infty f_\chi(iy)y^s \frac{dy}{y} = \Lambda_1(s,\chi)$$
so by Mellin inversion formula
$$f_\chi(iy) = \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} \Lambda_1(s,\chi)y^{-s}ds = i^k\chi(N)\psi(-D)\frac{\tau(\chi)^2}{D}\frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty}(D^2N)^{-s+k/2}\Lambda_2(k-s,\overline{\chi})ds$$

Same argument of Phragmén-Lindelöf principle as in proof of(21.3.6.18) shows $\Lambda_2(\sigma+it,\overline{\chi})$ converges to 0 for $t\to\infty$, uniformly on any compact subset, so we can move the integral horizontally and make a change of variable $s\mapsto k-s$ to get
$$\begin{aligned} f_\chi(iy) &= i^k\chi(N)\psi(-D)\frac{\tau(\chi)^2}{D}(D^2N)^{-k/2}y^{-k}\frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty}\Lambda_2(k-s,\overline{\chi})(D^2Ny)^s ds \\ &= i^k\chi(N)\psi(-D)\frac{\tau(\chi)^2}{D}(D^2N)^{-k/2}y^{-k}g_{\overline{\chi}}(\frac{i}{D^2Ny}) \end{aligned}$$
which is equivalent to21.3.

The rest is to manipulate 2×2 matrices and use(20.1.1.10) to show that $g\in M_k(N,\overline{\psi})$, Cf.[Bump, P62]**?**. □

Remark (21.3.6.24). For $\Gamma(1)$, the function only requires one functional equation, and we used the fact $\Gamma(1)$ is generated by S and T. But $\Gamma_0(N)$ is not generated by two elements, so we must assume functional equations for the twists $L(s,f,\chi)$ also. ⌟

Maass Forms

See Wei's notes.

7 Langlands-Shahidi Method

8 Triple Product

Cf.[Bump]

21.4 Dirichlet L-Functions and Theory of Primes

References are [Analytic Number Theory, Iwaniec-Kowaiski].

Notation (21.4.0.1).
- Let $F \in \mathtt{NField}$.

⌟

1 Representing Primes

Conj. (21.4.1.1) [Hardy-Littlewood]. There are infinitely many primes of the form $n^2 + 1, n \in \mathbb{Z}_+$. ⌟

Proof: □

Prop. (21.4.1.2). If $\underline{X} = (X_1, \ldots, X_n)$ and $f(\underline{X}) \in \mathbb{C}[\underline{X}]$ only takes values in $\mathbf{P}$ at non-negative integer points, then f is constant. ⌟

Proof: □

Prop. (21.4.1.3). There is an integral polynomial of degree 25 in 26 variables that its only positive values at integer points are primes. ⌟

Proof: Cf.[J. P. Jones, D. Sato, H. Wada and D. Wiens, "Diophantine representation of the set of prime numbers," Amer. Math. Monthly, 83 (1976) 449-464.]. □

Prop. (21.4.1.4) [Landau]. For $n \in \mathbb{Z}_+$, let $f(n)$ be the cardinality of numbers in $[n]_+$ that can be written as the form $x^2 + y^2$, then $f(n) = O(\frac{n}{\sqrt{\log n}})$. ⌟

Proof: ? □

Representing Primes by Quadratic Forms

References are [Primes of the form $x^2 + ny^2$, Cox].

Prop. (21.4.1.5) [Quadratic Forms]. For $D \in \mathbb{Z}_{<0}$ and $D \equiv 0, 1 (\text{mod } 4)$, the equivalence classes of quadratic forms $AX^2 + BXY + CY^2$ with discriminant D is in bijection with the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))$. ⌟

Thm. (21.4.1.6) [Representing Primes]. For any $n \in \mathbb{Z}_+$, there is a monic irreducible polynomial $f_n(T) \in \mathbb{Z}[T]$ of degree $h(-4n)$ s.t.:
For $p > 2 \in \mathbf{P}$ dividing neither n nor the discriminant of $f_n(T)$,

$$p \in \{x^2 + ny^2 | x, y \in \mathbb{Z}\} \iff \left(\frac{-n}{p}\right) = 1 \vee \{x \in \mathbb{Z} | f_n(x) = 0 \in \mathbb{F}_p\} \neq \varnothing.$$

Moreover, $f_n(T)$ is the minimal polynomial of a real algebraic integer α s.t. $L = K(\alpha)$ is ring class field of the order $\mathbb{Z}[\sqrt{-n}] \in K = \mathbb{Q}(\sqrt{-n})$, and any such f is of this form. ⌟

Proof: Cf.[Cox, $p = x^2 + ny^2$]P163.? □

Cor. (21.4.1.7). Let $p \in \mathbf{P}$, then

- $$\exists(x,y\in\mathbb{Z})p=x^2+y^2 \iff p\equiv 1 (\mathrm{mod}\ 4).$$
- $$\exists(x,y\in\mathbb{Z})p=x^2+2y^2 \iff p\equiv 1,3 (\mathrm{mod}\ 8).$$
- $$\exists(x,y\in\mathbb{Z})p=x^2+3y^2 \iff p=3\,\mathrm{or}\,p\equiv 1 (\mathrm{mod}\ 3).$$
- $$\exists(x,y\in\mathbb{Z})p=x^2+5y^2 \iff p\equiv 1,9 (\mathrm{mod}\ 2)0.$$
- $$\exists(x,y\in\mathbb{Z})p=x^2+27y^2 \iff \Big\{p\equiv 1 \mod 3\Big\}\wedge\Big\{\exists a,p|a^3-2\Big\}.$$
- $$\Big\{\exists(x,y\in\mathbb{Z})p=x^2+27y^2\Big\}\,\mathrm{or}\,\Big\{\exists(x,y\in\mathbb{Z})p=4x^2+2xy+7y^2\Big\} \iff p\equiv 1 \mod 3.$$

⌟

Proof:

□

Prop. (21.4.1.8). Let $ax^2+bxy+cy^2$ be a primitive definite quadratic form of discriminant $D<0$, and let $\mathscr{S}=\{p\in\mathbf{P}|p=ax^2+bxy+cy^2,\exists x,y\in\mathbb{Z}\}$, then $\mathscr{S}$ has Dirichlet density

$$\delta(\mathscr{S})=\begin{cases}\frac{1}{\mathrm{cl}(D)} & ,ax^2+bxy+cy^2 \text{ is properly equivalent to its opposite}\}\\ \frac{1}{\mathrm{cl}(D)} & ,\text{otherwise}\end{cases}.$$

⌟

Proof: Cf.[Cox13]P170. □

2 Dirichlet-Weber L-Functions

References are [Mil20].

Def. (21.4.2.1)[Partial L-Functions]. If $\mathfrak{m}$ is a modulus for F, $\mathcal{R}\subset\mathrm{Cl}_{\mathfrak{m}}(F)$ be an ideal class. Define the **partial L-function**

$$\zeta(F,\mathcal{R};s)=\sum_{\mathfrak{a}\in\mathcal{R}}\frac{1}{||\mathfrak{a}||^s}.$$

⌟

Prop. (21.4.2.2). Situation as in(21.4.2.1), $\zeta(F,\mathcal{R};s)$ is analytic for $\mathrm{Re}(s)>1-1/N$ except a simple pole at $s=1$, where it has residue $g_{\mathfrak{m}}$ depending only on $\mathfrak{m}$. ⌟

Proof: Cf.[Class Field Theory, Milne]. □

Prop. (21.4.2.3) [Weber L-Functions]. If $\mathfrak{m}$ is a modulus for F, $\chi : \mathrm{Cl}_{\mathfrak{m}}(F) \to \mathbb{C}^\times$ a Dirichlet character for F, then the **Weber L-function** attached to χ is defined to be the Euler product

$$L(F,\chi;s) = \prod_{\mathfrak{p}\nmid\mathfrak{m}} \frac{1}{1-\chi(\mathfrak{p})||\mathfrak{p}||^{-s}} = \sum_{(\mathfrak{a},\mathfrak{m})=1} \frac{\chi(\mathfrak{a})}{||N\mathfrak{a}||^s} = \sum_{\mathcal{R}\in\mathrm{Cl}_{\mathfrak{m}}(F)} \chi(\mathcal{R})\zeta(F,\mathcal{R};s).$$

Thus by(21.4.2.2), $L(K,\chi;s)$ is analytic for $\mathrm{Re}(s) > 1-1/N$, except for possibly a simple pole at $s=1$. And for $\chi \neq 1$, it is in fact analytic at $s=1$, as the residues cancelled out. ⌟

Def. (21.4.2.4) [Dirichlet L-Functions]. For $F=\mathbb{Q}$, the characters of $\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q})$ are just Dirichlet characters χ(14.4.4.32), thus the Weber L-function is

$$L(s,\chi) = \sum_{n=1}^\infty \frac{\chi(n)}{n^s},$$

where $\mathrm{Re}\, s > 1$. Called the **Dirichlet L-function** attached to χ. ⌟

Prop. (21.4.2.5)[Functional Equation for Dirichlet L-Functions]. Let χ be a Dirichlet character with $\chi(-1) = (-1)^\varepsilon$ where $\varepsilon = 0$ or 1, then

$$\Lambda(\chi;s) = L_{\mathbb{R}}(s+\varepsilon)L(\chi;s),$$

is the Hecke L-function attached to the Hecke character corresponding to χ(14.4.4.32)(21.3.3.5). Thus $L(s,\chi)$ can be extended to a meromorphic function for all $s\in\mathbb{C}$, and it has simple poles at $s=0,1$ when $\chi=1$, and analytic otherwise. When $\chi=1$, by(21.4.3.2),

$$\mathrm{res}_{s=1} L(1;s) = 1.$$

Moreover, there are functional equations

$$\Lambda(\chi;s) = (-\mathrm{i})^\varepsilon \tau(\chi) N^{-s} \Lambda(\chi^{-1};1-s)\text{(17.3.3.3)},$$

In other words,

$$\varepsilon(\chi;s) = (-\mathrm{i})^\varepsilon \tau(\chi) N^{-s}.$$

⌟

Proof: Cf.[Bum98]P10. □

Prop. (21.4.2.6). Let χ be a Dirichlet character modulo N, then

$$\begin{aligned} L(\chi;1) &= \frac{-\tau(\chi)}{N} \sum_{n\in\mathbb{Z}/(N)} \chi^{-1}(n)\log(1-e^{-2\pi\mathrm{i}\,n/N}) \\ &= \begin{cases} \frac{\tau(\chi)}{N^2}\pi\,\mathrm{i}\sum_{n\in\mathbb{Z}/(N)}\chi^{-1}(n)n & ,\chi(-1)=-1 \\ \frac{-\tau(\chi)}{N}\sum_{n\in\mathbb{Z}/(N)}\chi^{-1}(a)\log|1-e^{-2\pi\mathrm{i}\,n/N}| & ,\chi(-1)=1 \end{cases} \end{aligned}$$

⌟

Proof: Use Fourier transform**?**. □

Prop. (21.4.2.7). If $F\in \mathtt{NField}$ and $\chi \neq \mathbb{1}$ is a Hecke character on F, then $L(\chi;1+\mathrm{i}\,t) \neq 0$ for any $t\in\mathbb{R}$. ⌟

Proof: Cf.[GTM186, P289].?

We prove for $F=\mathbb{Q}$ and $\chi=1$: If ζ has a zero at $x+\mathrm{i}\,y$ for $y\neq 0$, then by(21.4.2.5), $\zeta(s)$ has a simple pole at $s=1$ and holomorphic at $s=x+2\,\mathrm{i}\,y$. But by(21.4.2.8)

$$\lim_{x\to 0^+}|\zeta(x)^3\zeta(x+\mathrm{i}\,y)^4\zeta(x+2\,\mathrm{i}\,y)|\geq 1,$$

contradiction. □

Lemma (21.4.2.8) [Mertens]. For $x,y\in\mathbb{R}$ with $x>1$, $|\zeta(x)^3\zeta(x+\mathrm{i}\,y)^4\zeta(x+2\,\mathrm{i}\,y)|\geq 1$. ⌟

Proof: For $s=x+\mathrm{i}\,y$,

$$\log|\zeta(s)|=-\sum_{p\in\mathbf{P}}\log|1-p^{-s}|=-\sum_{p\in\mathbf{P}}\mathrm{Re}\log(1-p^{-s})=\sum_{p\in\mathbf{P}}\sum_{n\in\mathbb{Z}_+}\frac{\mathrm{Re}(p^{-ns})}{n},$$

so

$$\log|\zeta(x+\mathrm{i}\,y)|=\sum_{p\in\mathbf{P}}\sum_{n\in\mathbb{Z}_+}\frac{\cos(ny\log p)}{np^{nx}}.$$

So

$$\begin{aligned}\log|\zeta(x)^3\zeta(x+\mathrm{i}\,y)^4\zeta(x+2\,\mathrm{i}\,y)|&=\sum_{p\in\mathbf{P}}\sum_{n\in\mathbb{Z}_+}\frac{3+4\cos(ny\log p)+\cos(2ny\log p)}{np^{nx}}\\&=\sum_{p\in\mathbf{P}}\sum_{n\in\mathbb{Z}_+}\frac{2(\cos(ny\log p)+1)^2}{np^{nx}}\geq 0\end{aligned}$$

□

Estimates

Prop. (21.4.2.9) [Louboutin]. Let χ be a Dirichlet character modulo $N>1$, then

$$|L(\chi;1)|\leq\begin{cases}\frac{1}{2}\log N+0.009 & .\chi(-1)=1\\ \frac{1}{2}\log N+0.716 & ,\chi(-1)=-1\end{cases}.$$

⌟

Proof: Cf.[S. Louboutin, Majorations explicites de $|L(1,\chi)|$]. □

Remark (21.4.2.10). It is easy to show that $|L(\chi;1)\leq\log(N)+C$:

$$\begin{aligned}|L(\chi;1)|&\leq|\sum_{n\leq N}\frac{\chi(n)}{n}|+|\sum_{n>N}\frac{\chi(n)}{n}|\\&\leq\sum_{n\leq N}\frac{1}{n}+\Big|\int_N^\infty(\sum_{N<n\leq t}\chi(n))\frac{\mathrm{d}t}{t^2}\Big|\\&\leq 1+\int_1^{N-1}\frac{\mathrm{d}t}{t}+\frac{1}{N}\max_X|\sum_{N<n\leq t}\chi(n)|\\&<\log N+1+\frac{\varphi(N)}{N}\end{aligned}$$

⌟

Thm. (21.4.2.11) [Zhang]. If χ is a real primitive Dirichlet character modulo $D > 1$, then there exists an absolute effectively computable constant $c_1 > 0$ s.t.

$$L(\chi;1) > C(\log D)^{-2022}$$

⌟

Proof: Cf.[Yitang Zhang, Discrete mean estimates and the Landau-Siegel zero]. □

Cor. (21.4.2.12). If χ is a real primitive Dirichlet character modulo $D > 1$, then there exists an absolute effectively computable constant $c_1 > 0$ s.t.

$$L(\sigma,\chi) \neq 0, \quad \sigma > 1 - c_2(\log D)^{-2024}.$$

⌟

Proof: **?** □

Cor. (21.4.2.13) [Siegel]. Let χ be a real primitive Dirichlet character modulo $N > 1$, then for any $\varepsilon > 0$, there exists $C(\varepsilon) > 0$ s.t.

$$L(1,\chi) \geq \frac{C(\varepsilon)}{q^\varepsilon}.$$

⌟

Proof: There is a direct proof of this theorem in**??** and [A simple proof of Siegel's theorem via Mellin's transform]. □

3 Riemann L-Functions

Def. (21.4.3.1) [Riemann L-Functions]. $\zeta(F;s) = L(F,\mathbb{1};s)$ is called the **Riemann L-function** for F. Also denote

$$\zeta(s) = \zeta(\mathbb{Q};s), \quad \Lambda(s) = \Lambda(\mathbb{Q},\mathbb{1};s) = L_\mathbb{R}(s)\zeta(s)\text{(11.6.1.13)}.$$

By(21.4.2.5), $\zeta(s)$ extends to a meromorphic function for all $s \in \mathbb{C}$ with a simple pole at $s = 1$. And there is a functional equation

$$\Lambda(s) = \Lambda(1-s).$$

⌟

Thm. (21.4.3.2) [Class Number Formula, Dirichlet]. By(21.3.3.6)(14.4.5.20),

$$\operatorname{res}_{s=1}\zeta(F;s) = \frac{2^{r_1}(2\pi)^{r_2}}{w(F)\sqrt{|d_F|}}\operatorname{cl}(F)\operatorname{Reg}(F)$$

where $w(F) = \#\mu(F)$, and $\operatorname{Reg}(F)$ is the regulator of F(14.4.1.27). In particular,

$$\operatorname{res}_{s=1}\zeta_\mathbb{Q}(s) = 1.$$

⌟

Prop. (21.4.3.3) [Dirichlet's Class Number Formula for Quadratic Fields]. Let $\mathcal{K} = \mathbb{Q}(\sqrt{D})$ be a quadratic field with discriminant D, and χ_D the (real)Dirichlet character associated to K, and $\varepsilon = 0$(resp. 1) if $\mathcal{K}$ is real(resp. complex), then

- The root number of χ_D(21.3.3.7) is given by

$$W(\chi_D)=\frac{\tau(\chi)}{\sqrt{|D|}}(-1)^{\varepsilon}\in\{\pm 1\}\in\{-1,1\},$$

- if $D<0$, then

$$\mathrm{cl}(\mathcal{K})=\frac{w(\mathcal{K})\sqrt{|D|}}{2\pi}L(\chi_D;1)=\frac{w(\mathcal{K})\,\mathrm{i}}{2|D|}\cdot\frac{\tau(\chi_D)}{\sqrt{|D|}}\cdot\sum_{a\in\mathbb{Z}/(D)}\chi(a)=\frac{w(\mathcal{K})W(\chi_D)\,\mathrm{i}}{2D}\cdot\sum_{a\in\mathbb{Z}/(D)}\chi(a)a.$$

⌟

Proof: For 1: Cf. [GTM 218]P305-306, Ex.14-15.?
For 2, in this case $r_1=0, r_2=1$, so $\mathrm{Reg}(\mathcal{K})=1$, and the rest follows from(21.2.1.8)(21.4.2.5)(21.4.2.6) and item1. □

Prop. (21.4.3.4) [Kronecker's First Limit Formula].

$$\zeta(s)=\frac{1}{s-1}+\gamma_0+O(s-1).$$

⌟

Proof: Cf.[Kronecker's First Limit Formula, Revisited]. This can be deduced from(21.1.1.4).? □

Remark (21.4.3.5). This is related to the the averaged Colmez's conjecture?. ⌟

Relation to Summations

Def. (21.4.3.6) [von Mangoldt Function]. The **von Mangoldt function** is defined to be

$$\Lambda:\mathbb{Z}_+\to\mathbb{R}:\Lambda(n)=\begin{cases}\log p & ,p\in\mathbf{P},n\in p^{\mathbb{Z}_+}\\ 0 & ,\text{otherwise}\end{cases}.$$

⌟

Def. (21.4.3.7) [Chebyshev Functions]. For $X\in\mathbb{R}_+$, define the first **Chebyshev function**

$$\vartheta(X)\triangleq\sum_{p\in\mathtt{Prime},p\leq X}\log p$$

and the second **Chebyshev function**

$$\psi(X)\triangleq\sum_{n\in\mathbb{Z}_+,n\leq X}\Lambda(n)(21.4.3.6).$$

Notice $\psi(X)\geq\vartheta(X)$. ⌟

Prop. (21.4.3.8). For $\mathrm{Re}(s)>1$,

$$-\frac{\zeta'(s)}{\zeta(s)}=\sum_{n\in\mathbb{Z}_+}\Lambda(n)n^{-s}.$$

⌟

Proof: ? □

Prop. (21.4.3.9). Let $g\in C^\infty(\mathbb{R})$ s.t. $e^{\beta x}g(x)\in\mathcal{S}$ for any $\beta\in\mathbb{R}_+$, then for any $\beta\in\mathbb{R}_{>1}$,

$$\sum_{n\in\mathbb{Z}_+}\Lambda(n)g(\log n)=-\frac{1}{2\pi\mathrm{i}}\int_{\mathrm{Re}(z)=\beta}\frac{\zeta'}{\zeta}(s)\mathcal{L}(g)(-s)\mathrm{d}s.$$

⌟

Proof: Cf.[Larry Guth]P79. □

Cor. (21.4.3.10). Situation as in(21.4.3.9), for $\sigma\in(0,1),T\in\mathbb{R}_+$, denote $\mathrm{Box}(\sigma,T)$ the open rectangular $\{s=x+\mathrm{i}\,y|\sigma<x<\beta,|y|<T\}$, and the arc

$$\gamma_{\sigma,T}=(\beta,-T)\longrightarrow(\sigma,-T)\longrightarrow(\sigma,T)\longrightarrow(\beta,T).$$

Then by residue formula,

$$\sum_{n\in\mathbb{Z}_+}\Lambda(n)g(\log n)=\int e^x g(x)\mathrm{d}x-\sum_{\rho\in\mathrm{Zero}(\zeta)\cap\mathrm{Box}(\sigma,T)}\int e^{\rho x}g(x)\mathrm{d}x-\frac{1}{2\pi\mathrm{i}}\int_{\gamma_{\sigma,T}}\frac{\zeta'}{\zeta}\mathcal{L}g(-s)\mathrm{d}s.$$

⌟

Estimates

Thm. (21.4.3.11). For $s\in\mathbb{C}$ with $\mathrm{Re}(s)>0$,

$$|\zeta(s)-\frac{1}{s-1}|\leq\frac{|s|}{\mathrm{Re}(s)}.$$

⌟

Proof: Cf.[Larry Guth]P87. □

Prop. (21.4.3.12)[Bounding Numbers of Zeros]. For ε, there exists $C(\varepsilon)\in\mathbb{R}_+$ s.t. for any $T\in\mathbb{R}_+$,

$$\#\,\mathrm{Zero}(\zeta)\cap\mathrm{Box}(\varepsilon,T)\leq C(\varepsilon)T\log T(21.4.3.10).$$

⌟

Proof: Cf.[Larry Guth]P87. □

Prop. (21.4.3.13). For any $\varepsilon>0$, there exists constant $C_\varepsilon>0$ s.t. $|\zeta(s)|^{-1}\leq C_\varepsilon|t|^\varepsilon$, where $s=\sigma+\mathrm{i}\,t,\sigma\geq1,|t|\geq1$. ⌟

Proof:

□

Prop. (21.4.3.14). There exists $C\in\mathbb{R}_+$ s.t. if $s=\sigma+\mathrm{i}\,t\in\mathbb{C}$ where $\sigma>1/4$ and $|t|>1$, then $|\zeta(s)|\leq C|s|$. ⌟

Proof: Cf.[Larry Guth]P92. □

Prop. (21.4.3.15). Given $\varepsilon \in \mathbb{R}_+$, then there exists $C(\varepsilon) \in \mathbb{R}_+$ s.t. for any $s \in \mathbb{C}$ with $\mathrm{Re}(s) > \varepsilon$,

$$\Big|\frac{\zeta'}{\zeta}(s) - \sum_{\rho \in \mathrm{Zero}(\zeta)} \frac{1}{s-\rho}\Big| \leq C(\varepsilon)\log(2+|\tau|).$$

⌟

Proof: Cf.[Larry Guth]P87.**?** □

Cor. (21.4.3.16). For $\varepsilon \in \mathbb{R}_+$ and $\tau \in \mathbb{R}$ with $|\tau| > 1$,

$$\mathrm{Re}(-\frac{\zeta'}{\zeta}(1+\varepsilon+\mathrm{i}\,\tau)) \leq O(\log|\tau|).$$

And if $\rho = 1-\delta+\mathrm{i}\,\tau$ is a zero of $\zeta(s)$, then

$$\mathrm{Re}(-\frac{\zeta'}{\zeta}(1+\varepsilon+\mathrm{i}\,\tau)) \leq -\frac{1}{\varepsilon+\delta} + O(\log|\tau|).$$

⌟

Proof: These follow from the fact that for a zero ρ of ζ and $s \in \mathbb{C}$ s.t. $\mathrm{Re}(s)$, we have $\mathrm{Re}(-\frac{1}{s-\rho}) < 0$.
□

Thm. (21.4.3.17) [Vinogradov]. There exists $c, C \in \mathbb{R}_+$ s.t. if $\beta, \tau \in \mathbb{R}$ satisfies $\beta > 1 - \frac{c}{\log^{2/3}(2+|\tau|)}$, then

$$|\zeta(\beta+\mathrm{i}\,\tau)| \leq C\log(2+|\tau|).$$

⌟

Proof: Cf.[Larry Guth]P101. □

Thm. (21.4.3.18) [Zero-Free Region, Vinogradov]. There exists $c \in \mathbb{R}_+$ s.t. if $\beta, \tau \in \mathbb{R}$ and

$$\beta > \frac{c}{\log^{2/3}(2+|\tau|)\log\log|\tau|},$$

then $\zeta(\beta+\mathrm{i}\,\tau) \neq 0$. ⌟

Proof: Cf.[Larry Guth]P97**?** and P101. □

Lemma (21.4.3.19). For $\sigma \in \mathbb{R}_{>1}$ and $\tau \in \mathbb{R}$,

$$\mathrm{Re}\Big(3\frac{-\zeta'}{\zeta}(\sigma) + 4\frac{-\zeta'}{\zeta}(\sigma+\mathrm{i}\,\tau) + \frac{-\zeta'}{\zeta}(\sigma+2\,\mathrm{i}\,\tau)\Big) \geq 0.$$

⌟

Proof: It follows from(21.4.3.8) that the LHS equals

$$\sum_{n\in\mathbb{Z}_+}\frac{\Lambda(n)}{n^\sigma}(3+4\cos(\tau\log n)+\cos(2\tau\log n)) = \sum_{n\in\mathbb{Z}_+}\frac{\Lambda(n)}{n^\sigma}2(1+\cos(\tau\log n))^2 \geq 0.$$

□

4 Sieve Theory

Thm. (21.4.4.1) [Iwaniec]. There are infinitely many primes $p \in \texttt{Prime}$ of the form $p = x^2 + y^4, x, y \in \mathbb{Z}_+$. ⌟

Proof: □

Numbers Represented by Homogenous Forms

Thm. (21.4.4.2) [Fermat/Jacobi]. For $n \in \mathbb{Z}_+$, let $r_2(n) = \#\{(x, y) \in \mathbb{Z} | x^2 + y^2 = n\}$, then $r(n) \neq 0$ iff $2 | v_p(n)$ for any $p \equiv 3 (\bmod\ 4)$. Moreover,

$$r_2(n) = 4\Big(\#\{d \in \mathbb{Z}_+, d|n, d \equiv 1 (\bmod\ 4)\} - \#\{d \in \mathbb{Z}_+, d|n, d \equiv 3 (\bmod\ 4)\}\Big).$$

⌟

Proof: $1 + \sum_{n \in \mathbb{Z}_+} r_2(n) e^{2\pi i n\tau} = \theta^2(\tau) \in \mathrm{MF}_1(\Gamma_0(4), \chi_4)$ by(20.2.1.29), and also

$$G_{4,\chi_4} = 1 + \sum_{n \in \mathbb{Z}_+} \Big(\sum_{d \in \mathbb{Z}_+, d|n} \chi_4(d) \Big) e^{2\pi i \tau} \in \mathrm{MF}_1(\Gamma_0(4), \chi_4)(20.2.4.10).$$

But $\dim \mathrm{MF}_1(\Gamma_1(4)) \leq 1$ by(20.2.3.17), so we can compare coefficients. □

Thm. (21.4.4.3) [Lagrange]. For $n \in \mathbb{Z}_+$, let $r_4(n) = \#\{(x, y) \in \mathbb{Z} | x^2 + y^2 = n\}$, then $r_4(n)$ equals 8 times the sum of positive divisors of n that are not multiples of 4.

In particular, any $n \in \mathbb{Z}_+$ is a sum of four squares. ⌟

Proof: Calculate $\theta^4(\tau) \in \mathrm{MF}_2(\Gamma_0(4))$, where $\dim \mathrm{MF}_2(\Gamma_0(4)) = 2$.?Cf.[Modular Forms 1-2-3]P27. □

Thm. (21.4.4.4) [Heath-Brown]. There are infinitely many primes $p \in \texttt{Prime}$ of the form $p = x^3 + 2y^3, x, y \in \mathbb{Z}_+$. ⌟

Proof: □

5 Primes in Arithmetic Progressions

Def. (21.4.5.1) [Prime Counting Functions]. For $N \in \mathbb{Z}_+, a \in (\mathbb{Z}/(N))^*, X \in \mathbb{R}_+$, define

$$\pi(X; N, a) = \#\{p \in \texttt{Prime} : p \leq X, p \equiv a (\bmod\ N)\}.$$

And $\pi(X; 1, 1)$ is also denoted by $\pi(X)$. ⌟

Def. (21.4.5.2) [Normalized Prime Counting Function]. The **normalized prime counting function** π_0 is defined to be the function $\pi_0 : \mathbb{R} \to \mathbb{R}_+$:

$$\pi_0(X) = \lim_{h \to 0} \frac{1}{2}(\pi(X + h) + \pi(X - h)).$$

⌟

Thm. (21.4.5.3) [Merten's Theorem]. For $X \in \mathbb{R}_+$,

- $$|\sum_{p\in\mathbf{P},p\leq X}\frac{\log p}{p}-\log X|\leq 2.$$

- $$\lim_{X\to\infty}\Big(\sum_{p\in\mathbf{P},p\leq X}\frac{1}{p}-\log\log X\Big)=M,$$
  where $M\approx 0.26$ is called the **Meissel–Mertens constant**.

- $$\lim_{X\to\infty}\Big(\sum_{p\in\mathbf{P},p\leq X}\log(1-\frac{1}{p})+\log\log X\Big)=\gamma.$$

⌟

Proof: Cf.https://terrytao.wordpress.com/2013/12/11/mertens-theorems/. □

Prop. (21.4.5.4) [Chebyshev]. $\pi(X)\sim\frac{X}{\log X}$ iff $\psi(X)\sim X$. ⌟

Proof: As $0\leq\psi(X)\leq\pi(X)\log(X)$, $\frac{\psi(X)}{X}\leq\frac{\pi(X)\log(X)}{X}$. Also for any $\varepsilon\in\mathbb{R}_+$,

$$\psi(X)\geq\sum_{p\in\mathtt{Prime},X^{1-\varepsilon}<p\leq X}\log p\geq(1-\varepsilon)\log(X)(\pi(X)-\pi(X^{1-\varepsilon})),$$

so

$$\frac{\psi(X)}{X}\leq\frac{\pi(X)\log(X)}{X}\leq(\frac{1}{1-\varepsilon})\frac{\psi(X)}{X}+\frac{\log(X)}{X^{\varepsilon}}.$$

So the theorem follows. □

Lemma (21.4.5.5) [Chebyshev]. For $X\geq 1$, $\vartheta(X)\leq(4\log 2)X$. ⌟

Proof:

$$2^{2n}=(1+1)^{2n}\geq\binom{2n}{n}\geq\prod_{n<p<2n,p\in\mathbf{P}}p,$$

so

$$\vartheta(2n)-\vartheta(n)\leq 2n\log 2.$$

From this the assertion easily follows. □

Lemma (21.4.5.6). Define the function $\Phi(s)=\sum_{p\in\mathbf{P}}p^{-s}\log p$, then $(\mathcal{L}\vartheta(e^t))(s)=\Phi(s)/s$. Thus $\Phi(s)$ is holomorphic on $\mathrm{Re}(s)>1$ by(11.11.2.17) and(21.4.5.5), and $\Phi(s)-\frac{1}{s-1}$ extends to meromorphic functions on $\mathrm{Re}(s)>1/2$ and holomorphic on $\mathrm{Re}(s)\geq 1$. ⌟

Proof: By(2.6.3.2) there are infinitely many primes. For $n\in\mathbb{Z}_+$, let p_n be the n-th smallest prime number, then the function $\vartheta(e^t)$ is constant on $(\log p_n,\log p_{n+1})$, and

$$\int_{\log p_n}^{\log p_{n+1}}e^{-st}\vartheta(e^t)\mathrm{d}t=\vartheta(p_n)\int_{\log p_n}^{\log p_{n+1}}e^{-st}\mathrm{d}t=\vartheta(p_n)\frac{p_n^{-s}-p_{n+1}^{-s}}{s}.$$

Thus

$$(\mathcal{L}\vartheta(e^t))(s)=\int_0^\infty e^{-st}\vartheta(e^t)\mathrm{d}t=\frac{1}{s}\sum_{n\in\mathbb{Z}_+}\vartheta(p_n)(p_n^{-s}-p_{n+1}^{-s})=\frac{1}{s}\sum_{n\in\mathbb{Z}_+}p_n^{-s}\log p_n=\frac{\Phi(s)}{s}.$$

For the last assertion, notice

$$-\frac{\zeta'(s)}{\zeta(s)}=(-\log\zeta(s))'=(\sum_{p\in\mathbf{P}}\log(1-p^{-s}))'=\sum_{p\in\mathbf{P}}\frac{\log p}{p^s-1}=\Phi(s)+\sum_{p\in\mathbf{P}}\frac{\log p}{p^s(p^s-1)},$$

And $\sum_{p\in\mathbf{P}}\frac{\log p}{p^s(p^s-1)}$ is absolutely convergent and holomorphic for $\mathrm{Re}(s)>1/2$, and $\frac{\zeta'(s)}{\zeta(s)}$ has a simple pole with residue 1 by(21.4.3.1). So the assertion follows. □

Prop. (21.4.5.7). For $X\in\mathbb{R}_{>17}$,

$$\frac{X}{\log X}<\pi(X)<1.25506\frac{X}{\log X}.$$

⌟

Proof: [ROSSER and L. SCHOENFELD, Approximate formulas for some functions of prime numbers, Ill. J. Math. 6(1962), 64-94.]Thm2? □

Thm. (21.4.5.8) [Brun–Titchmarsh]. For any $X\in\mathbb{R}_+,N\in\mathbb{Z}_+,a\in(\mathbb{Z}/(N))^*$ s.t. $N\le X$,

$$\pi(X;N,a)\le\frac{2X}{\varphi(N)\log(X/N)}.$$

In particular, $\pi(X)\le 2X/\log X$. ⌟

Proof:

□

Thm. (21.4.5.9) [Prime Number Theorem, Hadamard-Vallée-Poussin1896/Siegel-Walfisz]. For any $A\in\mathbb{R}_+$,

$$\pi(X;N,a)=\frac{1}{\varphi(N)}\,\mathrm{Li}(X)+O_A(\frac{X}{\exp(A\sqrt{\log X})}),X\to\infty$$

holds when $(a,N)=1$ and $N\le(\log X)^A$. ⌟

Proof: ?

We only prove that $\pi(X)\sim\frac{X}{\log X},X\to\infty$: This follows from(21.5.1.4) and(21.4.5.4).

The function $H(t)=\vartheta(e^t)e^{-t}-1$ is piecewise continuous and bounded by(21.4.5.5), and $(\mathcal{L}H)(s)=\frac{\Phi(s+1)}{s+1}-\frac{1}{s}$(21.4.5.6) extends to a holomorphic function on $\mathrm{Re}(s)\ge 0$. Then by(11.11.2.18), the integral

$$\int_0^\infty H(t)\mathrm{d}t=\int_0^\infty(\vartheta(e^t)e^{-t}-1)\mathrm{d}t=\int_1^\infty\frac{\vartheta(x)-x}{x^2}\mathrm{d}x$$

converges. Then by(11.3.2.14), $\vartheta(X)\sim X$, and so $\pi(X)\sim\frac{X}{\log X}$ by(21.4.5.4). □

Def. (21.4.5.10)[Restrictions on N]. Let $\mathscr{B}$ be the set of numbers $B\in(0,1)$ s.t. there exists $D_B\in\mathbb{N}$ s.t. when $X\in\mathbb{R}_+$ is large, there exists a set $\mathscr{D}_B(X)$ of at most D_B many integers bigger than $\log X$, s.t. for any $Y\in\mathbb{R}_+,N\in\mathbb{Z}_+$, $N\le\min(x^B,y/x^{1-B})$ and $a\in(\mathbb{Z}/(N))^*$,

$$\pi(y;N,a)\ge\frac{\pi(y)}{2\varphi(N)},$$

unless N divides one one of the numbers in $\mathcal{D}_B(X)$.

Also denote $B_{\pi,1}$ the supremum of numbers B s.t. there exists $D_B \in \mathbb{N}$ s.t. when $X \in \mathbb{R}_+$ is large, there exists a set $S_B(X)$ of at most D_B many integers bigger than $\log X$ s.t. for any $N \in \mathbb{Z}_+$, $N \leq X^B$,

$$\pi(X; N, 1) \geq \frac{\pi(X)}{2\varphi(N)},$$

unless N divides one one of the numbers in $S_B(X)$. Then it is clear that $(0, B_{\pi,1}) \subset \mathcal{B}$. ⌟

Prop. (21.4.5.11). $(0, 5/12) \in \mathcal{B}$. ⌟

Proof: [Alford-Granville-Pomerance, Carmichael numbers]. □

Thm. (21.4.5.12). For $m \in \mathbb{Z}_+$, $\tau(m) = 2^{(1+o(1))\log m/\log\log m}$ as $m \to \infty$.

This is the best bound, because one can prove that there exists $c \in \mathbb{R}_+$ s.t. there are infinitely many $m \in \mathbb{Z}_+$ with more than $2^{c\log m/\log\log m}$ many divisors d s.t. $d+1 \in \mathbf{P}$. ⌟

Proof: □

Prop. (21.4.5.13). For any $A \in \mathcal{A}$**?** and $\varepsilon, \delta \in \mathbb{R}_+$, there exist numbers $\eta_{\varepsilon,\delta}, D_{\varepsilon,\delta}$ s.t. for any X sufficiently large, there is a set $\mathcal{D}_{\varepsilon,\delta}(x)$ of integers in of cardinality$\leq D_{\varepsilon,\delta}$, s.t. every element of $\mathcal{D}_{\varepsilon,\delta}$ is bigger than $\log X$, and at most one of them is bigger than $X^{\eta_{\varepsilon,\delta}}$, and

$$|\vartheta(Y; N, a) - \frac{y}{\varphi(d)}| \leq \varepsilon\frac{y}{\varphi(d)}$$

for any $N \in \mathbb{Z}_+, Y \in \mathbb{R}_+, a \in (\mathbb{Z}/(N))^*$ s.t. N is not divisible by elements of $\mathcal{D}_{\varepsilon,\delta}(x)$, and $1 \leq d \leq \min(X^{1/A-\delta}, Y/X^{1-1/A+\delta})$. ⌟

Proof: Cf.[AGP94]P712.**?** □

Prop. (21.4.5.14). Suppose $B \in \mathcal{B}$(21.4.5.10), then for any X large and $L \in \mathbb{Z}_+$ s.t. L is square-free not divisible by any prime exceeding $X^{(1-B)/2}$, and

$$\sum_{p \in S(L)} \frac{1}{p} \leq (1-B)/32,$$

there exists $k \in \mathbb{Z}_+, k \leq X^{1-B}, (k, L) = 1$ s.t.

$$\#\{d \in \mathbb{Z}_+ : d|L, dk+1 \leq X, dk+1 \in \mathbf{P}\} \geq \frac{2^{-D_B-2}}{\log X}\#\{d \in \mathbb{Z}_+ : d|L, 1 \leq d \leq X^B\}.$$

⌟

Proof: Cf.[AGP94]P715.**?** □

Elliott-Halberstam Conjecture

Conj. (21.4.5.15) [Elliott-Halberstam]. For $N \in \mathbb{Z}_+$ and $X \in \mathbb{R}_+$, let

$$\mathrm{Err}(X; N) = \max_{(a,N)=1} |\pi(X; N, a) - \frac{\pi(X)}{\varphi(N)}|.$$

Then for any $\theta \in (0, 1)$ and $A \in \mathbb{R}_+$, there exists a constant $C \in \mathbb{R}_+$ s.t.

$$\sum_{1 \leq N \leq X^\theta} \mathrm{Err}(X; N) \leq C\frac{X}{\log^A X}.$$

⌟

Thm& Conj.Cor. (21.4.5.16) [Bombieri-Vinogradov]. The Elliott-Halberstam conjecture is true for $\theta < 1/2$. ⌟

Proof: □

Green-Tao Theorem

Thm. (21.4.5.17) [Green-Tao]. $\mathbf{P}$ contains arithmetic progressions of any length. In fact, if $A \subset P$ is a subset with positive natural upper density, then A contains arithmetic progressions of any length. ⌟

Proof: Cf.[Green-Tao]. Notice this is a consequence of the Erdös-Turán conjecture(25.6.2.7). □

Sophie-Germain Primes

Def. (21.4.5.18) [Sophie-Germain Primes]. A **Sophie-Germain prime** is a prime $p \in \texttt{Prime}$ s.t. $2p + 1$ is also a prime. ⌟

Conj. (21.4.5.19) [Sophie-Germain Primes Conjecture]. Let C_2 be the twin-prime constant?, then

$$\#\{p \in \mathbf{P} | p \leq m, 2p + 1 \in \texttt{Prime}\} \sim 2C_2 \frac{X}{\log X}, \quad X \to \infty.$$

⌟

Proof: □

6 Gaps between Primes

Small Gaps between Primes

Conj. (21.4.6.1) [Cramer]. The largest gap between consecutive primes$\leq X$ is $\Theta((\log X)^2)$. ⌟

Proof: □

Def. (21.4.6.2). For $Y, Y \in \mathbb{R}_+$, let $\pi(X|Y)$ be the cardinality of primes p s.t. $p \leq X$, and $p - 1$ is free of prime divisors exceeding Y. ⌟

Def. (21.4.6.3). Let E_π denote the supremum of numbers $E \in (0, 1)$ s.t. there exists $\gamma_1(E) \in \mathbb{R}_+$ s.t. $\pi(X|X^{1-E}) \geq \gamma_1(E)\pi(X)$ for $X \in \mathbb{R}_+$ sufficiently large. ⌟

Prop. (21.4.6.4). $E_\pi > 0$, and if $E \in (0, 1)$ has the property stated in(21.4.6.3), then so does $E + \varepsilon$ for some $\varepsilon \in \mathbb{R}_+$. ⌟

Proof: For the first assertion, Cf.[Erdos]?,

For the second assertion, for X large,

$$\pi(X|X^{1-E'}) \geq \pi(X|X^{1-E}) - \sum_{p \in \mathbf{P}, x^{1-E'} \leq p < x^{1-E}} \pi(X; p, 1)$$

$$(21.4.6.3) \geq \gamma_1(E)\pi(X) - \sum_{p \in \mathbf{P}, x^{1-E'} \leq p < x^{1-E}} \frac{2X}{\varphi(p)\log(X/p)}$$

$$\begin{aligned}(21.4.5.7) \geq \gamma_1(E)\frac{X}{\log X} &- \sum_{p\in\mathbf{P}, x^{1-E'}\leq p<x^{1-E}} \frac{2X}{E(p-1)\log X} \\ &= \frac{X}{\log X}\Big(\gamma_1(E) - \frac{2}{E}\sum_{p\in\mathbf{P}, x^{1-E'}\leq p<x^{1-E}}\frac{1}{p-1}\Big) \\ (21.4.5.3) &= \frac{X}{\log X}\Big(\gamma_1(E) - \frac{2}{E}\log\frac{1-E}{1-E'} + o(1)\Big)\end{aligned}$$

This shows that when E' is sufficiently closed to E, when X is large, E' also satisfies the property stated in(21.4.6.3). □

Conj. (21.4.6.5). $E_\pi = 1$. ⌟

Proof: □

Prop. (21.4.6.6) [Friedlander]. $1-(2\sqrt{e})^{-1}\leq E_\pi$. ⌟

Proof: [FRIEDLANDER, Shifted primes without large prime factors]. □

Prop. (21.4.6.7). $B_{\pi,1}\leq E_\pi$(21.4.5.10). ⌟

Proof: Cf.[AGP94]P720**?**. □

Carmichael Numbers

Def. (21.4.6.8) [Carmichael Numbers]. $n\in\mathbb{Z}_+$ is called a **Carmichael number** if $n\notin\mathbf{P}$ and $n|a^n-a$ for any $a\in\mathbb{Z}$. For $X\in\mathbb{R}_+$, let $\mathrm{Car}(X)$ denote the cardinality of Carmichael numbers not exceeding X. ⌟

Thm. (21.4.6.9) [Korselt]. For $n\in\mathbb{Z}_+$, $n|a^n-a$ for all $a\in\mathbb{Z}$ iff n is square-free and $p-1|n-1$ for any $p\in\mathbf{P}, p|n$. ⌟

Proof: Suppose n is a Carmichael number. Then n is square-free: For $p|n$, let $n=p^kn'$, then $(1+p)^{p^kn'}\equiv 1+p(\mathrm{mod}\ p^k)$, but $p^{k+1}|(1+p)^{p^kn'}-1$, so $p^k|p$, and $k=1$. And let g be a primitive root for p, then $g^n\equiv g(\mathrm{mod}\ n)$, thus $p-1|n-1$.

The converse is obvious. □

Cor. (21.4.6.10). Any Carmichael number $n\in\mathbb{Z}_+$ is odd, and has at least three prime divisors. ⌟

Proof: If n is even, because n is square-free(21.4.6.9), n has an odd prime divisor $p\in\mathbf{P}$, so $p-1|n-1$, contradiction. If $n=pq$, then $p-1|pq-1, q-1|pq-1$, thus $p-1|q-1|p-1$, and $p=q$, contradiction. □

Thm. (21.4.6.11) [Alford-Granville-Pomerance]. For each $E\in\mathcal{E}$(21.4.6.3) and $B\in\mathcal{B}$(21.4.5.10), then $\mathrm{Car}(X)\geq X^{EB}$ for X sufficiently large. ⌟

Proof: Because of(21.4.6.4), it suffices to show that $\mathrm{Car}(X)\geq X^{EB-\varepsilon}$ for any $\varepsilon\in\mathbb{R}_+$ and X sufficiently large.

□

Cor. (21.4.6.12) [Alford-Granville-Pomerance/Harman]. $(0,1-(2\sqrt{e})^{-1})\subset\mathcal{E}$(21.4.6.6), and $(0,5/12)\in\mathcal{B}$ by(21.4.5.11), so $\mathrm{Car}(X)>X^{2/7}$ for X sufficiently large. In fact, Harman proved that $\mathrm{Car}(X)>X^{1/3}$ for X sufficiently large. ⌟

Large Gaps between Primes

Conj. (21.4.6.13) [Cramér].

$$\lim_{n\to\infty} \frac{p_{n+1} - p_n}{\log^2 p_n} = 1.$$

⌟

Proof: □

Conj.Cor. (21.4.6.14) [Oppermann]. For any $n \in \mathbb{Z}_{\geq 2}$,

$$\pi(n^2 - n) < \pi(n^2) < \pi(n^2 + n).$$

⌟

Thm& Conj.Cor. (21.4.6.15) [Montgomery/Huxley/Baker-Harman-Pintz]. There exists an effectively constant $x_0 \in \mathbb{R}_+$ s.t. for any $X \in (x_0, \infty)$, $\mathtt{Prime} \cap [X - X^{0.525}, X] \neq \varnothing$. ⌟

Proof: □

7 Circle Method

8 Goldbach Problem

Conj. (21.4.8.1) [Goldbach]. For any $m \in \mathbb{Z}_{\geq 2}$, $2m$ is a sum of two prime numbers.

Hardy-Littlewood even conjectures that the number of representations of $2m$ is

$$N_2(2m) \sim 4 \prod_{q \in \mathtt{Prime}_{\geq 3}} (1 - \frac{1}{(q-1)^2}) \cdot \prod_{p \in \mathtt{Prime}_{\geq 3}, p | n} (\frac{p-1}{p-2}) \cdot \frac{m}{\log^2 m}.$$

⌟

Proof: □

Thm& Conj.Cor. (21.4.8.2) [Ternary Goldbach Conjecture, Vinogradov]. For any $k \in \mathbb{Z}_{\geq 3}$, $2k + 1$ is a sum of three primes. ⌟

Proof: ? □

9 Hardy-Littlewood Conjectures

Conj. (21.4.9.1) [Hardy-Littlewood Conjecture N]. There are infinitely many primes $p \in \mathtt{Prime}$ of the form $p = x^3 + y^3 + z^3$.

Moreover, for $X \in \mathbb{R}_+$, if $P(X)$ is the number of triples (x, y, z) s.t. $x^3 + y^3 + z^3 \in \mathtt{Prime} \cap [0, X]$, then

$$P(X) \sim \Gamma(\frac{4}{3})^3 \cdot \prod_{q \in \mathtt{Prime}, q \equiv 1 (\mathrm{mod}\ 3)} (1 - \frac{A_q}{q^2}) \cdot \frac{X}{\log X},$$

where $A_q \equiv 1 (\mathrm{mod}\ 3)$ and $4q = A_q^2 + 27 B_q^2$. ⌟

10 Prime Ideals

Def. (21.4.10.1) [Prime Ideal Counting Functions]. For $F \in \texttt{NField}$, let

$$\pi(X; F) = \#\{\mathfrak{p} \in \Sigma_F^{\text{fin}} : ||\mathfrak{p}|| \le X\}$$

⌟

Thm. (21.4.10.2) [Prime Ideal Theorem, Landau]. For $F \in \texttt{NField}$, there exists $c_F \in \mathbb{R}_+$ s.t.

$$\pi(X; F) = \mathrm{Li}(X) + O(\frac{X}{\exp(c_F\sqrt{\log X})}).$$

⌟

Proof: □

11 Others

Prop. (21.4.11.1). For any $p \in \mathbf{P}_{\ge 5}$, there exists $P \in \mathbf{P}, \ell \in \mathbf{P}_{\ge 3}, m, r \in \mathbb{Z}_+$ s.t. $P > p$, $\ell^r || (P-1)$, $\ell^r = 2m+1$, and

$$\frac{P}{p} \le \frac{2m+1}{m+1} - \frac{m}{m+1} \cdot \frac{1}{p}.$$

⌟

Proof: Cf.[Serre's Modularity Conjecture, the Level One Case]P582. □

Conj. (21.4.11.2) [Artin's Conjecture on Primitive Roots]. For any $n \in \mathbb{Z}_+ \setminus (\mathbb{Z}_+)^2$, there exists $A(n) > 0.35 \in \mathbb{R}_+$ s.t.

$$\#\{p \in \mathbf{P} | p \le X, \mathrm{ord}_p(n) = p-1\} \sim A(n)\frac{X}{\log X}, \quad X \to \infty$$

⌟

Proof: □

Prop. (21.4.11.3) [Fouvry]. There exists $C \in \mathbb{R}_+$ s.t. when $X \in \mathbb{R}_+$ is large,

$$\#\{\ell \in \mathbf{P} | \ell \le X, P_{\max}(\ell - 1) \ge \ell^{0.668}\} \ge C\frac{X}{\log X}.$$

⌟

Proof: Cf.[Fouvry, Théoréme de Brun-Titchmarsh; applicationau théoréme de Fermat], and [Baker and Harman, The Brun-Titchmarsh Theorem on average]. □

Cor. (21.4.11.4). When $n \in \mathbb{Z}_+$ is large, there exists $r \in \mathbb{Z}_+, r \le \log^3 n$ that $\mathrm{ord}_r(n) > \log^2 n$. ⌟

Proof: Notice by(21.4.11.3), for any $\varepsilon \in \mathbb{R}_+$, when n is large, there exists at least $\Omega(\log^{3+\frac{\varepsilon}{2}} n)$ primes $\ell \in \mathbf{P}$ s.t. $P_{\max}(\ell - 1) \ge \ell^{2/3}$ and $\log^2 n < \ell < \log^{3+\varepsilon} n$. Then $\mathrm{ord}_\ell(n) \ge \log^2 n$ or $\ell | n^k + 1$ for some $k \le \log^{1+\frac{\varepsilon}{3}} n$. The latter case happens only for $O(\log^{3+\frac{2\varepsilon}{3}} n)$ many ℓ. So we can find some $\ell < \log^{3+\varepsilon} n$ s.t. $\mathrm{ord}_r(n) \ge \log^2 n$. □

21.5 Riemann Conjecture

References are [Ivic, Aleksandar The Riemann zeta-function. The theory of the Riemann zeta-function with applications. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1985. xvi+517 pp. ISBN: 0-471-80634-X].

1 Distribution of Primes

Thm. (21.5.1.1) [Riemann-Mangoldt Formula]. Define

$$f(X) = \pi_0(X) + \frac{1}{2}\pi_0(X^{\frac{1}{2}}) + \frac{1}{3}\pi_0(X^{\frac{1}{3}}) + \ldots,$$

then by Möbius inversion,

$$\pi_0(X) = \sum_n \frac{\mu(n)}{n} f(X^{\frac{1}{n}}) = f(X) - \frac{1}{2}f(X^{\frac{1}{2}}) + \frac{1}{3}f(X^{\frac{1}{3}}) - \ldots.$$

Then there is a **Riemann-Mangoldt formula**

$$f(X) = \mathrm{li}(X) - \sum_\rho \mathrm{li}(X^\rho) - \log 2 + \int_X^\infty \frac{\mathrm{d}t}{t(t^2-1)\log t}.$$

⌟

Proof: ? □

Def. (21.5.1.2). For $X \in \mathbb{R}_+$, define $\mathrm{Err}(X) = \psi(X) - X$(21.4.3.7). ⌟

Prop. (21.5.1.3). The Riemann conjecture is equivalent to the following:

- $|\pi(X) - \mathrm{Li}(X)| = \widetilde{O}(X^{1/2})$.
- $\mathrm{Err}(X) = \widetilde{O}(X^{1/2})$(21.5.1.2).

⌟

Proof: This should follows from the Riemann-Mangoldt formula(21.5.1.1)?. □

Thm. (21.5.1.4) [Vinogradov]. $\mathrm{Err}(X) = O(Xe^{-C(\log X)^{3/5}(\log\log X)^{-1/5}})$. ⌟

Proof: We only prove that there exists $c \in \mathbb{R}_+$ s.t. $\mathrm{Err}(X) = O(Xe^{-C\log^{1/2} X})$:

Cf.[Larry Guth]. The assertion follows from(21.4.3.18). The same argument should work if we use the bigger zero-free region. □

2 Hilbert-Pólya Conjecture

References are [Rudnick-Sarnak, Zeros of Principal L-functions and Random Matrix Theory], [Trace formula in noncommutative geometry and the zeros of the Riemann zeta function].

Conj. (21.5.2.1) [Riemann Hypothesis, Riemann1859]. ⌟

3 Landau-Siegel Conjecture

21.6 B-S.D Conjecture

References are [Lectures on the Conjecture of Birch and Swinnerton-Dyer, Gross], [Sil99], http://virtualmath1.stanford.edu/~conrad/BSDseminar/, [Gross, Kolyvagin's work on modular elliptic curves(1989)].

1 Statements

References are [BSD65].

Elliptic Curves

Conj. (21.6.1.1) [Birch-S.Dyer]. Let $F \in \mathtt{NField}, E \in \mathcal{E}\mathrm{ll}/F$, and $L(E,s)$ be the L-function of E(21.2.6.2), then

- $\#Ш(E) < \infty$, $\mathrm{rank}(E/F) = \mathrm{rank}_{\mathrm{an}}(E/F) = r$, and
- $$L^\dagger(E;1) = \frac{2^{r_2}\Omega\langle\prod_{v\in\Sigma_F^{\mathrm{fin}}} c_v\rangle\langle\prod_{v\in\Sigma_F^{\mathrm{fin}}}|\omega/\omega_{E,v}|_v\rangle}{\sqrt{|d_K|}}\cdot\#Ш(E/K)\cdot\frac{\mathrm{Reg}(E/K)}{(\#E(K)_{\mathrm{tor}})^2},$$

where

- r_2 is the number of complex places of K,
- $\mathrm{Reg}(E/F)$ is the regulator of $E(F)/E(F)_{\mathrm{tor}}$ w.r.t the Neron-Tate height pairing on $E(F)$(15.13.1.7),
- c_v are the local Tamagawa numbers,
- ω is a non-zero global exterior differential form,
- $\Omega = \prod_{v\in\Sigma_F^\infty}\int_{E(F_v)}|\omega|_v$,
- $\omega_{E,v}$ are the Néron differentials on E_v.

⌟

Proof: □

Conj. (21.6.1.2) [p-Parts of the Birch-S.Dyer Conjecture]. ⌟

Prop. (21.6.1.3) [Nekovar]. The parity conjecture holds for elliptic curves over a totally real number field K if $Ш(E/K)$ is finite. ⌟

Proof: □

Abelian Varieties

Conj. (21.6.1.4) [Functional Equation Conjecture]. Let F be a number field, $A \in \mathcal{A}\mathrm{b}\mathcal{V}\mathrm{ar}^g/F$, then

- the zeta function $Z(A,s)$**?** extends to an entire function on $s\in\mathbb{C}$, and satisfies the functional equation
$$Z(A,s) = w_A Z(A,2-s),$$
where $w_A = \pm 1$ is called the **sign of functional equation of** A, and
- $w_A = w = \prod_{v\in\Sigma_F} w_v$, where w_v is the local root number of A/K at v.

⌟

Proof: □

Conj. (21.6.1.5) [Birch-S.Dyer-Tate]. Let $F \in \mathtt{NField}, A \in \mathcal{A}b\mathcal{V}ar^g/K$, let $L(A,s)$ be the L-function of A(21.2.6.2), then

- $L(A,s)$ extends to an entire function on $s \in \mathbb{C}$, $\#\text{Ш}(A) < \infty$, $\mathrm{rank}(A/F) = \mathrm{rank}_{\mathrm{an}}(A/F) = r$,
-
$$L^\dagger(A;1) = \frac{2^{gr_2}\Omega_A(\prod_{v\in\Sigma_K^0} c_v)(\prod_{v\in\Sigma_K^0}|\omega/\omega_{A,v}|_v)}{\sqrt{|d_K|}^g} \cdot \#\text{Ш}(A/K) \cdot \frac{\mathrm{Reg}(A/K)}{\#A(K)_{\mathrm{tor}}\#\widehat{A}(K)_{\mathrm{tor}}},$$

where

- r_2 is the number of complex places of F,
- $\mathrm{Reg}(A/F)$ the regulator of the Neron-Tate height pairing $A(K)/A(K)_{\mathrm{tor}} \times \widehat{A}(K)/\widehat{A}(K)_{\mathrm{tor}} \to \mathbb{R}$(15.13.1.7),
- c_v the local Tamagawa numbers,
- ω a non-zero global g-form,
- $\Omega_A = \prod_{v\in\Sigma_F^\infty}\int_{A(F_v)}|\omega|_v$,
- $\omega_{A,v}$ is a Néron differential on A_v.

⌟

Proof: □

Remark (21.6.1.6).

- The BSDT conjecture has been verified numerically for some elliptic curves over number fields, some Jacobians of genus 2 curves and (up to square) a few Jacobians of higher genus curves.
- BSDT conjecture implies BSD conjecture(21.6.1.1), as any $E \in \mathcal{E}ll/K$ is an Abelian variety of dimension 1, and $E \cong \widehat{E}$ canonically.

⌟

Prop. (21.6.1.7). If the BSDT conjecture holds for all Abelian varieties over $\mathbb{Q}$, then it holds for all Abelian varieties over any number fields. ⌟

Proof: Cf.[The Arithmetic of Abelian Varieties, Milne].**?** □

Conj. (21.6.1.8) [Parity Conjecture]. Let K be a number field and $A \in \mathcal{A}b\mathcal{V}ar/K$, then $\mathrm{rank}_{an}(A/K) \equiv \mathrm{rank}(A/K) \mod 2$. This is a consequence of BSDT conjecture(21.6.1.5). ⌟

2 Low Rank Cases

References are [Kolyvagin's Conjecture And Patched Euler Systems In Anticyclotomic Iwasawa Theory, Naomi] andhttp://www.math.columbia.edu/~chaoli/docs/KolyvaginConjecture.html.

We use notations in6.

Thm. (21.6.2.1) [Rank 0 Case]. For $E \in \mathcal{E}ll/\mathbb{Q}$ and $\ell \in \mathbf{P}$, there are implications:

- $\mathrm{rank}(E/\mathbb{Q}) = 0, \#\text{Ш}[\ell^\infty] < \infty \Rightarrow \mathrm{rank}_\ell(E/\mathbb{Q}) = 0$.
- $\mathrm{rank}_{\mathrm{an}}(E/\mathbb{Q}) = 0 \Rightarrow \mathrm{rank}(E/\mathbb{Q}) = 0, \#\text{Ш}[\ell^\infty] < \infty$.

- $\mathrm{rank}_\ell(E/\mathbb{Q}) = 0 \Rightarrow \mathrm{rank}_{\mathrm{an}}(E/\mathbb{Q}) = 0$ if $\ell \geq 3$ is good ordinary for E and $\overline{\rho}_{E,\ell} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}(E[\ell])$ surjective.

⌟

Proof: 1 is trivial.
2 is the work of Gross-Zagier and Kolyvagin.?
3 is the work of Skinner-Urban(2000s)?. □

Prop. (21.6.2.2). If $\mathrm{rank}_{\mathrm{an}}(E/\mathbb{Q}) = 0$, the p-part of the BSD formula(21.6.1.2) is know for $p \geq 3$ under similar hypothesis by work of Kato(2000s) and Skinner-Urban on the Iwasawa main conjecture for elliptic curves.? ⌟

Rank 1 Case

References are [Weil Zhang, Selmer groups and the divisibility of Heegner points (2013)] and [the Birch and Swinnerton-Dyer Formula for Elliptic Curves of Analytic Rank One].

Thm. (21.6.2.3) [Rank 1 Case]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ and $p \in \mathbf{P}$, there are implications:

- $\mathrm{rank}(E/\mathbb{Q}) = 1, \#Ш[p^\infty] < \infty \Rightarrow \mathrm{rank}_p(E/\mathbb{Q}) = 1$.
- $\mathrm{rank}_{\mathrm{an}}(E/\mathbb{Q}) = 1 \Rightarrow \mathrm{rank}(E/\mathbb{Q}) = 1, \#Ш[p^\infty] < \infty$.
- $\mathrm{rank}_p(E/\mathbb{Q}) = 1 \Rightarrow \mathrm{rank}_{\mathrm{an}}(E/\mathbb{Q}) = 1$ if $p \geq 5$ is good ordinary for E and $\overline{\rho}_{E,p} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ surjective with some mild ramification conditions.

⌟

Proof: 1 is trivial.
2 is the work of Gross-Zagier(21.8.2.2) and Kolyvagin(21.8.3.10).
3 follows from(21.8.3.14). □

Cor. (21.6.2.4). As a corollary of(21.6.2.1) and(21.6.2.3), [Bhargava-Skinner-Zhang] proved that at least 66% of Elliptic curves over $\mathbb{Q}$ satisfy the rank part of the BSD conjecture(21.6.1.1)? ⌟

Prop. (21.6.2.5). Under the hypothesis of(21.8.3.12), if $\mathrm{rank}_p(E/\mathbb{Q}) = 1$, then the p-part of the ⌟

Prop. (21.6.2.6). If $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ with conductor N satisfies $\mathrm{rank}_{\mathrm{an}}(E/\mathbb{Q}) = 1$, $p \in \mathbf{P}\backslash\{2,3\}$ and $\overline{\rho}_{E,p}$ is surjective and ramifies at any $\ell \in \mathbf{P}$ s.t. $v_\ell(N) = 1$, then the p-part of the BSD formula(21.6.1.2) holds. ⌟

Proof: Cf, [Weil Zhang, Selmer groups and the divisibility of Heegner points (2013)]. or http://www.math.columbia.edu/~chaoli/docs/KolyvaginConjecture.html. □

3 over Function Fields

Prop. (21.6.3.1) [Artin-Tate]. The BSD conjecture hold for an elliptic curve over a function field F iff $Ш(E/F)$ is finite. ⌟

Proof: □

4 Motivic B-S.D Conjectures

Prop. (21.6.4.1) [Motivic B-S.D conjectures]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$, consider the motive $h^1(E)$, then

$$L(E,s) = Z(h^1(E),s).$$

More generally, if we consider L-functions of the form

$$L_3(E,s) = \prod_p L(E_{\mathbb{F}_{p^3}},s).$$

Then there exists a motive $M \in M_{\mathrm{num}}(\mathbb{Q})$ s.t.

$$h^1(E)\otimes h^1(E)\otimes h^1(E) = 3h^1E(-1)\oplus M,$$

and

$$L_3(E,s) = Z(M,s).$$

⌟

Proof: □

21.7 Special Values of L-Functions

Main references are[Del79], [Conrad BSD notes], [Remarks on special values of L-functions, Scholl], [nLab].

1 Deligne Conjecture

Prop. (21.7.1.1). If $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{roj}/\mathbb{Q}$ and $M = h^i(X)(m)$, then $M^\vee \cong h^i(X)(i-m)$, i.e. it is polarized of weight $i-2m$**?**. ⌟

Proof: **?** Let $\eta \in h^2$ be a hyperplane section, then

$$H^{2d}(X)(d) \cong H^{2d}(\mathbb{P}^N)(d) = (\eta(1))^{\otimes d} \cong 1.$$

There is a pairing

$$h^i(X)(m) \times h^{2d-i}(X)(d-m) \to h^{2d}(X)(d),$$

and also an isomorphism

$$h^i(X)(i-m) \xrightarrow{\cup \eta^{d-i}} h^{2d-i}(X)(d-m).$$

□

Def. (21.7.1.2)[Critical Values]. For $M \in \mathrm{Mot}(\mathbb{Q})$, $m \in \mathbb{Z}$ is called a **critical value** for M if neither $L_\infty(M;s)$ nor $L_\infty(M^\vee;1-s)$ has a pole at $s=m$. M is called a **critical motive** if 0 is critical for M. ⌟

Prop. (21.7.1.3). M is critical iff the Betti realization satisfies

- $\mathrm{Real}_{\mathrm{Betti}}(M)^{p,q} = 0$ unless $p=q$ or $p<0\leq q$ or $q<0\leq p$.
- c acts on $\mathrm{Real}_{\mathrm{Betti}}(M)^{p,p}$ by -1 if $p \geq 0$, and 1 if $p<0$.

⌟

Deligne's Periods

Prop. (21.7.1.4)[Deligne's Periods]. We assume that $M \in \mathrm{Mot}(\mathbb{Q})$ is pure of weight w, and $\mathsf{c} = \pm 1$ on $M^{w/2,w/2}$ if $w \in 2\mathbb{Z}$. Notice these hypothesis are satisfied when M is critical.

Define

$$d(M) = \dim_{\mathbb{Q}} \mathrm{Real}_{\mathrm{Betti}}(M), \quad d^\pm(M) = \dim_{\mathbb{Q}} \mathrm{Real}_{\mathrm{Betti}}(M)^{\mathsf{c}=\pm 1},$$

And also the eigenvalue decomposition of c^* on $\mathrm{Real}_{\mathrm{Betti}}(M)$:

$$\mathrm{Real}_{\mathrm{Betti}}(M) = \mathrm{Real}_{\mathrm{Betti}}(M)^+ \oplus \mathrm{Real}_{\mathrm{Betti}}(M)^-.$$

Then it follows from(8.10.3.16) that

$$I_{\mathrm{dR}}(\mathrm{Real}_{\mathrm{Betti}}(M)^+ \otimes \mathbb{R}) \subset \mathrm{Real}_{\mathrm{dR}}(M), \quad I_{\mathrm{dR}}(\mathrm{Real}_{\mathrm{Betti}}(M)^- \otimes \mathbb{R}) \subset \mathrm{i}\,.\,\mathrm{Real}_{\mathrm{dR}}(M).$$

There are filtration steps $\mathrm{Fil}^\pm \subset \mathrm{Real}_{\mathrm{dR}}(M)$ of the deRham filtration s.t.

$$\mathrm{Fil}^\pm \mathrm{Real}_{\mathrm{dR}}(M) \otimes \mathbb{C} = I_{\mathrm{dR}}(\oplus_{p>q} \mathrm{Real}_{\mathrm{Betti}}(M)^{p,q} \oplus (\mathrm{Real}_{\mathrm{Betti}}(M)^{w/2,w/2})^{\mathsf{c}=\pm 1}).$$

Then we can define

$$\mathrm{Real}_{\mathrm{dR}}(M)^\pm = \mathrm{Real}_{\mathrm{dR}}(M)/\,\mathrm{Fil}^\mp \mathrm{Real}_{\mathrm{dR}}(M).$$

Since $\mathrm{Real}_{\mathrm{Betti}}(M)^{p,q} = \overline{\mathrm{Real}_{\mathrm{Betti}}(M)^{q,p}}$, the space $\mathrm{Real}_{\mathrm{Betti}}(M)^{\pm}$ lies (anti)diagonally, so the following maps

$$I^{\pm} : \mathrm{Real}_{\mathrm{dR}}(M)^{\pm} \otimes \mathbb{C} \subset \mathrm{Real}_{\mathrm{dR}}(M) \otimes \mathbb{C} \xrightarrow{I_{\mathrm{dR}}} \mathrm{Real}_{\mathrm{dR}}(M) \otimes \mathbb{C} \twoheadrightarrow \mathrm{Real}_{\mathrm{dR}}(M)^{\pm} \otimes \mathbb{C}$$

are isomorphisms.

Then because of the $\mathbb{Q}$-structure on $\mathrm{Real}_{\mathrm{dR}}(M)^{\pm}$ and $\mathrm{Real}_{\mathrm{dR}}(M)^{\pm}$, we have that

$$c^{\pm}_{\mathrm{Del}}(M) = \det(I^{\pm}) \in \mathbb{C}^{\times}/\mathbb{Q}^{\times}$$

are well-defined, called the **Deligne periods** of M(if both sides are $\{0\}$, let $c^{\pm}_{\mathrm{Del}}(M) = 1$). In fact, from the argument above, we see that $I^{\pm}$ are real, so in fact $c^{\pm}_{\mathrm{Del}} \in \mathbb{R}^{\times}/\mathbb{Q}^{\times}$. ⌟

Conj. (21.7.1.5) [Deligne]. Let $M \in \mathrm{Mot}(\mathbb{Q})$ be critical, then

$$L(M; s) \sim_{\mathbb{Q}} c^{+}_{\mathrm{Del}}(M) \in \widehat{\mathbb{P}}(21.7.1.4).$$

⌟

Proof: Cf.[Deligne, Values of L-functions] for the assertion that $c^{+}_{\mathrm{Del}}(M) \in \widehat{\mathbb{P}}$. □

Example (21.7.1.6) [Tate Modules]. For the Tate module $\mathbb{Q}(r)$, $\mathsf{c}^* = (-1)^r$ on $\mathrm{Real}_{\mathrm{Betti}}(\mathbb{Q}(n))$, so it follows from(8.10.3.15) that

$$c^{\varepsilon}(\mathbb{Q}(r)) = \begin{cases} (2\pi\,\mathrm{i})^r & ,\varepsilon = (-1)^r \\ 1 & ,\varepsilon = (-1)^{r-1} \end{cases}.$$

And $\mathbb{Q}(r)$ is critical iff $L_\infty(\mathbb{Q}) = \Gamma_{\mathbb{R}}(s)$ is holomorphic at both $r, 1-r$, and this is the case when $r \in 2\mathbb{Z}_+$ or $r \in 1 - 2\mathbb{Z}_+$. The Deligne's conjecture is true in this case, by(21.7.4.1). ⌟

General Coefficients

2 Beilinson-Bloch Conjecture

References are [Blo00], [Bei85], [Beilinsen, Higher regulators of modular curves, Applications of algebraic K-theory to algebraic geometry and number theory, Part I, II], [Iwasawa theory for the symmetric square of an elliptic curve, Flach], [Nekovar, Beilinson's Conjecture, in Motives, 537-570], [Algebraic K-Theory and Special Values of L-Functions: Beilinson's Conjecture].

Notation (21.7.2.1).

- Denote $m = i + 1 - n$.
- We assume that
  - the Euler product for $L(h^i(X); s)$ converges absolutely for $\mathrm{Re}(s) > i/2 + 1$.
  - $L(h^i(X); s)$ meromorphically extends to the whole plane, and possible poles can occur only when i is even and $s = i/2 + 1$.
  - $L(h^i(X); i/2 + 1) \neq 0$.
  - $\Lambda(h^i(X); s)$ has a functional equation

$$\Lambda(h^i(X); i + 1 - s) = \varepsilon(h^i(X); s)\Lambda(h^i(X); s).$$

⌟

Prop. (21.7.2.2). By(12.10.3.8), if $m < \frac{i+1}{2}$, there is an exact sequence

$$0 \to \operatorname{Fil}^n H^i_{\text{Betti}}(X, \mathbb{R}) \to H^i_{\text{Betti}}(X, \mathbb{R}(n-1))^{\mathsf{c}^* = (-1)^{n-1}} \to H^{i+1}_{\text{Del}}(X/\mathbb{R}, \mathbb{R}(n)) \to 0.$$

⌟

Prop. (21.7.2.3). If the functional equation and

$$\dim_{\mathbb{R}} H^{i+1}_{\text{Del}}(X/\mathbb{R}, \mathbb{R}(n)) = \begin{cases} \operatorname{ord}_{s=m} L(h^i(X), s) & , m < \frac{i}{2} \\ \operatorname{ord}_{s=m} L(h^i(X), s) - \operatorname{ord}_{s=m+1} L(h^i(X), s) & , m = \frac{i}{2} \end{cases}.$$

Notice if $m < i/2$, $H^{i+1}_{\text{Del}}(X/\mathbb{R}, \mathbb{R}(n)) = \{0\}$ iff $h^i(X)(m)$ is critical(21.7.1.2). ⌟

Proof: Cf.[Schneider's notes, P5].? □

Prop. (21.7.2.4) [Beilinson's Periods]. If $h^i(X)(m)$ is critical, then $H^{i+1}_{\text{Del}}(X/\mathbb{R}, \mathbb{R}(n)) = 0$, and the determinant c_{Bei} of the isomorphism

$$\operatorname{Fil}^n H^i_{\text{Betti}}(X, \mathbb{R}) \to H^i_{\text{Betti}}(X, \mathbb{R}(n-1))^{\mathsf{c}^* = (-1)^{n-1}}$$

satisfies $c_{\text{Bei}}(h^i(X)(m)) = c_{\text{Del}}(h^i(X)(m)) \in \mathbb{R}^\times/\mathbb{Q}^\times$. ⌟

Proof: Cf.[Deligne's conjecture, in Rapoports' notes, P42]?. □

<u>**Beilinson's Regulator Maps**</u>

Remark (21.7.2.5) [Beilinson't Regulator]. If $m < (i+1)/2$, then by(21.7.2.2), there is an isomorphism

$$\det \operatorname{Fil}^n H^i_{\text{Betti}}(X, \mathbb{R}) \otimes_{\mathbb{R}} \det H^{i+1}_{\text{Del}}(X/\mathbb{R}, \mathbb{R}(n)) \to \det H^i_{\text{Betti}}(X, \mathbb{R}(n-1))^{\mathsf{c}^* = (-1)^{n-1}},$$

and $\operatorname{Fil}^n H^i_{\text{Betti}}(X, \mathbb{R})$ and $H^i_{\text{Betti}}(X, \mathbb{R}(n-1))$ has natural $\mathbb{Q}$-structures. So if $\det H^{i+1}_{\text{Del}}(X/\mathbb{R}, \mathbb{R}(n))$ has a $\mathbb{Q}$-structure, then we can construct a $c_{\text{Bei}}(h^i(X)(m)) \in \mathbb{R}^\times/\mathbb{Q}^\times$. ⌟

Def. (21.7.2.6) [Beilinson's Regulator]. There is a regulator map(8.11.0.4)(8.11.0.6)

$$\begin{array}{ccccc} & (K_{2n-i-1}(X_{\mathbb{Z}})_{\mathbb{Q}})^{(n)} & & (K_{2n-i-1}(X_{\mathbb{R}})_{\mathbb{Q}})^{(n)} & \\ & \| & & \| & \\ r^{i+1}_X : & H^{i+1}_{\text{Mot}}(X, \mathbb{Q}(n))_{\mathbb{Z}} & \longrightarrow & H^{i+1}_{\text{Mot}}(X, \mathbb{Q}(n))_{\mathbb{R}} & \xrightarrow{\text{ch}_{2n-i-1}} H^{i+1}_{\text{Del}}(X/\mathbb{R}, \mathbb{R}(n)). \end{array}$$

⌟

Conj. (21.7.2.7) [Beilinson].

- If $w < -2$, then
  - $r_{\mathbb{R}} : H^{i+1}_{\text{Mot}}(X, \mathbb{Q}(n))_{\mathbb{Z}} \otimes \mathbb{R} \to H^{i+1}_{\text{Del}}(X/\mathbb{R}, \mathbb{R}(n))$(21.7.2.6) is an isomorphism.

– the determinant of the isomorphisms(21.7.2.2)

$$\begin{aligned}&\det \mathrm{Fil}^n H^i_{\mathrm{Betti}}(X,\mathbb{R})\otimes_{\mathbb{R}} \det(H^{i+1}_{\mathrm{Mot}}(X,\mathbb{Q}(n))_{\mathbb{Z}}\otimes\mathbb{R}) \xrightarrow{\mathrm{id}\otimes\det(r_{\mathbb{R}})}\\ &\det \mathrm{Fil}^n H^i_{\mathrm{Betti}}(X,\mathbb{R})\otimes_{\mathbb{R}} \det H^{i+1}_{\mathrm{Del}}(X/\mathbb{R},\mathbb{R}(n)) \to\\ &\det H^i_{\mathrm{Betti}}(X,\mathbb{R}(n-1))^{\mathsf{c}^*=(-1)^{n-1}}\end{aligned}$$

equals $L^\dagger(M;0)\in\mathbb{R}^\times/\mathbb{Q}^\times$.

- If $w=-2$, then $s=0$ may be a pole, and Tate conjecture predicts**?** that

$$-\operatorname{ord}_{s=0} L(M;0) = \dim_{\mathbb{Q}} N^{n-1}(X),$$

where $N^{n-1}(X)=\mathrm{CH}^{n-1}(X)/\mathrm{CH}^{n-1}(X)_0$, and $\mathrm{CH}^{n-1}(X)_0$ is the subgroup of homologically trivial cycle. In this case, there is also a cycle class map

$$r' : N^{n-1}(X)\to H^{i+1}_{M_\infty}(X_{\mathbb{R}},\mathbb{R}(n))\textbf{?},$$

and

– $(r\otimes r')\otimes\mathbb{R} : C_1\otimes\mathbb{R}\oplus N^{n-1}(X)\otimes\mathbb{R}\to H^{i+1}_{M_\infty}(X_{\mathbb{R}},\mathbb{R}(n))$ is an isomorphism.

– $L^\dagger(M,0)=\det(r\otimes r')\in\mathbb{R}^\times/\mathbb{Q}^\times$.

⌟

Def. (21.7.2.8) [Polylogarithm]. For $s\in\mathbb{Z}_+$, the power series

$$\mathrm{Li}_s(z)=\sum_{n\geq 1}\frac{z^n}{n^s}$$

converges absolutely for $|z|<1$ and can be analytically continued to a multi-valued function on $\mathbb{C}\backslash\{1\}$, called the **Polylogarithm function**. ⌟

Proof: In fact, $\mathrm{Li}_1(z)=-\log(1-z)$, and $\mathrm{Li}_{s+1}(z)=\int_0^z \mathrm{Li}_s(t)\frac{dt}{t}$. □

Def. (21.7.2.9) [Bloch-Wigner Dilogarithm]. The function

$$D(z)=\mathrm{Im}\left(\mathrm{Li}_2(z)+\log|z|\log(1-z)\right),\quad z\in\mathbb{C}(21.7.2.8)$$

is a real-valued function on $\mathbb{C}$, called the **Bloch-Wigner dilogarithm**. ⌟

Proof: Cf.[Blo00]P44. □

Height Pairings

Conj. (21.7.2.10) [Beilinson]. If $w=-1$, then M must be critical by drawing diagram, and

- There is a non-degenerate **Beilinson height paring**

$$h:\mathrm{CH}^n(X)_0\otimes \mathrm{CH}_0^{\dim X+1-n}\to\mathbb{R},$$

- and $\operatorname{ord}_{s=0}L(M;s)=\dim_{\mathbb{Q}}\mathrm{CH}^n(X)_0$.
- $L^\dagger(M;0)=c^+_{\mathrm{Del}}(M)\det(h)\in\mathbb{R}^\times/\mathbb{Q}^\times$.

⌟

Proof: □

3 Fontaine-Perrion.Riou Conjecture

Cf.[Fontaine-Perrion.Riou]**?**.

4 Examples

$\mathbb{A}^1$ Case

Prop. (21.7.4.1). For $k \in \mathbb{Z}_+$, $\zeta(2k) = \frac{B_{2k}}{(2k)!}(2\pi)^{2k}$. In particular, by(9.5.1.12),

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}, \quad \zeta(8) = \frac{\pi^8}{9450}.$$

⌟

Proof: Because

$$\cot(z) = i + \frac{2i}{e^{2iz} - 1},$$

$$z\cot(z) = 1 - \sum_{k=1}^{\infty} B_{2k}\frac{2^{2k}z^{2k}}{(2k)!}$$

where B_k are Bernoulli numbers(9.5.1.12). But also

$$z\cot(z) = 1 - 2\sum_{k=1}^{\infty}\zeta(2k)\frac{z^{2k}}{\pi^{2k}}.$$

by(11.4.3.11), thus the assertion follows. □

Cor. (21.7.4.2). For $k \in \mathbb{Z}_+$, $\zeta(1-2k) = (-1)^k\frac{B_{2k}}{2k}$. ⌟

Proof: **?** □

Prop. (21.7.4.3) [Leibniz Formula for π].

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots = \frac{\pi}{4}.$$

⌟

Proof: Use the arctan integration formula. □

Thm. (21.7.4.4) [Borel1972]. For $F \in \texttt{NField}$ and $m \in \mathbb{Z}_{>1}$, let

$$d_m = \mathrm{ord}_{s=1-m}\,\zeta_F(s) = \begin{cases} r_2 & ,m \in 2\mathbb{Z} \\ r_1 + r_2. & ,m \in 2\mathbb{Z}+1 \end{cases}.$$

Then

$$\dim_{\mathbb{Q}} K_{2m-1}(\mathcal{O}_F)_{\mathbb{Q}} = d_m$$

⌟

Proof: □

Prop. (21.7.4.5) [Comparison of Beilinson and Bloch's Regulator Maps]. Cf.[Rapoport, Comparison]. ⌟

Conj. (21.7.4.6) [Bloch Conjecture for Fields]. For a number field F, mapping the higher K-groups $K_{2i-1}(F)$ to a lattice with covolume $\zeta_F(m)$ via higher regulator maps. And the regular maps are made from m-th polylogarithm functions(21.7.2.8), so $\zeta_F(m)$ can be expressed by combinations of m-th polylogarithm functions of elements in F.

For example:

$$\zeta_{\mathbb{Q}(\sqrt{5})}(3) = \frac{24}{25\sqrt{5}}\operatorname{Li}_3(1)[\operatorname{Li}_3(\alpha) + \operatorname{Li}_3(-\alpha) + \frac{1}{2}(\log(\alpha))^3 - \frac{\pi^2}{6}\log(\alpha)], \alpha = \frac{\sqrt{5}-1}{2}.$$

This makes the numerical calculation of higher K-groups possible. ⌟

Proof: ? □

Remark (21.7.4.7). $m = 2$ case is proved by Bloch-Suslin-Merkuriev, $m = 3$ case is proved by Goncharov. ⌟

Elliptic Curve case

Def. (21.7.4.8) [Elliptic Dilogarithm]. Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{C}$ with complex parametrization $\mathbb{C}^\times/q^{\mathbb{Z}}$, define the **elliptic dilogarithm**:

$$D_q : \mathbb{C}^\times/q^{\mathbb{Z}} \to \mathbb{R} : z \mapsto \sum_{n\in\mathbb{Z}} D(q^n z)(21.7.2.9).$$

And it extends linearly to a map $Z_1(E) \to \mathbb{R}$. ⌟

Prop. (21.7.4.9) [Bloch]. Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{C}$, define

$$F : R(E)^\times \otimes R(E)^\times \to \mathbb{R} : f \otimes g \mapsto D_q(\sum m_i n_j [b_j - a_i]),$$

where $f, g \in R(E)^*$ with divisor $(f) = \sum m_i a_i, (g) = \sum n_j b_j$. Then F is additive, and

$$D(f \otimes (1-f)) = 0.$$

In particular, F factors through $R(E)^* \otimes R(E)^*/\{f \otimes (1-f)\} = K_2(R(E))$.

Thus, there is a composition $r_E : K_2(E) \to K_2(R(E)) \to \mathbb{R}$, called the (higher)**regulator map**. ⌟

Proof: □

Thm. (21.7.4.10) [Beilinson-Bloch]. Le $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ with complex parametrization $E(\mathbb{C}) \cong \mathbb{C}^\times/q^{\mathbb{Z}}$, then there exists a $\mathrm{Gal}_{\mathbb{Q}}$-invariant divisor P on E s.t. $D_q(P) \sim_{\mathbb{Q}^\times} L(E,2)/\pi$(21.7.4.8). ⌟

Proof: □

Thm. (21.7.4.11) [Weak Beilinson Conjecture, Beilinson-Bloch]. Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$. Situation as in(21.7.2.1), we consider the motive $h^1(E), i = 1, m = 1, n = 2$. Then $H^1_{\mathrm{Betti}}(E, \mathbb{R}(1))^{c^*=-1} \cong H^2_{\mathrm{Del}}(E/\mathbb{R}, \mathbb{R}(n))$ by(21.7.2.2).

Then there exists $\Phi \in H^2_{\mathrm{Mot}}(E_{\mathbb{Z}}, \mathbb{Q}(2))$ and $\Phi \in H^1_{\mathrm{Betti}}(E, \mathbb{Q}(1))^{c^*=-1}$ s.t.

$$r_{\mathrm{Del}}(\Phi) = L^\backprime(E,0)\Phi.$$

⌟

Proof: Cf.[Beilinson, Higher regulators of modular curves] and [Beilinson's Conjecture for elliptic curves with complex multiplication, Deninger-Wingberg]. □

Modular Curve case

Notation (21.7.4.12).
- Use notation as in Modular Curves.
- Denote $\Omega^1(M^c) = \varinjlim_K \Omega^1(M_K^c)$.

⌟

Prop. (21.7.4.13). Denote $\{\mathcal{O}^*(M_K), \mathcal{O}^*(M_K)\}$ the $\mathbb{Q}$-subspace of $H^2_{\mathrm{Mot}}(M_K, \mathbb{Q}(2))$ generated by the symbols $\{u, v\}$ with $u, v \in \mathcal{O}^*(M_K) \otimes \mathbb{Q} = H^1_{\mathrm{Mot}}(M_K, \mathbb{Q}(1))$.

Denote

$$\mathcal{Q}_K = H^2_{\mathrm{Mot}}(M_K^c, \mathbb{Q}(2)) \cap \{\mathcal{O}^*(M_K), \mathcal{O}^*(M_K)\},$$
$$\mathcal{P}_K = \cup K' \subset K\, \mathrm{Nm}_{K'/K}(\mathcal{Q}_{K'}) \subset H^2_{\mathrm{Mot}}(M_K^c, \mathbb{Q}(2)).$$

⌟

Prop. (21.7.4.14). By [Langlands, Modular Forms and l-adic Representations], The action of $GL(\mathbf{A}_f)$ on $\Omega^1(M^c)$ gives rise to a decomposition

$$\Omega^1(M) = \bigoplus_\pi V_\pi.$$

⌟

Proof: ? □

Thm. (21.7.4.15) [Beilinson's Conjecture for Modular Curves].
- $r_{\mathbb{R}}(\mathcal{P}_K)$(21.7.2.7) $= H^2_{\mathrm{Del}}(M_K^c/\mathbb{R}, \mathbb{R}(2)) = H^1_{\mathrm{Betti}}(M_K^c(\mathbb{R}), \mathbb{R}(1))$, thus giving a $\mathbb{Q}$-structure on $H^2_{\mathrm{Del}}(M_K^c, \mathbb{R}(2))$.
- Let g be the genus of M_K^c, then

$$\det r_{M_K^c}(\mathcal{P}_K) = L^{(g)}(H^1(M_K^c), 0) \cdot \det H^1_{\mathrm{Betti}}(M_K^c(\mathbb{R}), \mathbb{Q}(1)).$$

- $\mathcal{P}_K \subset H^2_{\mathrm{Mot}}(M_K^c, \mathbb{Q}(2))_{\mathbb{Z}}$.

⌟

Proof: This follows from(21.7.4.16), Cf.[Scholl, P8].? □

Thm. (21.7.4.16).
- For $u, v \in \mathcal{O}^*(M_K) \otimes \overline{\mathbb{Q}}$,

$$\int_{M_K(\mathbb{C})} \log|u| \overline{\mathrm{d}\log v} \wedge \omega \in \overline{\mathbb{Q}}.\Big(2\pi\,\mathrm{i}\, c^+(\pi) L'(\pi^\vee, 0)\Big) \in \overline{\mathbb{Q}} \otimes \mathbb{C}.$$

- For some choice of K, $\omega \in V_\pi^K$ and $u, v \in \mathcal{O}^*(M_K) \otimes \overline{\mathbb{Q}}$, the integral is non-zero.

⌟

Proof: Cf.[Scholl, Thm1.3.2].? □

Thm. (21.7.4.17). For χ s.t. $L(\pi\otimes\chi;1)\in(\overline{\mathbb{Q}}\otimes\mathbb{C})^\times$,

$$c^+(\pi)L'(\pi^\vee;0)\sim_{\overline{\mathbb{Q}}^\times}\frac{L(\pi;2)L(\pi\otimes\chi;1)}{L(\omega_\pi\chi;2)}.$$

⌟

Proof: Cf.[Scholl, Thm2.3].**?** □

Prop. (21.7.4.18). Situation as in(21.7.4.16),

$$\int_{M(\mathbb{C})}\log|u|\overline{\mathrm{d}\log v}\wedge\omega=\int_{M_K(\mathbb{C})}\mathcal{E}_\varphi(z,g;1)\overline{\eta}_\xi\wedge\omega.$$

⌟

21.8 Heegner Points

References are [Gross−Zagier formula and arithmetic fundamental lemma, Wei Zhang], [Gross-Zagier Formula notes], [Heegner Points and Representation Theory, Gross], [Gross–Zagier Revisited, Conrad]. [Moduli of Elliptic Curves, James Parson], [Heegner points and derivatives of L-series, Gross/Zagier]. http://math.columbia.edu/~yihang/GZSeminar.html.

1 Heegner Points

Def. (21.8.1.1) [Heegner Conditions]. Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ and $F/\mathbb{Q}$ an imaginary quadratic extension with $(d_F, N) = 1$ and associated quadratic character $\eta_F : (\mathbb{Z}/d_F)^\times \to \{\pm 1\}$. Then the **Heegner condition** is the hypothesis that every prime factor of N splits in F. ⌟

Prop. (21.8.1.2). In the Heegner situation(21.8.1.1), the sign of functional equation for E(21.2.6.4) $w_E = -1$**?**, thus $\mathrm{rank}_{\mathrm{an}}(E/\mathbb{Q})$ is odd and the BSD conjecture(21.6.1.1) predicts $\mathrm{rank}(E/\mathbb{Q})$ is odd, so at least it has a non-torsion rational point. ⌟

Def. (21.8.1.3) [Heegner Points]. In the Heegner situation(21.8.1.1), there exists an ideal $\mathcal{N} \subset \mathcal{O}_F$ of conductor N. Then for any $n \in \mathbb{Z}_+$, $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_F$ is an order of $\mathcal{O}_F$ of conductor n. Thus for $(n, N) = 1$,

$$\mathbb{C}/\mathcal{O}_F \to \mathbb{C}/(\mathcal{O}_F \cap \mathcal{N})^{-1}$$

is an isogeny of degree N, thus defines a point $x_n \in X_0(N)$, by moduli characterization**?**, called a **Heegner point**. Then by theory of complex multiplication**?**, x_n is defined over the ring class field F_n corresponding to the open compact subgroup $(\mathcal{O}_n \otimes \widehat{\mathbb{Z}})^\times \subset A_F^\times$. ⌟

Proof: □

Def. (21.8.1.4) [Heegner Points]. In the Heegner situation(21.8.1.1), using the modular parametrization $\varphi_E : X_0(N) \to E$ over $\mathbb{Q}$(19.4.2.6), $y_n = \varphi_E(x_n) \in E(K_n)$. In particular, define $y_F = \mathrm{tr}_{F_1/F}(y_1) \in E(F)$, called the (principal)**Heegner point of** E. ⌟

Prop. (21.8.1.5). The Heegner point $y_F \in E(F)$ is uniquely defined up to sign and torsion. ⌟

Proof: □

2 Gross-Zagier Formula

Thm. (21.8.2.1) [Gross-Zagier]. In the Heegner situation(21.8.1.1),

$$L'(E/F;1) = \frac{\int_{E(\mathbb{C})} \omega \wedge \overline{\omega}}{|d_F|^{1/2}} \cdot \frac{1}{c^2} \cdot \langle y_F, y_F \rangle_{\text{N-T}}$$

⌟

Proof: □

Cor. (21.8.2.2). If $\mathrm{rank}_{\mathrm{an}}(E/F) = 1$, then the Heegner point y_F is non-torsion, by(15.13.1.5). And if $\mathrm{rank}_{\mathrm{an}}(E/F) = 1$, y_F is torsion. ⌟

3 Kolyvagin's Work

Main references are [Gro89], [Finiteness of $E(\mathbb{Q})$ and Ш$(E/\mathbb{Q})$ for a subclass of Weil curves, Kolyvagin], [Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties, Kolyvagin-Yu] and [Euler Systems, Kolyvagin].

Def. (21.8.3.1) [Kolyvagin Primes]. In the Heegner situation(21.8.1.1), let $p \in \mathbf{P}$, a **Kolyvagin prime** ℓ for E is a prime $\ell \in \mathbf{P}\backslash S(Npd_F)$ s.t. ℓ is inert in F and $p|\ell+1, p|a_{\ell,E}$. Equivalently, Frob_ℓ is in the conjugacy class of $\mathsf{c} \in \mathrm{Gal}(F(E[p])/F)$**?**. So by Chebotarev density theorem, the set of Kolyvagin primes has positive Dirichlet density.

For a Kolyvagin prime ℓ, $M(\ell) = \min\{v_p(\ell+1), v_p(a_{\ell,E})\}$ is called the **Kolyvagin index** of ℓ.

A product of distinct Kolyvagin primes is called a **Kolyvagin number** for E. The set of Kolyvagin numbers is denoted by Λ_E. For a Kolyvagin number n, define the **Kolyvagin index** of n as $M(n) = \min_{\ell|n}\{M(\ell)\}$. ⌟

Prop. (21.8.3.2). In the Heegner situation(21.8.1.1), let ℓ be a Kolyvagin prime for E, then

$$\mathrm{Gal}(F_\ell/F_1) \cong \mathrm{Pic}(\mathcal{O}_\ell)/\,\mathrm{Pic}(\mathcal{O}_F) \cong \mathbb{Z}/(\ell+1) = \langle\sigma\rangle.$$

⌟

Proof: □

Def. (21.8.3.3) [Kolyvagin Derivative]. In the situation(21.8.3.1), let ℓ be a Kolyvagin prime for E, define the **Kolyvagin derivative** $D_\ell = \sum_{i=1}^{\ell} i\sigma^i \in \mathbb{Z}[\mathrm{Gal}(F_\ell/F_1)]$. Then $(\sigma-1)D_\ell = \ell+1-\mathrm{tr}_\ell$. ⌟

Prop. (21.8.3.4). In the situation(21.8.3.1), for $\ell \in \Lambda_E \cap \mathbf{P}$ and Heegner point $y_\ell \in E(F_\ell)$, $D_\ell y_\ell \in E(F_\ell)/p^M E(F_\ell) \subset H^1(F_\ell, E[p^M])$ is invariant under the action of $\mathrm{Gal}(F_\ell/F_1)$.

Thus for any $n \in \Lambda_E$ and $M \leq M(n)$, $D_n y_n \in H^1(F_n, E[p^M])$ is invariant under the action of $\mathrm{Gal}(F_\ell/F_1) \cong \prod_{\ell|n} G_\ell$, thus descends to an element in $H^1(F_1, E[p^M]) \cong H^1(F_n, E[p^M])^{\mathrm{Gal}(F_n,F_1)}$ by Hochschild-Serre spectral sequence(8.7.1.13) and the fact $E[p^M](K_n) = 0$**?** ⌟

Proof: By(21.8.3.3), it suffices to show that $(\sigma-1)D_\ell y_\ell = (\ell+1-\mathrm{tr}_\ell)y_\ell \in p^M E(F_1)$: This follows from the definition(21.8.3.1) and the fact $\mathrm{tr}_\ell\, y_\ell$ is just the Hecke operator action T_ℓ on y_1, which maps to $a_\ell y_1 \in E(F_1)$**?** □

Def. (21.8.3.5) [Kolyvagin Systems]. In the situation(21.8.3.1), for $n \in \Lambda_E$, define the **Kolyvagin cohomology classes**

$$c_M(n) = \sum_{s \in \mathrm{Gal}(F_1/F)} sD_n y_n \in H^1(F, E[p^M]), \quad M \leq M(n).$$

The collection of cohomology classes

$$\kappa = \{c_M(n) \in H^1(F, E[p^M]) | n \in \Lambda_E, M \in \mathbb{Z}_+, M \leq M(n)\}$$

is called a **Kolyvagin system** of E. ⌟

Def. (21.8.3.6) [p-Divisibility]. In the situation(21.8.3.1), for $r \in \mathbb{N}$, denote Λ_r to be the subset of Λ_E consisting of numbers with exactly r prime factors, and define $\mathcal{M}_r \in [0,\infty]$ to be the maximal integer s.t. $p^{\mathcal{M}_r}|c_M(n)$ for any $n \in \Lambda_r, M \leq M(n)$. ⌟

Prop. (21.8.3.7) [Order of Kolyvagin Systems]. In the situation(21.8.3.1), $\mathcal{M}_0 \geq \mathcal{M}_1 \geq \ldots \geq 0$.

In particular, we can define $\mathcal{M}_\infty = \lim_{r\to\infty} \mathcal{M}_r$. Clearly, $\mathcal{M}_\infty = \infty$ iff $\kappa = 0$. The **vanishing order of** κ is the minimal r s.t. $\mathcal{M}_r \neq \infty$, denoted by $\operatorname{ord}\kappa$. ⌟

Proof: □

Prop. (21.8.3.8). $\mathcal{M}_0$ is just the p-divisibility of the Heegner point y_F. In particular, $\mathcal{M}_0 < \infty$ iff y_F is non-torsion?. ⌟

Thm. (21.8.3.9) [Kolyvagin]. Let $\operatorname{ord}\kappa < \infty$, then

- $\mathrm{Sel}^{p^\infty}(E/F)$ is contained in the subgroup of $H^1(F, E[p^\infty])$ generated by κ.
- $\mathrm{rank}_p^{w_E(-1)^{\operatorname{ord}\kappa+1}}(E/F) = \operatorname{ord}\kappa + 1, \mathrm{rank}_p^{w_E(-1)^{\operatorname{ord}\kappa}}(E/F) = \operatorname{ord}\kappa - d$ and $d \in 2\mathbb{N}$.
- Let
$$\widetilde{Ш}(E/F)[p^\infty]^{\operatorname{ord}\kappa+1} = (\bigoplus_{i\geq 1} \mathbb{Z}/(p^{a_i}))^2, \quad \widetilde{Ш}(E/F)[p^\infty]^{\operatorname{ord}\kappa} = (\bigoplus_{i\geq 1} \mathbb{Z}/(p^{b_i}))^2,$$
where $(a_i), (b_i)$ is non-increasing, then
$$a_i = \mathcal{M}_{\operatorname{ord}\kappa+2i-1} - \mathcal{M}_{\operatorname{ord}\kappa+2i}, \quad b_{d+i} = \mathcal{M}_{\operatorname{ord}\kappa+2i-2} - \mathcal{M}_{\operatorname{ord}\kappa+2i-1}.$$

In particular, $\#\widetilde{Ш}(E/F)[p^\infty]^{\operatorname{ord}\kappa+1} \geq p^{\mathcal{M}_{\operatorname{ord}\kappa} - \mathcal{M}_\infty}$, with equality iff $d = 0$. ⌟

Proof: □

Cor. (21.8.3.10). If $\operatorname{ord}\kappa = 0$, i.e. y_F is non-torsion(21.8.3.8), then $d = 0$, and $r(E/\mathbb{Q}) = 1, \#Ш(E/K) < \infty$. ⌟

<u>**Kolyvagin's Conjecture**</u>

Conj. (21.8.3.11) [Kolyvagin]. Let $p \in \mathbf{P}\backslash\{2\}$ s.t. $\overline{\rho}_{E,p}$ is surjective, then $\kappa \neq \{0\}$. Equivalently, $\mathcal{M}_\infty < \infty$. ⌟

Thm. (21.8.3.12) [Zhang]. Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ with conductor N and $p \geq 5$ is good ordinary and $\overline{\rho}_{E,p}$ is surjective and ramifies at every prime $\ell \in \mathbf{P}$ s.t. $v_\ell(N) = 1$, then $\mathcal{M}_\infty = 0$. In particular, Kolyvagin's conjecture(21.8.3.11) is true. ⌟

Remark (21.8.3.13). There are results that generalize this. ⌟

Cor. (21.8.3.14). Under the hypothesis of(21.8.3.12), if $\mathrm{rank}_p(E/\mathbb{Q}) = 1$, then $r_{\mathrm{an}}(E/\mathbb{Q}) = r(E/\mathbb{Q}) = 1$, and $\#Ш(E/\mathbb{Q}) < \infty$. ⌟

Proof: Cf.[Wei Zhang]. □

4 p-adic Gross-Zagier Formula

References are [Heegner points and a p-adic Gross-Zagier formula].

5 Waldspurger's Period Formula

6 Higher Gross-Zagier over Function Fields, Yun-Zhang

Remark (21.8.6.1). The formula relates arbitrary order central derivative of the base change L-function of an unramified automorphic representation of $PGL(2)$ over a function field to the self-intersection number of a certain algebraic cycle on the moduli stack of Shtukas. ⌟

21.9 (Arithmetic)Gan-Gross-Prasad Conjecture

References are [Wei, More Arithmetic Fundamental Lemma Conjectures: The Case Of Bessel Subgroups].

1 Introduction

The GGP conjecture is a generalization of the the Gross-Zagier formula to higher dimensional varieties. It concerns the central derivative of the L-function and special cycles of Shimura varieties.

AGGP conjecture has applications to the Beilinson-Bloch conjecture, which is a generalization of the BSD conjecture.

2 restriction Problems

Conj. (21.9.2.1) [Local Restriction Problems]. Let K be a local field with an involution σ, $K_0 = K^\sigma$. Let $V \in \mathcal{V}\mathrm{ect}\,/K$ with a non-degenerate sesqui-linear form. Let $G(V)$ be the identity component of the subgroup of $GL(V_{k_0})$ preserving this form.

There are natural non-degenerate subspace $W \subset V$, there will be a subgroup $H \subset G(W) \times G(V)$ containing the diagonally embedded subgroup $G(W)$, and a unitary representation ν of H?.

The **local restriction problem** is to determine for each $\pi \in \mathrm{Irr}(G)$, the number

$$d(\pi) = \dim \mathrm{Hom}_H(\pi|_H \otimes \overline{\nu}, \mathbb{1}).$$

⌟

Def. (21.9.2.2)[Arithmetic Periods]. Let F be a global field and G a reductive group over F, $H \subset G$ an algebraic subgroup, $Z = Z(G) \cap H$. Denote $[H] = Z(A_F)H(F)\backslash H(A_F)$. For $\chi \in \widehat{H(A_F)}$, denote the (twisted)**automorphic L-period map**:

$$l_{H,\chi} : \mathcal{A}_0(G/F) \to \mathbb{C} : \varphi \mapsto \int_{[H]} \chi(h)\varphi(h)dh.$$

(? Convergence). ⌟

3 Statements

References are [Symplectic Local Root Numbers, Central Critical L-Values, And Restriction Problems In The Representation Theory Of Classical Groups, Gan-Gross-Prasad].

Conj. (21.9.3.1). ⌟

4 Arithmetic Fundamental Lemma

Jacquet−Rallis proposed an approach using relative trace formula to attack the unitary case of Gan−Gross−Prasad conjecture. The fundamental lemma is proved by Yun.

Later Wei Zhang proposed an analogous approach using the arithmetic fundamental lemma, equality between certain intersection numbers and the first derivatives of some relative orbital integrals, and is not proved yet.

21.10 Colmez Conjecture

Conj. (21.10.0.1) [Colmez]. Let (F,Φ) be a CM number field and $A\in \mathcal{A}b\mathcal{V}ar/F$ is a CM with type $(\mathcal{O}_F,\Phi)$ with good reduction $\mathcal{A}/\mathcal{O}_F$. Let $\alpha\in\wedge^g\Omega_{\mathcal{A}}$ be a Néron differential that is everywhere non-vanishing, and ⌟

Chowla-Selberg Formulas

Def. (21.10.0.2) [Epstein Zeta Functions]. For a positive-definite quadratic form $Q(X,Y)=aX^2+bXY+cY^2\in\mathbb{Z}[X,Y]$, the **Epstein zeta function** $\zeta_Q(s)$ is defined to be

$$\zeta_Q(s)=\frac{1}{2}\sum_{(m,n)\in\mathbb{Z}^2\backslash(0,0)}\frac{1}{Q(m,n)^{-s}}.$$

⌟

Thm. (21.10.0.3) [Chowla-Selberg Formula]. For a positive-definite quadratic form $Q(X,Y)=aX^2+bXY+cY^2\in\mathbb{Z}[X,Y]$ with discriminant $d=b^2-4ac<0$,

$$\begin{aligned}Z_Q(s)&=a^{-s}\zeta(2s)+a^{-s}\sqrt{\pi}\frac{\Gamma(s-1/2)}{\Gamma(s)}\zeta(2s-1)k^{1-2s}\\&+\frac{4a^{-s}k^{-s+1/2}}{\pi^{-s}\Gamma(s)}\sum_{n\in\mathbb{Z}_+}n^{s-1/2}\sigma_{1-2s}(n)K_{s-1/2}(2\pi n\frac{\sqrt{d}}{2a})\cos(n\pi b/a).\end{aligned}$$

⌟

Proof: □

Prop. (21.10.0.4) [Chowla-Selberg Formula]. Let $\mathcal{K}$ be an imaginary quadratic field with discriminant D and $f\in\mathbb{Z}_+$. For any proper ideals $\mathfrak{a}\in\mathrm{Cl}(\mathcal{O}_{\mathcal{K},f})$(14.4.1.48), denote

$$F(\mathfrak{a})=\Delta(\mathfrak{a})\Delta(\mathfrak{a}^{-1}),$$

then

$$\prod_{\mathfrak{a}\in\mathrm{Pic}(\mathcal{O}_{\mathcal{K},f})}F(\mathfrak{a})=\Big(\frac{2\pi}{f^2|d_{\mathcal{K}}|}\Big)^{12\,\mathrm{cl}(\mathcal{O}_{\mathcal{K},f})}\prod_{a=1}^{|d_{\mathcal{K}}|-1}\Big(\Gamma\Big(\frac{a}{|d_{\mathcal{K}}|}\Big)^{6\chi(a)\#\mu(\mathcal{K})}\Big)^{\mathrm{cl}(\mathcal{O}_{K,f})/\mathrm{cl}(\mathcal{K})}\cdot\Big(\prod_{p\in\mathtt{Prime},p|f}p^{12e(p)}\Big)^{\mathrm{cl}(\mathcal{O}_{\mathcal{K},f})},$$

where $\chi(a)=\left(\frac{d_{\mathcal{K}}}{a}\right)$ and

$$e(p)=\frac{(1-p^{-n})(1-\chi(p))}{(1-p^{-1})(p-\chi(p))}.$$

Notice that $6e(p)\,\mathrm{cl}(\mathcal{O}_{K,f})\in\mathbb{Z}$ by(14.4.3.7).

In particular, for $f=1$,

$$\prod_{\mathfrak{a}\in\mathrm{Cl}(\mathcal{K})}F(\mathfrak{a})=\Big(\frac{2\pi}{|d_{\mathcal{K}}|}\Big)^{12\,\mathrm{cl}(\mathcal{K})}\prod_{a=1}^{|d_{\mathcal{K}}|-1}\Gamma\Big(\frac{a}{|d_{\mathcal{K}}|}\Big)^{6\chi(a)\#\mu(\mathcal{K})},$$

⌟

Proof: Cf.[N-T91] and [Elliptic Functions, Weil]. □

1 Averaged Colmez Conjecture

References are [On Faltings heights of abelian varieties with complex multiplication, Xinyi Yuan].

22 Iwasawa Theory

22.1 Euler Systems

Cf.[Rub00], [Rub96], [Kat04] and [Scholl].

Notation (22.1.0.1).

- Fix $p \in \mathbf{P}$, $F \in \texttt{NField}$.
- For each modulus $\mathfrak{m}$ of F, let $F(\mathfrak{m})$ be the maximal p-extension of F inside the ray class field $F_{\mathfrak{m}}$, and $\Gamma_{\mathfrak{m}} = \mathrm{Gal}(F(\mathfrak{m})/F(1))$.
- Fix $T \in \mathrm{Rep}_{\mathbb{Z}_p}(\mathrm{Gal}_F), V = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, W = V/T = T \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p)$.
- Suppose T is unramified outside f.m. places of F.
- WARNING: notations in this section may subject to change.**?**

⌟

1 Local Cohomologies

This subsection should be moved to somewhere else.

Prop. (22.1.1.1). If $p \in \mathbf{P}, K \in \text{p-}\texttt{Field}, \ell \in \mathbf{P} \setminus \{p\}$, and $V \in \mathrm{Rep}^{\mathrm{fd}}_{\mathbb{Q}_\ell}(\mathrm{Gal}_K)$, then

$$\dim H^1_{\mathrm{ur}}(K,V) = V^{\mathrm{Gal}_K}, \quad \dim\Big(H^1(K,V)/H^1_{\mathrm{ur}}(K,V)\Big) = \dim H^2(K,V).$$

⌟

Proof: Cf.[Rubin, P5]. □

Prop. (22.1.1.2). Suppose $K \in \texttt{Field}$ and K_∞/K is an infinite p-extension, $T \in \mathrm{Rep}^{\mathrm{fg}}_{\mathbb{Z}_p}(\mathrm{Gal}_K)$, then

$$\varprojlim_{K \subset_{\mathrm{fin}} L \subset K_\infty} T^{\mathrm{Gal}_L} = 0,$$

where the transition maps are norm maps. ⌟

Proof: Define $T_0 = \varinjlim_{K \subset_{\mathrm{fin}} L \subset K_\infty} T^{\mathrm{Gal}_L} \subset T$, so T_0 is also f.g. over $\mathbb{Z}_p$. Then $T_0 = T^{\mathrm{Gal}_{L_0}}$ for some $K \subset_{\mathrm{fin}} L_0$. Then

$$\varprojlim_{K \subset_{\mathrm{fin}} L \subset K_\infty} T^{\mathrm{Gal}_L} = \varprojlim_{L_0 \subset_{\mathrm{fin}} L \subset K_\infty} T_0 = 0.$$

□

Prop. (22.1.1.3). If $\ell \in \mathbf{P} \setminus \{p\}$, $\mathbb{Q}_\ell \subset_{\text{fin}} K$, and K_∞ is the unique $\mathbb{Z}_p$-extension of K. Suppose $\{c_L\} \in \varprojlim_{K \subset_{\text{fin}} L \subset K_\infty} H^1(L,T)$, then for any L, $c_L \in H^1_{\text{ur}}(L,T)$. ⌟

Proof: K_∞/K is unramified**?**, so for any $K \subset_{\text{fin}} L \subset K_\infty$, there is an exact sequence

$$0 \to H^1_{\text{ur}}(L,T) \to H^1(L,T) \to H^1(I_K,T)^{\text{Gal}_K}.$$

But $H^1(I_K,T)$ is f.g. over $\mathbb{Z}_p$ by [Rubin, B.2.7]**?**, so taking limit of these exact sequences, we get

$$\varprojlim_{K \subset_{\text{fin}} L \subset K_\infty} H^1_{\text{ur}}(L,T) = \varprojlim_{K \subset_{\text{fin}} L \subset K_\infty} H^1(L,T)$$

by(22.1.1.2). □

Cor. (22.1.1.4). Let F_∞ be an $\mathbb{Z}_p^d$-extension of F, $F \subset_{\text{fin}} L \subset F_\infty$, and $v \in \Sigma_L^p$ has infinite decomposition group in $\text{Gal}(F_\infty/F)$. Suppose

$$\{c_L\} \in \varprojlim_{F \subset_{\text{fin}} L \subset F_\infty} H^1(L,T),$$

then $(c_L)_v \in H^1_{\text{ur}}(F_\lambda,T)$. In particular, this applies to $L = F$. ⌟

Proof: Cf.[Rubin, P155]. □

Cor. (22.1.1.5). If $\Sigma \subset \Sigma_F$ is a finite set of places containing all primes of F s.t. T is ramified, and all primes over p, and all primes whose decomposition group in $\text{Gal}(F_\infty/F)$ is finite, then

$$\varprojlim_{F \subset_{\text{fin}} L \subset F_\infty} H^1(L,T) = \varprojlim_{F \subset_{\text{fin}} L \subset F_\infty} H^1(F_\Sigma/L,T).$$

⌟

Proof: Cf.[Rubin, P155]. □

2 Selmer Groups

Def. (22.1.2.1) [Selmer Local Conditions]. For $F \in \texttt{NField}, v \in \Sigma_F^p$, denote

$$H^1_f(F_v,V) = H^1_{\text{ur}}(F_v,V) = \ker\Big(H^1(F_v,V) \to H^1(F_v^{\text{ur}},V)\Big) = H^1(F_v^{\text{ur}}/F_v, V^{I_v})(8.7.1.13)$$

And for places of F over p, fix a choice of invariant subspaces $H^1_s(F,V) \subset H^1(F_v,V)$.

Then we can define for any $v \in \Sigma_{\text{cycl}_{p,n}(\mathbb{Q})}$,

$$H^1_f(F_v,W) \subset H^1(F_v,W), \quad H^1_f(F_v,T) \subset H^1(F_v,T)$$

the image and inverse image of $H^1_f(F_v,V)$ under the maps on cohomologies induced by the exact sequence

$$0 \to T \to V \to W \to 0.$$

Next, for any $v \in \Sigma_F$, denote

$$H^1_s(F_v,T) = H^1(F_v,T)/H^1_f(F_v,T)$$

$$\text{loc}_v^s(T) : H^1(F,T) \to H^1_s(F_v,T)$$

and similarly for W. ⌟

Prop. (22.1.2.2). For $v \in \Sigma_F^p$,

- $H^1_f(F_v, W) = H^1_{\text{ur}}(F_v, W)_{\text{div}}$.
- $H^1_{\text{ur}}(F_v, T) \subset H^1_f(F_v, T)$ has finite index, and $H^1_s(F_v, T)$ is torsion-free.
- Let $\mathcal{W} = W^{I_v}/(W^{I_v})_{\text{div}}$ be finite, then there are natural isomorphisms
$$H^1_f(F_v, W)/H^1_{\text{ur}}(F_v, W) \cong \mathcal{W}/(\text{Frob}_v - 1)W, \quad H^1_{\text{ur}}(F_v, T)/H^1_f(F_v, T) \cong \mathcal{W}^{\text{Frob}_v = 1}.$$
- If T is unramified at v, then
$$H^1_f(F_v, W) = H^1_{\text{ur}}(F_v, W), \quad H^1_{\text{ur}}(F_v, T) = H^1_f(F_v, T)$$

⌟

Proof: 1, 2, 4 follow from 3. For 3, Cf.[Rubin, P6]**?**. □

Def. (22.1.2.3) [Selmer Groups]. Situation as in(22.1.2.1), define
$$\text{Sel}(F, W) = \ker\Big(H^1(F, W) \xrightarrow{\text{loc}^s(W)} \bigoplus_{v \in \Sigma_F} H^1_s(F_v, W)\Big).$$

Moreover, if Σ is a finite set of places, then we can define
$$\text{Sel}^\Sigma(F, W) = \ker\Big(H^1(F, W) \to \bigoplus_{v \notin \Sigma} H^1_s(F_v, W)\Big).$$
$$\text{Sel}_\Sigma(F, W) = \ker\Big(\text{Sel}^\Sigma(F, W) \to \bigoplus_{v \in \Sigma} H^1(F_v, W)\Big).$$

⌟

Def. (22.1.2.4) [Hypothesis]. Situation as in(22.1.2.1), assume for all the time that the choices $H^1_f(F_p, V)$ and $H^1_f(F_p, V^D)$ satisfy:

- $H^1_f(\text{cycl}_{p,n}(\mathbb{Q}_p), V)$ and $H^1_f(\text{cycl}_{p,n}(\mathbb{Q}_p), V^D)$ are orthogonal complements under the cup product pairing
$$H^1(\text{cycl}_{p,n}(\mathbb{Q}_p), V) \times H^1(\text{cycl}_{p,n}(\mathbb{Q}_p), V^D) \to H^2(\text{cycl}_{p,n}(\mathbb{Q}_p), \mathbb{Q}_p(1)) = \mathbb{Q}_p.$$ **?**
- For $m \geq n$,
$$\text{cor}^{\text{cycl}_{p,m}(\mathbb{Q}_p)}_{\text{cycl}_{p,n}(\mathbb{Q})} H^1_f(\text{cycl}_{p,m}(\mathbb{Q}), V) \subset H^1_f(\text{cycl}_{p,n}(\mathbb{Q}_p), V).$$
$$\text{res}^{\text{cycl}_{p,n}(\mathbb{Q}_p)}_{\text{cycl}_{p,m}(\mathbb{Q})} H^1_f(\text{cycl}_{p,n}(\mathbb{Q}), V) \subset H^1_f(\text{cycl}_{p,m}(\mathbb{Q}_p), V).$$

⌟

Prop. (22.1.2.5) [Selmer Group of Elliptic Curves]. If $T = T_p(E), W = E[p^\infty]$ where $E \in \mathcal{E}\text{ll}/\mathbb{Q}$, and define
$$H^1_f(\mathbb{Q}_{n,p}, V) = \text{Im}\Big(E(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p \hookrightarrow H^1(\mathbb{Q}_{n,p}, V)\Big),$$
then $\text{Sel}(\mathbb{Q}_n, W) = \text{Sel}^{p^\infty}(E/\mathbb{Q}_n)$(15.13.6.9)(15.13.6.4) is the classical Selmer group. ⌟

Proof: For $v \in \Sigma^p_{\mathbb{Q}_n}$, by(15.11.4.16), $\#E(\mathbb{Q}_{n,v})[p^\infty] < \infty$, so $E(\mathbb{Q}_{n,v}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$. And also by(22.1.1.1),
$$\dim H^1_f(\mathbb{Q}_{n,v}, V_p(E)) = \dim V_p(E)^{\text{Gal}_{\mathbb{Q}_{n,v}}} = 0,$$
because $\#E(\mathbb{Q}_{n,v})[p^\infty] < \infty$. So
$$H^1_f(\mathbb{Q}_{n,v}, W) = \text{Im}\Big(E(\mathbb{Q}_{n,v}) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(\mathbb{Q}_{n,v}, W)\Big)$$
for any place v. Thus the assertion follows from the definitions(22.1.2.1)(15.13.6.4). □

Selmer Groups over F_∞

Def. (22.1.2.6). Define Λ_p-modules22.2

$$\mathrm{Sel}(F_\infty, W) = \varinjlim_{F\subset_{\mathrm{fin}} F'\subset F_\infty} \mathrm{Sel}(F', W), \quad X_\infty = \mathrm{Hom}(\mathrm{Sel}(F_\infty, W^D), \mathbb{Q}_p/\mathbb{Z}_p),$$

$$H^1_\infty(F, T) = \varprojlim_{F\subset_{\mathrm{fin}} F'\subset F_\infty} H^1(F', T), \quad H^1_{\infty,s}(F_p, T) = \varprojlim_{F\subset_{\mathrm{fin}} F'\subset F_\infty} H^1_s(F', T).$$

where the transition maps are induced by restriction and corestriction maps(22.1.2.4). Then they are f.g. Λ_p-modules**?**.

Similarly define

$$\mathrm{Sel}_{S(p)}(F_\infty, W) = \varinjlim_{F\subset_{\mathrm{fin}} F'\subset F_\infty} \mathrm{Sel}_{S(p)}(F', W), \quad X_{\infty,S(p)} = \mathrm{Hom}(\mathrm{Sel}_{S(p)}(F_\infty, W^D), \mathbb{Q}_p/\mathbb{Z}_p).$$

⌟

Prop. (22.1.2.7). There is an exact sequence

$$0 \to H^1_{\infty,s}(F_p, T)/\operatorname{loc}^s_{\infty,S(p)}(H^1_\infty(F, T)) \to X_\infty \to X_{\infty,S(p)} \to 0.$$

⌟

Proof: Cf.[Rubin, P29].**?** □

Poitou-Tate Duality

Prop. (22.1.2.8) [Poitou-Tate Duality]. Let $m \in \mathbb{Z}^\times, \Sigma_0 \subset \Sigma \subset \Sigma_F$ be two finite set of places, then

- There are exact sequences

$$0 \to \mathrm{Sel}^{\Sigma_0}(F, W[m]) \to S^\Sigma(F, W[m]) \xrightarrow{\operatorname{loc}^s_{\Sigma,\Sigma_0}} \bigoplus_{v\in\Sigma\setminus\Sigma_0} H^1_s(F_v, W[m])$$

$$0 \to \mathrm{Sel}_\Sigma(F, W[m]) \to S^{\Sigma_0}(F, W[m]) \xrightarrow{\operatorname{loc}^f_{\Sigma,\Sigma_0}} \bigoplus_{v\in\Sigma\setminus\Sigma_0} H^1_f(F_v, W[m])$$

- $\mathrm{Im}(\operatorname{loc}^s_{\Sigma,\Sigma_0})$ and $\mathrm{Im}(\operatorname{loc}^f_{\Sigma,\Sigma_0})$ are orthogonal w.r.t. the pairing $\sum_{v\in\Sigma\setminus\Sigma_0}\langle -, -\rangle_v$.
- There is an isomorphism

$$\mathrm{Sel}_{\Sigma_0}(F, W^D[m])/\mathrm{Sel}_\Sigma(F, W^D[m]) \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Coker}(\operatorname{loc}^s_{\Sigma,\Sigma_0}), \mathbb{Z}_p/(m)).$$

⌟

Proof: 1 is clear, and 3 follows from 2. For 2, Cf.[Rubin, P17].**?** □

Remark (22.1.2.9). When Σ is large, we can make $\mathrm{Sel}_\Sigma(F, W^D[m]) = 0$, then $\#\mathrm{Sel}_{\Sigma_0}(F, W^D[m]) = \#\mathrm{Coker}(\operatorname{loc}^s_{\Sigma,\Sigma_0})$. So if we can construct enough element in $S^\Sigma(F, W[m])$, then we bound $\mathrm{Sel}_{\Sigma_0}(F, W^D[m])$. And this can be done by Kolyvagin's derivative construction4 applied to Euler classes. ⌟

Cor. (22.1.2.10). There is an isomorphism

$$\mathrm{Sel}(F, W^D)/\mathrm{Sel}_{S(p)}(F, W^D) \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Coker}(\operatorname{loc}^s_{S(p)}), \mathbb{Q}_p/\mathbb{Z}_p).$$

⌟

3 Euler Systems

Def. (22.1.3.1) [Euler Systems]. Suppose $F \in \texttt{NField}, p \in \mathbf{P}$ and F_∞/F is an $\mathbb{Z}_p^d$-extension s.t. no finite place of F splits completely(This is satisfies if F_∞ contains the cyclotomic $\mathbb{Z}_p$-extension of F**?**). Suppose

- $\mathcal{K}$ is an Abelian extension of F containing F_∞ and $F(\mathfrak{p})$ for any $\mathfrak{p} \in \Sigma_F^{\mathrm{fin}}$,
- $\mathcal{N}$ is an ideal of F divisible by p and all finite places that T is ramified(22.1.0.1).

Then an **Euler system** for $(T, \mathcal{K}, \mathcal{N})$ is a collection of cohomology classes

$$\mathbf{c} = \{\mathbf{c}_{F'} \in H^1(F', T) : F \subset_{\mathrm{fin}} F' \subset \mathcal{K}\}$$

satisfying

$$\mathrm{cor}_{F''/F'}(\mathbf{c}_{F''}) = \Big(\prod_{\mathfrak{q}\in\Sigma(F''/F')} P_{\mathfrak{q}}(||\mathfrak{q}||^{-1}\,\mathrm{Frob}_{\mathfrak{q}}^{-1})\Big)(\mathbf{c}_{F'}),$$

where $\Sigma(F''/F')$ is the set of finite places of F not dividing $\mathcal{N}$ that is ramified in F'' but not in F'.

And an Euler system for (T, F_∞) is any Euler system for such $(T, \mathcal{K}, \mathcal{N})$. ⌟

Example (22.1.3.2) [Euler Systems for $\mathbb{Q}$]. For $N \in \mathbb{Z}_+$, let $\mathcal{R}(N)$ be the set of square-free integers r s.t. $(r, N) = 1$, and $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, then an Euler system $\mathbf{c}$ for $(T, \mathbb{Q}_\infty)$ is a collection of cohomology classes

$$\mathbf{c}_{\mathbb{Q}_n(\mu_r)} \in H^1(\mathbb{Q}_n(\mu_r); T)$$

s.t. for any $r \in \mathcal{R}(N), \ell \in \mathbf{P}, r\ell \in \mathcal{R}(N)$ and $m \geq n \in \mathbb{N}$,

$$\mathrm{cor}_{\mathbb{Q}_n(\mu_{r\ell})/\mathbb{Q}_n(\mu_r)}(\mathbf{c}_{\mathbb{Q}_n(\mu_{r\ell})}) = P_\ell(\ell^{-1}\,\mathrm{Frob}_\ell^{-1})(\mathbf{c}_{\mathbb{Q}_n(\mu_r)}).$$

⌟

Def. (22.1.3.3). If $\mathbf{c}$ is an Euler system, denote $\mathbf{c}_{F,\infty}$ the corresponding element in $H^1_\infty(F, T)$, and the ideal

$$\mathrm{ind}_{\Lambda_p}(\mathbf{c}) = \{\varphi(\mathbf{c}_{F,\infty}) : \varphi \in \mathrm{Hom}_{\Lambda_p}(H^1_\infty(F, T), \Lambda_p)\} \subset \Lambda_p.$$

and also

$$\mathrm{ind}_{\mathbb{Z}_p}(\mathbf{c}) = \sup\{n : \mathbf{c}_F \in p^n H^1(F, T) + H^1(F, T)_{\mathrm{tor}}\}.$$

⌟

Twisting by Characters

Prop. (22.1.3.4) [Twisting Cohomology Groups]. For any extension of number fields $L/F \in \texttt{NField}$, denote $H^1_\infty(L, T) = \varprojlim_{F \subset_{\mathrm{fin}} F' \subset F_\infty} H^1(F'L, T)$, $L_\infty = LK_\infty$. Then for any character $\rho : \mathrm{Gal}(L_\infty/K) \to \mathbb{Z}_p^*$ and $S(p) \subset \Sigma \subset \Sigma_F$, then there are Gal_K-isomorphisms

$$H^1_\infty(L, T)(\rho) \cong H^1_\infty(L, T(\rho)), \quad \mathrm{Sel}_\Sigma(L_\infty, W)(\rho) \cong \mathrm{Sel}_\Sigma(L_\infty, W(\rho)).$$

⌟

Proof: Cf.[Rubin, P91].**?** □

Prop. (22.1.3.5). Suppose $\mathbf{c}$ is an Euler system for $(T,\mathcal{K},\mathcal{N})$, and $\rho:\mathrm{Gal}(F_\infty/F)\to\mathbb{Z}_p^*$ is a character with fixed field L and conductor $\mathfrak{f}$, then for any field $F\subset_{\text{fin}}F'\subset\mathcal{K}$, denote by $\mathbf{c}^\rho_{F'}\in H^1(F,T(\chi))$ the image of $\mathbf{c}_{F'L}(\rho)$ under the map

$$H^1(F'L,T)(\rho)\xrightarrow{\text{cor}}H^1(F',T(\rho)).$$

Then $\{\mathbf{c}^\rho_{F'}\}$ form an Euler system for $(T(\rho),\mathcal{K},\mathfrak{f}p^\infty\mathcal{N})$. ⌟

Proof: Cf.[Rubin, P30, 93].? □

4 Kolyvagin Derivatives

Def. (22.1.4.1) [Kolyvagin Primes]. Suppose $F\subset_{\text{fin}}F'\subset F_\infty, m\in\mathbb{Z}_+$, define $\mathcal{R}_{F',m}\subset\mathcal{R}(\mathcal{N})$ to be the set of products of primes $\mathfrak{q}$ of F s.t.

- $m|[F(\mathfrak{q}):F(1)]$,
- $P_\mathfrak{q}(||\mathfrak{q}||^{-1})/m\in\mathbb{Z}_p$,
- $\mathfrak{q}$ splits completely in $F'(1)/F$.

⌟

Def. (22.1.4.2) [Kolyvagin Derivatives]. For any $\mathfrak{q}\in\Sigma_F^p$, $\Gamma_\mathfrak{q}=\mathrm{Gal}(F(\mathfrak{q})/F(1))$ is canonical isomorphic to a cyclic group with generator $\sigma_\mathfrak{q}$(?, [Rubin, P62]). Define

$$D_\mathfrak{q}=\sum_{i=0}^{\#\Gamma_\mathfrak{q}-1}i\sigma_\mathfrak{q}^i\in\mathbb{Z}[\Gamma_\mathfrak{q}],$$

and for any $\mathfrak{r}\in\mathcal{R}(\mathcal{N})$, define

$$D_\mathfrak{r}=\prod_{\mathfrak{q}|\mathfrak{r}}D_\mathfrak{q}\in\mathbb{Z}[\Gamma_\mathfrak{r}].$$

And if $F\subset_{\text{fin}}L\subset F_\infty$, fix an element $N_{L(1)/L}\in\mathbb{Z}[\mathrm{Gal}(L(\mathfrak{r})/L)]$ whose restriction to $\mathrm{Gal}(F(1)/F)$ is $\sum_{\gamma\in\mathrm{Gal}(F(1)/F)}\gamma$, then define

$$D_{\mathfrak{r},L}=N_{L(1)/L}D_\mathfrak{r}.$$

⌟

Def. (22.1.4.3) [Kolyvagin Systems]. Suppose $\mathbf{c}$ is an Euler system, $F\subset_{\text{fin}}L\subset F_\infty, m\in\mathbb{Z}_+$, and $\mathfrak{r}\in\mathcal{R}_{L,m}$, define

$$\kappa_{L,\mathfrak{r},M}=\delta_L(\mathbf{d}(D_{\mathfrak{r},L}x_{F(\mathfrak{r})})\in H^1(F,W[m]).$$

⌟

Proof: ?. Cf.[Rubin, P66]. □

Cor. (22.1.4.4) [Properties of $\kappa_{L,\mathfrak{r},m}$].

- $\kappa_{L,1,m}$ is the image of $\mathbf{c}_L$ in $H^1(L,W[m])$.
- The restriction of $\kappa_{L,\mathfrak{r},m}$ to $L(\mathfrak{r})$ is the image of $D_{\mathfrak{r},L}\mathbf{c}_{L(\mathfrak{r})}$ in $H^1(L(\mathfrak{r}),W[m])$.
- $\kappa_{L,1,m}$ is compatible with m.

⌟

Proof: Cf.[Rubin, P67]?. □

Local Properties

Thm. (22.1.4.5). Suppose $F \subset_{\text{fin}} F' \subset F_\infty, m \in \mathbb{Z}_+$, and $\mathfrak{r} \in \mathcal{R}_{F',m}$, then

$$\kappa_{F,\mathfrak{r},m} \in \operatorname{Sel}^{S(p\mathfrak{r})}(F', W[m]).$$

⌟

Proof: Cf.[Rubin, P67]. □

Thm. (22.1.4.6) [Ramification of Kolyvagin Systems]. Suppose $F \subset_{\text{fin}} F' \subset F_\infty, m \in \mathbb{Z}_+$, and $\mathfrak{r}\mathfrak{q} \in \mathcal{R}_{F,m}$, then

$$\operatorname{loc}^s_{\mathfrak{q}}(\kappa_{F,\mathfrak{r}\mathfrak{q},m}) = \phi^{fs}_{\mathfrak{q}}(\kappa_{F,\mathfrak{r},m}).$$

⌟

Proof: Cf.[Rubin, P68]. □

5 p-adic L-Functions for Elliptic Curves

Thm. (22.1.5.1)[p-adic L-Functions]. Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}, p \in \mathbf{P}$. Suppose $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ has good ordinary reduction or multiplicative reduction at p. Let $\alpha \in \mathbb{Z}_p^*, \beta = p/\alpha \in p\mathbb{Z}_p^*$ be the eigenvalues of Frob_p on $T_p(E)$ if E has good ordinary reduction at p, or $(\alpha, \beta) = (1, p)$ or $(-1, -p)$ if E has split or non-split multiplicative reduction.

Then there exists $c_E \in \mathbb{Z}_+$ independent of p and a **p-adic L-function** $\mathcal{L}_E \subset c_E^{-1}\Lambda_p$ s.t. for any character χ of $\operatorname{Gal}(\operatorname{cycl}_p(\mathbb{Q})/\mathbb{Q})$ of finite order,

$$\chi(\mathcal{L}_E) = \begin{cases} (1-\alpha^{-1})^2 L(E;1)/\Omega_E & ,\chi = 1 \& E \text{ has good reduction at } p. \\ (1-\alpha^{-1}) L(E;1)/\Omega_E & ,\chi = 1 \& E \text{ has multiplicative reduction at } p. \\ \alpha^{-n}\tau(\chi) L(E,\chi^{-1};1)/\Omega_E & ,\mathfrak{c}(\chi) = p^n > 1 \end{cases}.$$

And for any $N \in \mathbb{Z}_+$, we can define

$$\mathcal{L}_{E,N} = \prod_{q|N, q\neq p} P_\ell(\ell^{-1}\operatorname{Frob}_\ell^{-1})\mathcal{L}_E \in \Lambda_p.$$

⌟

Proof: Cf.[Mazur-Tate-T]**?**. □

Coleman Map

Def. (22.1.5.2) [Coleman Map]. Suppose $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ has good ordinary reduction or multiplicative reduction at p, then there is an injective Λ_p-module map

$$\operatorname{Col}_\infty : H^1_{\infty,s}(\mathbb{Q}_p, T_p(E)) \hookrightarrow \Lambda_p$$

s.t.

- For any element $z = \{z_n\} \in H^1_{\infty,s}(\mathbb{Q}_p, T_p(E))$ and any non-trivial character χ of $G_n = \operatorname{Gal}(\operatorname{cycl}_{p,n}(\mathbb{Q})/\mathbb{Q})$ of conductor p^m,

$$\chi(\operatorname{Col}_\infty(z)) = \alpha^{-m}\tau(\chi)\sum_{\gamma\in G_n}\chi^{-1}(\gamma)\exp^*_{\omega_E}(z_n^\gamma).$$

- If χ_0 is the trivial character, then

$$\chi_0(\mathrm{Col}_\infty(z)) = (1-\alpha^{-1})(1-\beta^{-1})^{-1}\exp^*_{\omega_E}(z).$$

- If E has split multiplicative reduction at p, then the image of Col_∞ is contained in the augmentation ideal $\mathscr{J}_p$ of Λ_p.

$\lrcorner$

Proof: Cf.[Rubin short, Appendix]?. □

Local Cohomology Groups

Prop. (22.1.5.3). Let $K \in$ p-`Field` and $E \in \mathcal{E}\mathrm{ll}/K$ with a Neron differential ω_E, then $\mathrm{Tgt}^*(E/K) = K\omega_E$, and $\mathrm{Tgt}(E/K) = K\omega_E^*$. There exists an exponential map

$$\exp_E : \mathrm{Tgt}(E/K) \cong E(K) \otimes \mathbb{Q}_p$$

and the following diagram is commutative:

$$\begin{array}{ccccc} \mathrm{Tgt}(E/K) & & \xrightarrow{\quad\exp_E\quad} & & E(K)\otimes\mathbb{Q}_p \\ {\scriptstyle \cdot\omega_E^*}\uparrow & & & & \uparrow{\scriptstyle =} \\ K & \xleftarrow[\log_E]{} & \widehat{E}(\mathfrak{m}_K)\otimes\mathbb{Q}_p & \xrightarrow{\cong} & E_1(K)\otimes\mathbb{Q}_p \end{array}$$

where all the maps are isomorphisms. $\lrcorner$

Proof: ? □

Prop. (22.1.5.4). By the definition and local Tate pairing,

$$\mathrm{Hom}(E(\mathbb{Q}_{n,p}),\mathbb{Q}_p) = \mathrm{Hom}(H^1_f(\mathbb{Q}_{n,p},V_p(E)),\mathbb{Q}_p) \cong H^1_s(\mathbb{Q}_{n,p},V_p(E)).$$

So we can define a dual exponential map

$$\exp^*_E : H^1_s(\mathbb{Q}_{n,p},V) \to \mathrm{Tgt}^*(E/\mathbb{Q}_{n,p})$$

and its composite with ω_E^*:

$$\exp^*_{\omega_E} : H^1_s(\mathbb{Q}_{n,p},V) \to \mathrm{Tgt}^*(E/\mathbb{Q}_{n,p})/\omega_E \cong \mathbb{Q}_{n,p}.$$

More explicitly, for $z \in H^1_s(\mathbb{Q}_{n,p},V_p(E)), x \in E(\mathbb{Q}_{n,p})$,

$$\mathrm{tr}_{\mathbb{Q}_{n,p}/\mathbb{Q}_p}(\lambda_E(x)\exp^*_{\omega_E}(z)) = \langle x,z\rangle_{\mathbb{Q}_{n,p}}.$$

$\lrcorner$

Prop. (22.1.5.5).

$$\exp^*_{\omega_E}(H^1_s(\mathbb{Q}_p,T)) = \frac{1}{p}[E(\mathbb{Q}_p):E_1(\mathbb{Q}_p)+E(\mathbb{Q}_p)_{\mathrm{tor}}]\mathbb{Z}_p.$$

$\lrcorner$

Proof: By duality, if $\lambda_E(\mathbb{Q}_p) = p^{-a}\mathbb{Z}_p$, then $\exp^*_{\omega_E}(H^1_s(\mathbb{Q}_p,T)) = p^a\mathbb{Z}_p$. But $\lambda_E(E_1(\mathbb{Q}_p)) = p\mathbb{Z}_p$, so the assertion follows. □

6 Bounding Selmer Groups

Notation (22.1.6.1).

- Fix an Euler system $\mathbf{c}$ for (T, F_∞)(22.1.3.2). $\mathbf{c}_F \in \mathrm{Sel}^{S(p)}(F, T)$ by(22.1.1.4) and(22.1.2.2).
- Suppose the choices of Selmer local conditions satisfy hypothesis(22.1.2.4).

┘

Hypothesis on Representations

Def. (22.1.6.2) [Hypothesis]. T satisfies the hypothesis

Hypothesis $\mathrm{Hyp}(F_\infty; T)$ if:

- There exists $\tau \in \mathrm{Gal}_{F(1)F(\mu_{p^\infty})}$ s.t. $T/(\tau - 1)T$ is free of rank 1 over $\mathbb{Z}_p$, and
- $T/(p) \in \mathrm{Irr}_{\mathbb{F}_p}(\mathrm{Gal}_{F_\infty})$.

Hypothesis $\mathrm{Hyp}(F_\infty; V)$ if:

- There exists $\tau \in \mathrm{Gal}_{F(1)F(\mu_{p^\infty})}$ s.t. $\dim_{\mathbb{Q}_p} V/(\tau - 1)V = 1$, and
- $V \in \mathrm{Irr}_{\mathbb{Q}_p}(F_\infty)$.

Hypothesis $\mathrm{Hyp}(F_\infty/F)$ if:

- $\mathrm{rank}_{\mathbb{Z}_p}(\mathrm{Gal}_{F_\infty/F}) > 1$ or
- neither T nor $T(-1)$ is trivial, or
- F is imaginary quadratic, or
- F is totally real and leopoldt's conjecture holds for F.

┘

Prop. (22.1.6.3). Suppose $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ without CM, then

- $T = T_p(E)$ satisfies the hypothesis $\mathrm{Hyp}(\mathrm{cycl}_p(\mathbb{Q}); V)$(22.1.6.2), and $\#H^1(\mathbb{Q}(E[p^\infty])/\mathbb{Q}, E[p^\infty]) < \infty$.
- If $\rho_{E,p} : \mathrm{Gal}_\mathbb{Q} \to \mathrm{Aut}(T_p)$ is surjective, then $T_p(E)$ satisfies the hypothesis $\mathrm{Hyp}(\mathrm{cycl}_p(\mathbb{Q}), T)$(22.1.6.2), and $H^1(\mathbb{Q}(E[p^\infty])/\mathbb{Q}, E[p^\infty]) = 0$.

┘

Proof: By Weil pairing,

$$\rho_{E,p}(\mathrm{Gal}_{\mathbb{Q}(\mu_{p^\infty})}) = \rho_{E,p}(\mathrm{Gal}_\mathbb{Q}) \cap \mathrm{SL}(2, \mathbb{Z}_p).$$

When $\rho_{E,p} : \mathrm{Gal}_\mathbb{Q} \to \mathrm{Aut}(T_p)$ is surjective, then $\overline{\rho_{E,p}}$ is surjective thus irreducible, and also we can take $\rho_{E,p}(\tau) = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix}$. So $T_p(E)$ satisfies the hypothesis $\mathrm{Hyp}(\mathrm{cycl}_p(\mathbb{Q}), T)$.

And because E has no CM, by [Serre, Galois Property Points Elliptiques, (1972) Cor1 of Thm3], $\rho_{E,p}(\mathrm{Gal}_\mathbb{Q}) \subset \mathrm{GL}(2, \mathbb{Z}_p)$ is open. So $\rho_{E,p}|_{\mathrm{Gal}_{\mathbb{Q}(\mu_{p^\infty})}}$ is irreducible, and we can take $\rho_{E,p}(\tau) = \begin{bmatrix} 1 & x \\ & 1 \end{bmatrix}$ for some $x \neq 0$. So $T_p(E)$ satisfies the hypothesis $\mathrm{Hyp}(\mathrm{cycl}_p(\mathbb{Q}), V)$.

Finally, the cohomology group can be calculated directly?. □

Bounding Selmer Groups over F

Thm. (22.1.6.4). Suppose V satisfies $\mathrm{Hyp}(F;V)$(22.1.6.2), and V is not the trivial representation.

- If $\mathbf{c}_F \notin H^1(F,T)_{\mathrm{tor}}$, then $\#\,\mathrm{Sel}_{S(p)}(F,W^D) < \infty$.
- If $\mathrm{loc}_p^s(\mathbf{c}_\mathbb{Q}) \neq 0$ and $[H_s^1(\mathbb{Q}_p,T) : \mathbb{Z}_p \,\mathrm{loc}_p^s(\mathbf{c}_\mathbb{Q})] < \infty$, then $\#\,\mathrm{Sel}(\mathbb{Q},W^D) < \infty$.

(If V is trivial, this is true iff the Leopodlt's conjecture holds). ⌟

Proof: Cf.[Rubin, P24].?
2: It follows from(22.1.2.10) that

$$[\mathrm{Sel}(\mathbb{Q},W^D) : \mathrm{Sel}_p(\mathbb{Q},W^D)] = [H_s^1(\mathbb{Q}_p,T) : \mathbb{Z}_p \,\mathrm{loc}_p^s(\mathrm{Sel}^p(\mathbb{Q},T))] \leq [H_s^1(\mathbb{Q}_p,T) : \mathbb{Z}_p \,\mathrm{loc}_p^s(\mathbf{c}_\mathbb{Q})].$$

So the assertion follows from item1. □

Cor. (22.1.6.5). Suppose V satisfies $\mathrm{Hyp}(\mathrm{cycl}_p(\mathbb{Q});V)$(22.1.6.2), $\mathrm{loc}_p^s \mathbf{c}_\mathbb{Q} \neq 0$, and $\mathrm{rank}_{\mathbb{Z}_p} H_s^1(\mathbb{Q}_p,T) = 1$, then $\#\,\mathrm{Sel}^{p^\infty}(\mathbb{Q},W^D) < \infty$. ⌟

Proof: This is because $H_s^1(\mathbb{Q}_p,T)$ is torsion-free. □

Thm. (22.1.6.6). Suppose T satisfies $\mathrm{Hyp}(\mathrm{cycl}_p(\mathbb{Q});T)$(22.1.6.2), $p > 2$. Let $\Omega = \mathbb{Q}(W)\mathbb{Q}((\mathbb{Z}_p^*)^{1/p^\infty})$, where $\mathbb{Q}(W)$ is the minimal extension of $\mathbb{Q}$ that $\mathrm{Gal}_{\mathbb{Q}(W)}$ acts trivially on W.

- Then

$$\#\,\mathrm{Sel}_p(\mathbb{Q},W^D) \leq p^{\mathrm{ind}_{\mathbb{Z}_p}(\mathbf{c})}\#\Big(H^1(\Omega/\mathbb{Q},W)\cap \mathrm{Sel}^p(\mathbb{Q},W)\Big)\#\Big(H^1(\Omega/\mathbb{Q},W)\cap \mathrm{Sel}_p(\mathbb{Q},W^D)\Big)$$

- If $\mathrm{loc}_p^s(\mathbf{c}_\mathbb{Q}) \neq 0$(22.1.2.1), then

$$\#\,\mathrm{Sel}(\mathbb{Q},W^D) \leq [H_s^1(\mathbb{Q}_p,T) : \mathbb{Z}_p \,\mathrm{loc}_p^s(\mathbf{c}_\mathbb{Q})]\#\Big(H^1(\Omega/\mathbb{Q},W)\cap \mathrm{Sel}^p(\mathbb{Q},W)\Big)\#\Big(H^1(\Omega/\mathbb{Q},W^D)\cap \mathrm{Sel}_p(\mathbb{Q},W^D)\Big).$$

Notice $\#H^1(\Omega/\mathbb{Q},W)\#H^1(\Omega/\mathbb{Q},W^D) < \infty$ when V is irreducible and $\dim V > 2$, by [Rubin, P162].? ⌟

Proof: Cf.[Rubin, P24].?
2: Notice $H^1(\mathbb{Q},T)/\mathrm{Sel}^p(\mathbb{Q},T) \hookrightarrow \oplus_{v\in\Sigma_\mathbb{Q}^p} H_s^1(\mathbb{Q}_v,T)$ is torsion-free, so $\mathbf{c}_\mathbb{Q} \in p^n H^1(\mathbb{Q},T) + H^1(\mathbb{Q},T)_{\mathrm{tor}}$ implies $\mathbf{c}_\mathbb{Q} \in p^n \,\mathrm{Sel}^p(\mathbb{Q},T) + H^1(\mathbb{Q},T)_{\mathrm{tor}}$, which implies $\mathrm{loc}_p^s(\mathbf{c}_\mathbb{Q}) \in p^n \,\mathrm{loc}_p^s(\mathrm{Sel}^p(\mathbb{Q},T))$. Then the assertion follows from(22.1.2.10) and item1. □

Bounding Selmer Groups over F_∞

Prop. (22.1.6.7). Suppose V satisfies $\mathrm{Hyp}(F_\infty,V)$ with τ. Define Z(resp. Z^D) to be the maximal Gal_{F_∞}-stable submodule of $(\tau-1)W$(resp. W^D), and

$$a_\tau = [W^\tau : (W^\tau)_{\mathrm{div}}].\max(\#Z,\#Z^D).$$

Then $a_\tau < \infty$. And if T satisfies $\mathrm{Hyp}(F_\infty,T)$, then $a_\tau = 1$. ⌟

Proof: Cf.[Rubin, P98].? □

Thm. (22.1.6.8). Suppose V satisfies $\mathrm{Hyp}(F_\infty;V)$ and $\mathrm{Hyp}(F_\infty/F)$(22.1.6.2), $\mathbf{c}_{F,\infty} \notin H_\infty^1(F,T)_{\Lambda_p-\mathrm{tor}}$, then

- (Weak Leopoldt Conjecture) $X_{\infty,S(p)}$ is a torsion Λ_p-module.
- There exists $t \in \mathbb{N}$ s.t. $\operatorname{char}(X_{\infty,S(p)})|p^t \operatorname{ind}_{\Lambda_p}(\mathbf{c})$.
- If moreover T satisfies $\operatorname{Hyp}(F_\infty;T)$(22.1.6.2), then $\operatorname{char}(X_{\infty,S(p)})| \operatorname{ind}_{\Lambda_p}(\mathbf{c})$.

⌟

Proof: 1: [Rubin, Thm2.3.2].?

2,3: Cf.[Rubin, P101]?. Given item1, there exists an injective pseudo-isomorphism

$$\bigoplus_{i=1}^{r} \Lambda_p/(f_i) \to X_{\infty,S(p)},$$

where $f_{i+1}|f_i$. Then by(22.1.6.7), it suffices to show that $\operatorname{char}(X_{\infty,S(p)})|a_\tau^{5r} \operatorname{ind}_{\Lambda_p}(\mathbf{c})$.

Suppose $h \in \Lambda_p$ satisfies(22.1.6.14), and a finite set of places $\Sigma_F^\infty \cup S(p) \cup \operatorname{Ram}(T) \subset \Sigma \subset \Sigma_F$, then by(22.1.6.15),

$$h^r a_\tau^{5r} \mathbf{c}_L \in \operatorname{char}(X_{\infty,S(p)}).H^1(F_\Sigma/L,T)_{\mathrm{lf}}.$$

Then by taking limit over L(?[Rubin, P101]),

$$h^r a_\tau^{5r} \mathbf{c}_{F,\infty} \in \operatorname{char}(X_{\infty,S(p)}).H^1(F,T)_{\mathrm{lf}}.$$

Then by the definition of $\operatorname{ind}_{\Lambda_p}(\mathbf{c})$ and the fact h is prime to $\operatorname{char}(X_{\infty,S(p)})$(22.1.6.14), we get $\operatorname{char}(X_{\infty,S(p)})|a_\tau^{5r} \operatorname{ind}_{\Lambda_p}(\mathbf{c})$. □

Cor. (22.1.6.9). Suppose V satisfies $\operatorname{Hyp}(\operatorname{cycl}_p(\mathbb{Q});V)$(22.1.6.2), $\operatorname{loc}^s_{p,\infty}(\mathbf{c}_{F,\infty})$ is non-torsion over Λ_p, and $H^1_{\infty,s}(F_p,T)/\Lambda_p.\operatorname{loc}^s_{p,\infty}(\mathbf{c}_{F,\infty})$ is torsion, define

$$\mathcal{L} = \operatorname{char}\left(H^1_{\infty,s}(F_p,T)/\Lambda_p.\operatorname{loc}^s_{p,\infty}(\mathbf{c}_{F,\infty})\right),$$

then

- (Weak Leopoldt Conjecture) X_∞ is a torsion Λ_p-module.
- There exists $t \in \mathbb{N}$ s.t. $\operatorname{char}(X_\infty)|(p^t\mathcal{L})$.
- If T satisfies $\operatorname{Hyp}(F_\infty;T)$(22.1.6.2), then $\operatorname{char}(X_\infty)|\mathcal{L}$.

⌟

Proof: By(22.1.6.8), $X_{\infty,S(p)}$ is torsion over Λ_p, so by(22.1.2.7) and the hypothesis, X_∞ is also torsion over Λ_p, and

$$\operatorname{char}(X_\infty) = \operatorname{char}(X_{\infty,S(p)}) \operatorname{char}\left(H^1_{\infty,s}(F_p,T)/\operatorname{loc}^s_{p,\infty}(H^1_\infty(F,T))\right).$$

Notice the hypothesis also implies $\operatorname{loc}^s_{p,\infty}(H^1_\infty(F,T))$ has rank 1 over Λ_p, so by the definition of $\operatorname{ind}_{\Lambda_p}(\mathbf{c})$,

$$\operatorname{ind}_{\Lambda_p}(\mathbf{c})|\operatorname{char}\left(\operatorname{loc}^s_{p,\infty}(H^1_\infty(F,T))/\Lambda_p.\operatorname{loc}^s_{p,\infty}(\mathbf{c}_{F,\infty})\right).$$

Thus the assertion follows. □

Proof over F_∞

Lemma (22.1.6.10). Let $\rho : \mathrm{Gal}(F_\infty/F) \to \Lambda_p$ be a character, then theorem(22.1.6.8) for T and $\mathbf{c}$ are equivalent to the theorem for $T(\rho)$ and $\mathbf{c}^\rho$. ⌟

Proof: The hypothesis $\mathrm{Hyp}(F_\infty; V), \mathrm{Hyp}(F_\infty/F)$ and $\mathrm{Hyp}(F_\infty; T)$ depends only on T as a Gal_{F_∞}-module, so they are not affected. And the rest follows from the fact everything is twisted by ρ, by(22.1.3.4). □

Prop. (22.1.6.11). There are elements $z_1, \ldots, z_r \in X_{\infty,S(p)}$ and ideals $\mathfrak{g}_1, \ldots, \mathfrak{g}_r \in \Lambda_p$ s.t. for $1 \le k \le r$,

- $z_k \in \mathrm{ev}^*(\tau\, \mathrm{Gal}_{\Omega_\infty})$.
- $a_\tau \mathfrak{g}_k \in f_k \Lambda_p$, and $\mathfrak{g}_k \subset \mathfrak{g}_{k+1}$.
- There is a split exact sequence

$$0 \to \sum_{i=1}^{k-1} \Lambda_p z_i \to \sum_{i=1}^{k} \Lambda_p z_i \to \Lambda_p/\mathfrak{g}_k \to 0.$$

- $a_\tau(X_{\infty,S(p)}/\sum_{i=1}^r \Lambda_p z_i)$ is pseudo-null.

⌟

Proof: Cf.[Rubin, P98]. □

Def. (22.1.6.12) [Selmer Sequences and Kolyvagin Sequences]. Fix a sequence $(z_1, \ldots, z_r)$ for $X_{\infty,S(p)}$ as in(22.1.6.11), and let $Z_\infty \subset X_{\infty,S(p)}$ be the submodule they generate. Then for $0 \le k \le r$, $F \subset_{\mathrm{fin}} L \subset F_\infty$, then

- A **Selmer sequence** of length k is a sequence $(\sigma_1, \ldots, \sigma_k)$ s.t. Cf.[Rubin, P99].**?**
- A **Kolyvagin sequence** of length k for L and M is a sequence $(\mathfrak{Q}_1, \ldots, \mathfrak{Q}_k)$ of primes of L**?** Cf.[Rubin, P99].

Let $\Pi(k, L, M)$ be the set of Kolyvagin sequences of length k for F and M, and define

$$\Psi(k, L, M) = \sum_{\pi \in \Pi(k,L,M)} \sum_{\psi \in \mathrm{Hom}(\Lambda_p \kappa_{L,\mathfrak{r}(\pi),M}, \Lambda_{L,M})} \psi(\kappa_{L,\mathfrak{r}(\pi),M}) \subset \Lambda_{L,M}$$

⌟

Lemma (22.1.6.13). Suppose $G \in \mathcal{A}b^{\mathrm{fin}}$, $R \in \mathfrak{CRing}$ is a PID, and B is a f.g. $R[G]$-module without R-torsion. Suppose $f \in R[G]$ is a non-zerodivisor, $b \in B$, and

$$\{\psi(b) : \psi \in \mathrm{Hom}_{R[G]}(B, R[G])\} \subset fR[G],$$

then $b \in fB$. ⌟

Proof: Cf.[Rubin, P101]. □

Prop. (22.1.6.14). Situation as in(22.1.6.8), there exists $h \in \Lambda_p$ relatively prime to $\mathrm{char}(X_{\infty,S(p)})$, and for each $F \subset_{\mathrm{fin}} L \subset F_\infty$ a number $N_L \in p^{\mathbb{Z}_+}$, s.t. if $M \in p^{\mathbb{Z}_+}, N_L | M, 0 \le k \le r$, then

$$h a_\tau^5 \Psi(k, L, M N_L) \subset f_{k+1} \Psi(k+1, L, M)(22.1.6.12).$$

⌟

Proof: Cf.[Rubin, P100]**?**. □

Cor. (22.1.6.15). Situation and notation as in(22.1.6.14), if $F \subset_{\text{fin}} L \subset F_\infty$ and finite set of places $\Sigma_F^\infty \cup S(p) \cup \text{Ram}(T) \subset \Sigma \subset \Sigma_F$, then

$$h^r a_\tau^{5r} \mathbf{c}_L \in \text{char}(X_{\infty,S(p)}).H^1(F_\Sigma/L,T)_{\text{lf}}.$$

⌟

Proof: It follows from(22.1.6.14) and induction that

$$h^r a_\tau^5 \Psi(0,L,MN_L^r) \subset (\prod_{i=1}^r f_i)\Psi(r,L,M) \subset \text{char}(X_{\infty,S(p)})\Lambda_{L,M}.$$

By(22.1.6.13), it suffices to show that for any $\psi \in \text{Hom}(H^1(F_\Sigma/L,T),\Lambda_L)$, $h^r a_\tau^{5r}\psi(\mathbf{c}_L) \in \text{char}(X_{\infty,S(p)})\Lambda_L$. For this, notice by(22.1.4.4), $\kappa_{L,1,MN_L^r}$ is the image of $\mathbf{c}_L$ under the map

$$H^1(F_\Sigma/L,T)/(MN_L^r) \hookrightarrow H^1(F_\Sigma/L,W[MN_L^r]) \hookrightarrow H^1(L,W[MN_L^r]),$$

so we can define $\overline{\psi}$ to be the map

$$\Lambda_{L,MN_L^r}\kappa_{L,1,MN_L^r} \subset H^1(F_\Sigma/L,T)/(MN_L^r) \xrightarrow{\psi} \Lambda_{L,MN_L^r} \to \Lambda_{L,M}.$$

Then by definition $\overline{\psi}(\kappa_{L,1,MN_L^r}) \in \Psi(0,L,MN_L^r)\Lambda_{L,M}$, and $\overline{\psi}(\kappa_{L,1,MN_L^r}) \equiv \psi(\mathbf{c}_L)(\text{mod } M)$. Thus we get $\psi(\mathbf{c}_L) \in \Psi(0,L,MN_L^r)$ by noticing M can arbitrarily large.

□

7 Euler System for Elliptic Curves(Kato)

Thm. (22.1.7.1)[Kato]. Suppose $E \in \mathcal{E}\text{ll}/\mathbb{Q}$ with conductor N, and $p \in \mathbf{P}$. Then there exists $D, D \not\equiv 1 \mod p, (DD',6pN) = 1$, and $r_E \in \mathbb{Z}_+$ independent of p, and an Euler system $\overline{\mathbf{c}} = \overline{\mathbf{c}}(D,D')$ for $T_p(E)$(22.1.3.2):

$$\{\overline{\mathbf{c}}_{\mathbb{Q}_n(\mu_r)} \in H^1(\mathbb{Q}_n(\mu_r),T_p(E))\}_{r\in\mathcal{R}(NpDD'),n\in\mathbb{N}},$$

s.t. for any character $\chi \in \text{Gal}(\mathbb{Q}_n/\mathbb{Q})^\vee$,

$$\sum_{\gamma\in\text{Gal}(\mathbb{Q}_n/\mathbb{Q})} \chi(\gamma)\exp^*_{\omega_E}(\text{loc}_p^s(\overline{\mathbf{c}}_{\mathbb{Q}_n}^\gamma)) = r_E DD'(D-\chi^{-1}(D))(D'-\chi^{-1}(D'))L_{Np}(E,\chi;1)/\Omega_E.$$

⌟

Proof: Take $r = p^m$ and take corestriction to $\mathbb{Q}_n$. But we need to verify that $\exp^*_{\omega_E}\circ\text{loc}_p^s$ equals the dual exponential map defined in(22.4.3.2). □

Cor. (22.1.7.2). Situation as in(22.1.7.1), suppose that E has good ordinary reduction or multiplicative reduction at p, then there is an Euler system $\mathbf{c}$ for $T_p(E)$ s.t.

- $\exp^*_{\omega_E}(\text{loc}_p^s(\mathbf{c}_\mathbb{Q})) = r_E L_{Np}(E;1)/\Omega_E$.
- $\text{Col}_\infty(\text{loc}_{p,\infty}^s(\mathbf{c}_{\mathbb{Q},\infty})) = r_E\mathcal{L}_{E,N}$(22.1.5.1).

⌟

Proof: Let $\sigma_D, \sigma_{D'} \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ denote the automorphism $\zeta \mapsto \zeta^D, \zeta \in \mu_{p^\infty}$, then since $D, D' \nmid 1(\bmod\ p)$, $(D-\sigma_D)(D'-\sigma_{D'}) \in \Lambda_p$ is invertible. Let $\rho_{D,D'} \in \mathbb{Z}_p[[\mathrm{Gal}_\mathbb{Q}]]$ be any element that restricts to $(D-\sigma_D)^{-1}(D'-\sigma_{D'})^{-1}$, then we can define

$$\mathbf{c}_{\mathbb{Q}_n(\mu_r)} = (DD')^{-1}\rho_{D,D'}\bar{\mathbf{c}}_{\mathbb{Q}_n(\mu_r)},$$

which is also an Euler system, and by(22.1.7.1) and a change of variable, we get

$$\sum_{\gamma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})} \chi(\gamma) \exp^*_{\omega_E}(\mathrm{loc}^s_p(\mathbf{c}^\gamma_{\mathbb{Q}_n})) = r_E L_{Np}(E,\chi;1)/\Omega_E.$$

Then if χ is the trivial character, this gives equation1. And for any $\chi \in \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})^\vee$,

$$\chi\Big[\mathrm{Col}_\infty(\mathrm{loc}^s_{p,\infty}(\mathbf{c}_{\mathbb{Q},\infty}))\Big] =$$

$$\begin{cases} (1-\alpha^{-1})(1-\beta^{-1})^{-1}\exp^*_{\omega_E}(\mathrm{loc}^s_p(\mathbf{c}_\mathbb{Q})) = r_E L_{Np}(E;1)/\Omega_E & ,\chi = 1 \\ \alpha^{-n}\tau(\chi)\sum_{\gamma\in\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})}\chi^{-1}(\gamma)\exp^*_{\omega_E}(\mathrm{loc}^s_p(\bar{\mathbf{c}}^\gamma_{\mathbb{Q}_n})) = r_E L_{Np}(E;\chi^{-1},1)/\Omega_E & \mathfrak{c}(\chi) = p^n > 1 \end{cases}$$

$$= \chi(r_E\mathcal{L}_{E,N}).$$

Thus $\mathrm{Col}_\infty(\mathrm{loc}^s_{p,\infty}(\mathbf{c}_{\mathbb{Q},\infty})) = r_E\mathcal{L}_{E,N}$. □

Bounding Selmer Groups

Prop. (22.1.7.3). Suppose $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ without CM. Notation as in(22.1.7.1),

- If E has good ordinary reduction or non-split multiplicative reduction at p, then $X_\infty(E[p^\infty])$ is f.g. torsion over Λ_p, and there exists $t \in \mathbb{N}$ s.t. $\mathrm{char}(X_\infty)|(p^t\mathcal{L}_{E,N})$. And if $\rho_{E,p}$ is surjective with $p \nmid r_E\prod_{q|N,q\neq p}\ell_q(q^{-1})$, then $\mathrm{char}(X_\infty)|(\mathcal{L}_E)$.
- If E has split multiplicative reduction at p, then similar results hold with $\mathrm{char}(X_\infty)$ replaced by $\mathcal{J}\,\mathrm{char}(X_\infty)$.

⌟

Proof: Because Col_∞ is injective(22.1.5.2), by(22.1.7.2),

$$\mathcal{L} = \mathrm{char}\left(H^1_{\infty,/\mathrm{Sel}}(\mathbb{Q}_p,T)/\Lambda_p.\,\mathrm{loc}^s_{p,\infty}(\mathbf{c}_\mathbb{Q})\right)\Big|\,\mathrm{char}\left(\mathrm{Im}(\mathrm{Col}_\infty)/(\mathrm{Col}_\infty(\mathrm{loc}^s_{p,\infty}(\mathbf{c}_\mathbb{Q})))\right)\Big|(r_E\mathcal{L}_{E,N})$$

So item1 follows from(22.1.6.9). Notice the hypothesis are satisfied by(22.1.6.3). Item2 also follows, by noticing that $\mathrm{Im}(\mathrm{Col}_\infty) \subset \mathcal{J}_p$(22.1.5.2). □

Cor. (22.1.7.4) [Greenberg]. Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ without CM, then there exists $M_E \in \mathbb{Z}_+$ s.t. if $p \in \mathbf{P}$ is good ordinary for E and $p \nmid M_E$, then $X_\infty(E)$(22.1.2.6) has no non-zero finite submodules. ⌟

Proof: Cf.[Rubin short, P363] and [Greenberg, Iwasawa theory for p-adic Representations]**?**. □

Cor. (22.1.7.5). Let $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ without CM, $p \in \mathbf{P}$ is a good place for E and $p \nmid 2r_EM_E\prod_{q|N}\ell_q(q^{-1})$(22.1.7.1)(22.1.7.4), and $\rho_{E,p}$ is surjective, then

$$\#\text{Ш}(E)[p^\infty]\Big|\frac{L(E;1)}{\Omega_E}.$$

⌟

Proof: If p is good supersingular for E, then $p \nmid \#\widetilde{E}(\mathbb{F}_p)$, and Cf.[Rubin short, P362]**?**

If p is good ordinary for E, then by(22.1.7.4), we may assume $X_\infty(E) \subset \prod_i \Lambda_p/(f_i^{n_{ij}})$, and then

$$\mathrm{Sel}(\mathrm{cycl}_p(\mathbb{Q}), E[p^\infty])^{\mathrm{Gal}(\mathrm{cycl}_p(\mathbb{Q})/\mathbb{Q})} = (X_\infty(E))_{\mathrm{Gal}(\mathrm{cycl}_p(\mathbb{Q})/\mathbb{Q})} \subset \chi_0(\prod_i \Lambda_p/(f_i^{n_{ij}}))$$

and the RHS has cardinality $\chi_0(\mathrm{char}(X_\infty(E)))$, which by(22.1.7.3) divides

$$\chi_0(\mathcal{L}_E) = (1-\alpha^{-1})^2 \prod_{q|N} \ell_q(q^{-1}) L(E;1)/\Omega_E (22.1.5.1).$$

Also, one show by proof of Mazur control theorem that

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \to \mathrm{Sel}(\mathrm{cycl}_p(\mathbb{Q}), E[p^\infty])^{\mathrm{Gal}(\mathrm{cycl}_p(\mathbb{Q})/\mathbb{Q})}.$$

is injective with cokernel of order divisible by $(1-\alpha^{-1})^2$**?**. Thus the assertion follows. □

Cor. (22.1.7.6). Suppose $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ without CM, and $L(E;1) \neq 0$, then $\#E(\mathbb{Q}) < \infty, \#\text{Ш}(E) < \infty$. ⌟

Proof: This is proven by Kolyvagin before, but Kato proved it again as follows:

For each $q|N, \ell_q(q^{-1}) \neq 0$, so $L_{Np}(E;1) \neq 0$, and then by(22.1.7.2), $\mathrm{loc}_p^s(\mathbf{c}_\mathbb{Q}) \neq 0$, then it follows from(22.1.6.5) that $\mathrm{Sel}^{p^\infty}(E/\mathbb{Q}) < \infty$. Notice the hypothesis is satisfied by(22.1.5.5).

But then by Serre's theorem, $\rho_{E,p}$ is surjective for a.e. p, so by(22.1.7.5), $\text{Ш}(E)[p^\infty] = 0$ for a.e. e. Thus the assertion follows. □

Thm. (22.1.7.7) [Kato]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$, if $F/\mathbb{Q}$ is an Abelian extension and $\chi \in \mathrm{Gal}(F/\mathbb{Q})^\vee$, and $L(E,\chi;1) \neq 0$, then $\#E(F)^\chi < \infty, \#\text{Ш}(E_L)^\chi < \infty$. ⌟

Proof: We only prove for the case E without CM. For the CM case, Cf.[Coates-Wiles77], [Rubin, The Iwasawa Main conjecture for Imaginary Quadratic Fields] or [Rubin-Wiles, Mordell-Weil Groups of Elliptic Curves over Cyclotomic Fields].**?**

The proof is similar to that of(22.1.7.6): $\chi(\mathrm{char}(X_\infty(E)))$ is a non-zero multiple of $L(E,\chi;1)$, so $\#\,\mathrm{Sel}(\mathrm{cycl}_p(\mathbb{Q}), E[p^\infty])^\chi < \infty$. Then use a variant of(22.1.7.5) to bound $\#\text{Ш}(E)$. □

Cor. (22.1.7.8) [Kato]. For $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ and $F/\mathbb{Q}$ an Abelian extension, $p \in \mathbf{P}$, $E(\mathbb{Q}(\mu_{p^\infty}))$ is a f.g. Abelian group. ⌟

Proof: It follows from [Roh84]**?** that $L(E,\chi,1) \neq 0$ for a.e. character χ of finite order of $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$. **?** □

Def. (22.1.7.9) $[r_p(E/F)]$**.** For $F \in \mathtt{NField}, E \in \mathcal{E}\mathrm{ll}/F, p \in \mathbf{P}$, define

$$r_p(E/F) = \sum_{v \in S(p), E \text{ has potential supersingular reduction at } v} [F_v : \mathbb{Q}_p].$$

⌟

Conj. (22.1.7.10). For $F \in \mathtt{NField}, E \in \mathcal{E}\mathrm{ll}/F, p \in \mathbf{P}$, let $\Gamma = \mathrm{Gal}(\mathrm{cycl}_p(F)/F) \cong \mathbb{Z}_p$, then

$$\mathrm{rank}_{\mathrm{Frac}(\mathbb{Z}_p(\Gamma))}[\mathrm{Sel}(E/\mathrm{cycl}_p(F)) \otimes_{\mathbb{Z}_p(\Gamma)} \mathrm{Frac}(\mathbb{Z}_p(\Gamma))] = r_p(E/F) (22.1.7.9)$$

⌟

Proof: □

Conj.Cor. (22.1.7.11). For $F \in \texttt{NField}, E \in \mathcal{E}\mathrm{ll}/F, p \in \mathbf{P}$,

$$\mathrm{rank}_{\mathrm{Frac}(\Lambda_p)}[\mathrm{Sel}(E/\mathrm{cycl}_p(F)) \otimes_{\Lambda_p} \mathrm{Frac}(\Lambda_p)] \geq r_p(E/F)(22.1.7.9)$$

⌟

Proof: Cf.[Coates, Galois of Elliptic Curves, P19]. □

Cor. (22.1.7.12). For $F \in \texttt{NField}, E \in \mathcal{E}\mathrm{ll}/F, p \in \mathbf{P}$, if E has potential good ordinary reduction at all places dividing p, and $\mathrm{Sel}(E/F)$ is finite, then $\mathrm{Sel}(E/\mathrm{cycl}_p(F))^\vee$ is $\mathbb{Z}_p(\Gamma)$-torsion. ⌟

Proof:

□

Cor. (22.1.7.13). If $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ and $\mathrm{rank}_{\mathrm{an}}(E) = 0$, then $\mathrm{Sel}(E/\mathrm{cycl}_p(\mathbb{Q}))^\vee$ is Λ_p-torsion. ⌟

Proof: This follows from(21.6.2.1) and(22.1.7.12). □

Cor. (22.1.7.14). Suppose $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ and $p \in \mathbf{P}$ is of good ordinary reduction for E, then

$$\mathrm{Sel}(\mathbb{Q}(\mu_{p^\infty}), E)^\vee$$

is torsion over Λ_p. ⌟

Proof: Cf.[Kato]. □

Prop. (22.1.7.15) [Euler Characteristic of $\mathrm{Sel}(E/\mathrm{cycl}_p(F))$]. Let $p \in \mathbf{P} \setminus \{2\}, F \in \texttt{NField}$, and $E \in \mathcal{E}\mathrm{ll}/F$ with good ordinary reduction over all places $v \in S(p)$. Suppose $\mathrm{Sel}(E/F)$ is finite, then $\mathrm{Sel}(E/F)$ has finite Γ-Euler characteristic, and

$$\chi(\Gamma, \mathrm{Sel}(E/\mathrm{cycl}_p(F))) = \rho_p(E/F) = \Big|\frac{\#\text{Ш}(E/F)[p^\infty]}{(\#E(F)[p^\infty])^2} \cdot \prod_{v \in \Sigma_F^{\mathrm{fin}}} c_v \cdot \prod_{v \in S(p)} (\#\widetilde{E}_v(\kappa_v))^2\Big|_p^{-1}$$

⌟

Proof: Cf.[Coates, Galois cohomology of Elliptic Curves, P28]. □

8 Examples

Example (22.1.8.1). There are three elliptic curves of conductor 11 over $\mathbb{Q}$, namely

$$A_0 : y^2 + y = x^3 - x^2 - 10x - 20$$

$$A_1 : y^2 + y = x^3 - x^2$$

$$A_2 : y^2 + y = x^3 - x^2 - 7820x - 263580.$$

And they are all isogenous. ⌟

Proof: □

22.2 Iwasawa Theory

1 Iwasawa Theory for Fields

$\mathbb{Z}_[[T]]$

Prop. (22.2.1.1). ⌟

Iwasawa Algebra

Def. (22.2.1.2) [Iwasawa Algebra]. Let $\Gamma \cong \mathbb{Z}_p$, the **Iwasawa algebra** Λ_p is defined to be

$$\Lambda_p = \mathbb{Z}_p[\Gamma].$$

And it is non-canonically isomorphic to $\mathbb{Z}_p[[T]]$: Let γ be any topological generator of Γ, then

$$\Lambda_p \cong \mathbb{Z}_p[\Gamma] : \gamma \mapsto T + 1.$$

⌟

Proof: Let $\Gamma_n = \Gamma/\Gamma^{p^n}$, then it can be easily shown that $\mathbb{Z}_p[\Gamma_n] \cong \mathbb{Z}_p[T]/((T+1)^{p^n} - 1)$. Then it suffices to show that

$$\mathbb{Z}_p[[T]] \cong \varprojlim \mathbb{Z}_p[[T]]/((T+1)^{p^n} - 1).$$

For this, denote $P_n(T) = (T+1)^{p^n} - 1$, then $P_n(T)$ is distinguished(14.2.5.11), and $P_n(T)|P_{n+1}(T)$, and $P_{n+1}(T)/P_n(T) = (1+T)^{p^n(p-1)} + (1+T)^{p^n(p-2)} + \ldots + (1+T)^{p^n} + 1 \in (p, T)$ Thus $P_n(T) \in (p,T)^{n+1}$. By p-adic Weierstrass preparation theorem(14.2.5.12), for any $f(T) \in \mathbb{Z}_p[[T]]$ and $n \in \mathbb{N}$, $f(T) = q_n(T)P_n(T) + f_n(T)$, where $f_n(T)$ is a polynomial with degree$< p^n$.

And $f_{n+1}(T) - f_n(T) = (q_n - q_{n+1}P_{n+1}/P_n)P_n$, so by(14.2.5.14), $f_{n+1}(T) \equiv f_n(T) (\mathrm{mod}\ P_n(T))$ as polynomials. Then $(f_0, f_1, \ldots, f_n, \ldots) \in \varprojlim \mathbb{Z}_p[T]/(P_n(T))$.

Now if $f_k = 0$ for each k, then $P_k(T)|f(T)$ for each k, and then $f \in \cup_k (p,T)^{k+1} = 0$. And conversely, given any $(f_i) \in \varprojlim \mathbb{Z}_p[T]/(P_n(T))$, $f(T) = \lim f_k(T)$ exists in $\mathbb{Z}_p[[T]]$, and it can be shown that $f(T)$ is mapped to (f_i). Thus we are done. □

Def. (22.2.1.3) [Pseudo-Isomorphisms]. A homomorphism between Λ_p-modules are called a **pseudo-isomorphism** if its kernel and cokernel are all finite. ⌟

Lemma (22.2.1.4). If $f, g \in \Lambda_p$ are relatively prime(3.2.3.4), then

- The natural map $\Lambda_p/(fg) \to \Lambda_p/(f) \oplus \Lambda_p/(g)$ is an injection with finite cokernel.
- There exists an injection $\Lambda/(f) \oplus \Lambda/(g) \to \Lambda_p/(fg)$ with finite cokernel.

⌟

Proof: Cf.[Mazur Control Theorem, P9]. □

Thm. (22.2.1.5) [Classification of Modules over Λ_p]. For $M \in \mathcal{M}\mathrm{od}^{\mathrm{fg}}_{\Lambda_p}$, there exists $r, s, t, n_i, m_j \in \mathbb{N}$ and f_j distinguished and irreducible, s.t. M is pseudo-isomorphic to

$$\Lambda_p^{\oplus r} \oplus (\bigoplus_{i=1}^{s} \Lambda_p/(p^{n_i})) \oplus (\bigoplus_{j=1}^{t} \Lambda_p/(f_j(T)^{m_j})).$$

⌟

Proof: Cf.[Washington, P272] or [Mazur Control Theorem, P11]. □

Prop. (22.2.1.6). If $B \in \mathcal{M}\mathrm{od}_{\Lambda_p}^{\mathrm{tor,fg}}$, then there exists $f_i \in \Lambda_p^*$ and a pseudo-isomorphism(22.2.1.3)

$$B \to \bigoplus_i \Lambda_p/(f_i).$$

Moreover, the ideal $(\prod_i f_i) \subset \Lambda_p$ is well-defined, called the **characteristic ideal of** B, denoted by $\mathrm{char}(B)$. ⌟

Proof: □

Prop. (22.2.1.7). If $X \in \mathcal{M}\mathrm{od}_{\Lambda_p}^{\mathrm{fg}}$ and $\#X_\Gamma < \infty$, then X is torsion over Λ_p. ⌟

Proof: Cf.[Washington]. □

22.3 p-adic L-Functions

1 p-adic L-Functions

Main references are [Fontaine's rings and p-adic L-functions, Colmez], and [Mazur, B.; Tate, J.; Teitelbaum, J. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. Invent. Math. 84 (1986), no. 1, 1–48.]

Thm. (22.3.1.1)[Kummer]. Let $a \geq$ be coprime to p and $k \geq 1$. If $n_1, n_2 \geq k$ that $n_1 \equiv n_2 \mod \varphi(p)$, then

$$(1 - a^{n_1})\frac{B_{n_1}}{n_1} \equiv (1 - a^{n_2})\frac{B_{n_2}}{n_2} \mod p^k.$$

⌟

Proof: Cf.[p-adic L-functions, Colmez]P5. □

Remark (22.3.1.2). This has vast generalizations in Iwasawa theory, Cf.[Iwasawa, On p-adic L-functions]. ⌟

2 Iwasawa Main Conjectures

[Wiles, A. The Iwasawa conjecture for totally real fields. Ann. of Math. (2) 131 (1990), no. 3, 493 – 540], [Rubin, Karl The "main conjectures" of Iwasawa theory for imaginary quadratic fields. Invent. Math. 103 (1991), no. 1, 25–68.].

Thm. (22.3.2.1)[Herbrand]. Let $p \in \mathbf{P}$, $Y = \mathrm{Cl}(\mathbb{Q}(\mu_p))[p]$, then $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) = (\mathbb{Z}/(p))^\times$ acts on Y as a $\mathbb{F}_p$-space by conjugation. Let Y^j be the subspace of Y that $(\mathbb{Z}/(p))^\times$ acts by character $a \mapsto a^j$. Then for $1 < j < p-1$ an odd integer, if $Y^j \neq 1$, then the Bernoulli number B_{p-j} has numerator divisible by p. ⌟

Proof: Cf.[Eisenstein Ideals, Mazur, P52]. □

3 Iwasawa Main Conjectures for GL(2)

Main references are [the Iwasawa Main Conjectures for GL(2), Skinner-Urban].

22.4 Kato's Euler Systems

Cf.[Kat04] and [Scholl], [Chao Li's Notes].

1 Kato-Siegel Functions

Thm. (22.4.1.1) [Kato-Siegel-Functions]. For $d \in \mathbb{Z}$ prime to 6, there exists a unique rule ϑ_d that associates each elliptic curve E/S a section $\vartheta_d^{(E/S)} \in \mathcal{O}^*(E \setminus E_S[d])$. satisfying:

- $\mathrm{div}(\vartheta_d^{(E/S)}) = d^2(e_E) - E_S[d]$.
- For a base change $g : E'/S' \to E/S$, $g^*\vartheta^{(E/S)} = \vartheta^{(E'/S')}$.
- If $\alpha : E/S \to E'/S$ is an isogeny and $(\deg \alpha, d) = 1$, then $\alpha_*\vartheta_d^{(E/S)} = \vartheta_d^{(E'/S)}$.
- $\vartheta_{-d} = \vartheta_d$,$\vartheta_1 = 1$. And if $d = mc$ where $m, c \in \mathbb{Z}_+$, then

$$[m]_*\vartheta_d = \vartheta_c^{m^2}, \quad \vartheta_c \circ [m] = \vartheta_d/\vartheta_m^{c^2}.$$

  In particular, $[d]_*\vartheta_d = 1$.

- If $\tau \in \mathscr{H}$ and $E_\tau/\mathbb{C} = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$, then

$$\vartheta_d^{(E_\tau/\mathbb{C})}(u) = (-1)^{\frac{d-1}{2}}\Theta(u,\tau)^{d^2}\Theta(du,\tau)^{-1},$$

  where

$$\Theta(u,\tau) = q^{\frac{1}{12}}(t^{1/2} - t^{-1/2})\prod_{n\in\mathbb{Z}_+}(1-q^n t)(1-q^n t^{-1}), \quad q = e^{2\pi\,\mathrm{i}\,\tau}, t = e^{2\pi\,\mathrm{i}\,u}.$$

  In fact, this should be the case over the Tate curve.

⌟

Proof: Cf.[Scholl, P384]**?** □

Modular Eisenstein Series

Def. (22.4.1.2) [Eisenstein Series]. Let $S \in \mathcal{S}\mathrm{ch}_{\mathrm{int}}, E \in \mathcal{E}\mathrm{ll}/S, d, N \in \mathbb{Z}_+$, $(N,d) = 1$, and $x \in E(S)$ is a torsion section of exact order N. If x is disjoint with $E_S[d]$, then $\vartheta_d(x) = x^*\vartheta_d \in \mathcal{O}^*(S)$. This is the case if N is invertible on S or N is not a prime power.

In this case, define

$$\mathrm{dlog}_v\,\vartheta_d \in \Gamma(E \setminus E_S[d], \Omega^1_{E/S})$$

and

$${}_d\,\mathrm{Eis}(E/S,x) = x^*\mathrm{d}\log_v\vartheta_d \in \Gamma(S, x^*\Omega^1_{E/S}) = \Gamma(S,\omega_{E/S}).$$

is a modular form of weight 1(20.2.5.1).

Of course, we can also define $\mathrm{dlog}\,\vartheta_d(x) \in \Gamma(S,\Omega^1_S)$. ⌟

Def. (22.4.1.3) [Eis$(E/S,x)$]. Situation as in (22.4.1.2), by(22.4.1.1), for $d, d' \in \mathbb{Z}$ prime to 6,

$$(\vartheta_d)^{d'^2} \cdot\!\cdot \vartheta_{d'} \circ [d] = (\vartheta_{d'})^{d^2} \cdot\!\cdot \vartheta_d \circ [d'] = \vartheta_{dd'},$$

so

$$d'^2\mathrm{d}\log_v\vartheta_d - [d']^*\mathrm{d}\log_v\vartheta_d = d^2\mathrm{d}\log_v\vartheta_{d'} - [d]^*\mathrm{d}\log_v\vartheta_{d'}.$$

And
$$d'^2{}_d\operatorname{Eis}(E/S,x) - d'{}_d\operatorname{Eis}(E/S,d'x) = d^2{}_{d'}\operatorname{Eis}(E/S,x) - {}_{d}{}_{d'}\operatorname{Eis}(E/S,dx).$$
In particular, if $d \equiv 1 \mod N$ and $d \neq \pm 1$, then
$$\operatorname{Eis}(E/S,x) = \frac{1}{d^2-d}{}_d\operatorname{Eis}(E/S,x) \in \Gamma(S[\frac{1}{d(d-1)}],\omega)$$
is independent of d. And because d is arbitrary, we can in fact glue the definition to a section
$$\operatorname{Eis}(E/S,x) \in \Gamma(S[\frac{1}{2N}],\omega).$$

⌟

Cor. (22.4.1.4). For any $d \in \mathbb{Z}$ prime to 6,
$${}_d\operatorname{Eis}(E/S,x) = d^2\operatorname{Eis}(E/S,x) - d\operatorname{Eis}(E/S,dx) \in \Gamma(S[\frac{1}{2N}],\omega).$$

⌟

Example (22.4.1.5) [Eisenstein Series Over $\mathbb{C}$]. If $E = \mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$, and $x = \frac{a_1}{N}\omega_1 + \frac{a_2}{N}\omega_2 \in E[N]\setminus\{O\}$, then
$$\operatorname{Eis}(E/\mathbb{C},x) = \Big(\sum_{m_i \in \frac{a_i}{N}+\mathbb{Z}} \frac{1}{(m_1\omega_1+m_2\omega_2)|m_1\omega_1+m_2\omega_2|^{2s}}\Big)\Big|_{s=0} du.$$

⌟

Proof: Cf.[Scholl, P389]. □

Example (22.4.1.6) [Eisenstein Sereis over Tate Curves]. Consider the Tate curve $\operatorname{Tate}(q)$ over $\mathbb{Z}[\mu_N]((q^{1/N}))$, there is a level N structure
$$(\mathbb{Z}/(N))^2 \cong \operatorname{Tate}(q)_{\mathbb{Z}[\mu_N]((q^{1/N}))}[N] : (a_1,a_2) \mapsto \zeta_N^{a_1} q^{a_2/N}.$$
Then if $x = \zeta_N^{a_1} q^{a_2/N}, 0 \leq a_1, a_2 < N$, then
$$\operatorname{Eis}(\operatorname{Tate}(q)/\mathbb{Z}[\mu_N]((q^{1/N})),x) = \begin{cases} \Big[\frac{a_2}{N} - \frac{1}{2} - \sum_{n\in\mathbb{Z}_+}\Big(\sum_{d\in\mathbb{Z}, d|n, n/d \equiv a_2 (\mathrm{mod}\ N)} \operatorname{sgn}(d)\zeta_N^{a_1 d}\Big)q^{n/N}\Big]\operatorname{dlog} t & a_2 \neq 0 \\ ? & a_2 = 0 \end{cases}$$

Similarly, we can calculate that in $\Omega^1_{\mathbb{Z}[\mu_N]((q^{1/N}))/\mathbb{Z}}$,
$$\operatorname{dlog}\vartheta_d(x) \equiv \frac{{}_d\operatorname{Eis}(\operatorname{Tate}(q)/\mathbb{Z}[\mu_N]((q^{1/N})),x)}{\operatorname{dlog} t}(a_1\operatorname{dlog}\zeta_N + a_2\operatorname{dlog}(q^{1/N}))(\mathrm{mod}\ N).$$

⌟

Proof: Cf.[Scholl, P390]. □

2 Norm Relations

Suppose $\ell \in \mathbf{P}$, and $d, d' \in \mathbb{Z}$ s.t. $(6\ell, dd') = 1$. Denote $\vartheta = \vartheta_d^{(E/S)}$ and $\vartheta' = \vartheta_{d'}^{(E/S)}$.

Prop. (22.4.2.1). If $S = Y_H$ is a modular curve of level prime to ℓ, and z, z' are torsion sections of $E/S(\ell)$ whose projections onto $E_S[\ell]$ are linearly independent, then

$$\mathrm{Nm}_{S(\ell)/S}\{\vartheta(z), \vartheta'(z')\} = (1 - T_\ell \circ \langle \ell \rangle_* + \ell \langle \ell \rangle_*)\{\vartheta(\ell z), \vartheta'(\ell z')\}.$$

⌟

Proof: Cf.[Scholl, P399]**?**. □

Prop. (22.4.2.2). Suppose Y_H is a modular curve of level prime to ℓ and z, z' are two torsion sections of $E/Y_H(\ell^m, \ell^n)$ with $m, n \in \mathbb{Z}_{\geq 2}$. If the projections of z, z' into $E_S[\ell]$ are linearly independent, then

$$\mathrm{Nm}_{Y_H(\ell^m,\ell^n)/Y_H(\ell^{m-1},\ell^{n-1})}\{\vartheta(z), \vartheta(z')\} = \{\vartheta(\ell z), \vartheta'(\ell z')\}.$$

⌟

Proof: Cf.[Scholl, P400]**?**. □

Prop. (22.4.2.3). Suppose Y_H is a modular curve of level prime to ℓ and z, z' are two torsion sections of $E/Y_H(\ell^m, \ell^n)$ with $m, n \in \mathbb{Z}_{\geq 2}$. If the projections of z, z' into $E_S[\ell]$ are linearly independent, then

$$\mathrm{tr}_{Y_H(\ell^m,\ell^n)/Y_H(\ell^{m-1},\ell^{n-1})}\left({}_d\mathrm{Eis}(z) \cdot {}_{d'}\mathrm{Eis}(z')\right) = \ell^{-2}{}_d\mathrm{Eis}(\ell z) \cdot {}_{d'}\mathrm{Eis}(\ell z')$$

$$\mathrm{tr}_{Y_H(\ell^m,\ell^n)/Y_H(\ell^{m-1},\ell^{n-1})}\left(\mathrm{KS}\left({}_d\mathrm{Eis}(z) \cdot {}_{d'}\mathrm{Eis}(z')\right)\right) = \ell^2\,\mathrm{KS}\left(\ell^{-2}{}_d\mathrm{Eis}(\ell z) \cdot {}_{d'}\mathrm{Eis}(\ell z')\right)$$

⌟

Proof: Cf.[Scholl, P401]**?**. □

3 Dual Exponentials

Notation (22.4.3.1).

- Let $p \in \mathbf{P}$, $\mathbb{Q}_p \subset_{\text{fin}} K$.
- Let $K_n = K(\mu_{p^n})$, and $\mathfrak{d}_n = \mathfrak{d}_{K_n/K}$.

⌟

Def. (22.4.3.2) [Bloch-Kato Dual Exponential Maps]. For any $V \in \mathrm{Rep}_{\mathbb{Q}_p}^{\mathrm{dR}}(\mathrm{Gal}_K)$, the **dual exponential map**

$$\exp_p^* : H^1(K, V) \to D_{\mathrm{dR}}^0(V)$$

is defined to be

$$H^1(K, V) \to H^1(K, B_{\mathrm{dR}}^0 \otimes_{\mathbb{Q}_p} V) \overset{(18.4.5.5)}{=} H^1(K, \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_K D_{\mathrm{dR}}(V))) \cong D_{\mathrm{dR}}^0(V).$$

where the last isomorphism follows from Tate's computation(18.4.1.12) and the isomorphisms $B_{\mathrm{dR}}^j / B_{\mathrm{dR}}^{j+1} \cong \mathbb{C}_K(j)$. ⌟

Example (22.4.3.3). In case that $X \in \mathcal{S}\mathrm{m}\mathcal{P}\mathrm{rpr}/K$ and $V = H^1(X, \mathbb{Q}_p(1))$, if $D^1_{\mathrm{dR}}(V) = 0$, then the Hodge-Tate decomposition

$$\mathbb{C}_K \otimes_{\mathbb{Q}_p} V \cong \otimes_{i\in\mathbb{Z}} \mathbb{C}_K(-i) \otimes_K \mathrm{gr}^i D_{\mathrm{dR}}(V),$$

so the the dual exponential map is just

$$H^1(K,V) \to H^1(K, \mathbb{C}_K \otimes_K V) \cong H^1(K, \mathbb{C}_K) \otimes_K D^0_{\mathrm{dR}}(V) \xleftarrow{\cup \log \chi_{\mathrm{cycl}}} D^0_{\mathrm{dR}}(V).$$

⌟

Cor. (22.4.3.4). If Y be a smooth $\mathcal{O}_K$-scheme, which is a complement in a smooth proper $\mathcal{O}_K$-scheme X of a divisor Z with relatively normal crossings, define

$$H^i_{\mathrm{dR}}(Y/\mathcal{O}_K) = H^i(X, \Omega^i_{X/\mathcal{O}}(\log Z)),$$

and $V = \mathrm{H}^1_{\text{ét}}(Y_{\overline{K}}, \mathbb{Q}_p(1))$.

Then V is also de Rham, and the deRham comparison also holds?, so

$$D^{-1}_{\mathrm{dR}}(V) = D_{\mathrm{dR}}(V) = H^1_{\mathrm{dR}}(Y/\mathcal{O}_K) \otimes_{\mathcal{O}_K} K,$$
$$D^0_{\mathrm{dR}}(V) = H^0(X, \Omega^1_{X/\mathcal{O}_K}(\log Z)) \otimes_{\mathcal{O}_K} K = \mathrm{Fil}^1 H^1_{\mathrm{dR}}(Y/\mathcal{O}_K) \otimes_{\mathcal{O}_K} K,$$
$$D^1_{\mathrm{dR}}(V) = 0.$$

Thus by the same reasoning as in(22.4.3.3), the dual exponential map is known if we can compute the projection

$$\mathrm{pr}_1 : \mathbb{C}_K \otimes_{\mathbb{Q}_p} V \cong \mathbb{C}_K \otimes_{\mathcal{O}_K} H^0(X, \Omega^1_{X/\mathcal{O}_K}(\log Z)) \bigoplus \mathbb{C}_K(1) \otimes_{\mathcal{O}_K} H^1(X, \mathcal{O}_X) \to \mathbb{C}_K \otimes_{\mathcal{O}_K} H^0(X, \Omega^1_{X/\mathcal{O}_K}(\log Z)),$$

which is the inversion by p of the limit of the map

$$H^1_{\text{ét}}(Y_{\overline{K}}, \mu_{p^n}) \cong H^0(Y_{\overline{K}}, \mathcal{O}^*_{\overline{K}}/p^n) \xleftarrow{\cong} H^0(Y_{\mathcal{O}_{\overline{K}}}, \mathcal{O}^*/p^n) \xrightarrow{\mathrm{dlog}} H^0(X, \Omega^1_{X/\mathcal{O}_K}(\log Z)) \otimes \mathcal{O}_{\overline{K}}/p^n.$$

⌟

Proof: Cf.[Scholl, P408].? □

Explicit Reciprocity Law

Thm. (22.4.3.5). If $2 \neq p \in \mathbf{P}$, $K/\mathbb{Q}_p$ is unramified, then there exists $c \in \mathbb{N}$ s.t. for any $n \in \mathbb{Z}_+$, the following diagram

$$\begin{array}{ccc}
K_2(Y_{\mathcal{O}_{K_n}}) \otimes \mu_{p^n}^{-1} & \xrightarrow{\quad c_2 \quad} & H^2(Y_{K_n}, \mu_{p^n}) \\
\big\downarrow \mathrm{dlog} & & \big\downarrow \text{H-S} \\
H^0(X_{\mathcal{O}_{K_n}}, \Omega^2_{X_{\mathcal{O}_{K_n}}/\mathcal{O}_K}(\log Z))(-1) & & H^1(K_n, H^1(Y_{\overline{K}}, \mu_{p^n})) \\
\big\| & & \big\downarrow \mathrm{pr}_1 (\mathrm{mod}\ p^{n-1}) \\
\Omega^1_{\mathcal{O}_{K_n}/\mathcal{O}_K}(-1) \otimes \mathrm{Fil}^1 H^1_{\mathrm{dR}}(Y/\mathcal{O}_K) & & H^1(K_n, \mathcal{O}_{\overline{K}}/p^{n-1}) \otimes_{\mathcal{O}_K} \mathrm{Fil}^1 H^1_{\mathrm{dR}}(Y/\mathcal{O}_K) \\
\mathrm{dlog}(\zeta_{p^n}) \otimes [\zeta_{p^n}]^{-1} \mapsto 1 \big\downarrow \cong & & \big\uparrow \cup \frac{1}{p^n} \log \chi_{\mathrm{cycl}} \\
\mathcal{O}_{K_n}/\mathfrak{d}_n \otimes_{\mathcal{O}_K} \mathrm{Fil}^1 H^1_{\mathrm{dR}}(Y/\mathcal{O}_K) & \longrightarrow & \mathcal{O}_{K_n}/p^{n-1} \otimes_{\mathcal{O}_K} \mathrm{Fil}^1 H^1_{\mathrm{dR}}(Y/\mathcal{O}_K)
\end{array}$$

where H-S is the Hochschild-Serre boundary map defined as in(10.1.4.15), dlog is defined in(10.1.4.12), pr_1 is defined in(22.4.3.4). ⌟

Proof: Cf.[Scholl, P410]. □

Remark (22.4.3.6). ? The assumption that $K/\mathbb{Q}_p$ is unramified is not essential for the proof. The case $p=2$ is excluded because we don't know the compatibility of the trace map in this case. ⌟

Cor. (22.4.3.7) [Kato's Explicit Reciprocity Law]. If $2\neq p\in\mathbf{P}$, $K/\mathbb{Q}_p$ is unramified, then for any $m\in\mathbb{N}$, the following diagram is commutative:

$$\begin{array}{ccc}
\varprojlim_n (K_2(Y_{\mathcal{O}_{K_n}}))\otimes\mu_{p^n}^{-1} & \xrightarrow{\text{H-S}\circ c_2} & \varprojlim_n H^1(K_n, H^1(Y_{\overline{K}},\mu_{p^n})) \\
\downarrow{\scriptstyle \mathrm{dlog}} & & \downarrow{\scriptstyle \mathrm{cor}} \\
\varprojlim_n H^0(X_{\mathcal{O}_{K_n}},\Omega^2_{X_{\mathcal{O}_{K_n}}/\mathcal{O}_K}(\log Z))(-1) & & \varprojlim_{n\geq m} H^1(K_m, H^1(Y_{\overline{K}},\mu_{p^n})) \\
\| & & \| \\
\varprojlim_n \Omega^1_{\mathcal{O}_{K_n}/\mathcal{O}_K}(-1)\otimes \mathrm{Fil}^1 H^1_{\mathrm{dR}}(Y/\mathcal{O}_K) & & H^1(K_m, H^1(Y_{\overline{K}},\mathbb{Z}_p(1))) \\
{\scriptstyle \mathrm{dlog}(\zeta_{p^n})\otimes[\zeta_{p^n}]^{-1}\mapsto 1}\downarrow{\scriptstyle\cong} & & \downarrow{\scriptstyle \exp^*} \\
\mathcal{O}_{K_n}/\mathfrak{d}_n\otimes_{\mathcal{O}_K}\mathrm{Fil}^1 H^1_{\mathrm{dR}}(Y/\mathcal{O}_K) & \xrightarrow{\{\frac{1}{p^n}\mathrm{tr}_{\mathcal{O}_{K_n}/\mathcal{O}_{K_m}}\}_{n\geq m}} & K_m\otimes_{\mathcal{O}_K}\mathrm{Fil}^1 H^1_{\mathrm{dR}}(Y/\mathcal{O}_K)
\end{array}$$

⌟

Proof: It follows from(22.4.3.4) that there is a commutative diagram

$$\begin{array}{ccc}
H^1(K_m, H^1(Y_{\overline{K}},\mathbb{Q}_p(1))) & \xrightarrow{\mathrm{pr}_1} & H^1(K_m,\mathbb{C}_K\otimes_{\mathcal{O}_K}\mathrm{Fil}^1 H^1_{\mathrm{dR}}(Y/\mathcal{O}_K)) \\
\downarrow{\scriptstyle \exp^*} & & \| \\
K_m\otimes_{\mathcal{O}_K}\mathrm{Fil}^1 H^1_{\mathrm{dR}}(Y/\mathcal{O}_K) & \xrightarrow{\cup\log\chi_{\mathrm{cycl}}} & H^1(K_m,\mathbb{C}_K)\otimes_{\mathcal{O}_K}\mathrm{Fil}^1 H^1_{\mathrm{dR}}(Y/\mathcal{O}_K)
\end{array}.$$

And also for any $n\geq m$, there exists a commutative diagram(Cf. [Scholl, P416]?)

$$\begin{array}{ccc}
\mathcal{O}_{K_n} & \xrightarrow{\frac{1}{p^n}\log\chi_{\mathrm{cycl}}} & H^1(K_n,\mathcal{O}_{\mathbb{C}_K}) \\
{\scriptstyle \frac{1}{p^{n-m}}\mathrm{tr}_{\mathcal{O}_{K_n}/\mathcal{O}_{K_m}}}\downarrow & & \downarrow{\scriptstyle \mathrm{cor}} \\
\mathcal{O}_{K_m} & \xrightarrow{\frac{1}{p^m}\log\chi_{\mathrm{cycl}}} & H^1(K_m,\mathcal{O}_{\mathbb{C}_K})
\end{array}.$$

Thus the assertion follows from(22.4.3.5) by taking limit and inverting p. ? How the check the compatibility of the limits? □

4 Rankin-Selberg Convolution

Notations

Def. (22.4.4.1). For $t\in\mathbb{Q}_p$ with $v_p(t)<0$, denote

$$\phi_p^0=\chi_{\mathbb{Z}_p\times\mathbb{Z}_p},\quad \phi_p^{1,t}=\chi_{(t+\mathbb{Z}_p)\times\mathbb{Z}_p},\quad \phi_p^{2,t}=\chi_{(t+\mathbb{Z}_p)\times\mathbb{Z}_p^*}-p^{-1}\chi_{(t+p^{-1}\mathbb{Z}_p)\times\mathbb{Z}_p^*}.$$

And for any $\varphi\in C^\infty(\mathbb{Z}_p\times\mathbb{Z}_p)$, denote $\varphi^{\mathrm{tr}}(x,y)=\varphi(y,x)$.

For $\varphi\in\mathscr{S}(\mathbf{A}_f^2)$ and $\delta\in\mathbf{I}_f$, denote $[\delta]\varphi(\underline{x})=\varphi(\delta^{-1}\underline{x})$. ⌟

Results

Notation (22.4.4.2) [Setup].

- Let $F \in S_{k+l}(\Gamma(1))$, generating an irreducible $\pi = \otimes' \pi_p$, and whose Whittaker function $A(g) = \prod A_p(g_p)$ factorizes, with $A_p(1) = 1$ for each p.?
- Let ε be the character of $GL(2, \mathbf{A}_f)$ on A^*?.
- Let $M, R, N \in \mathbb{Z}_+, (R, N) = 1, M|N$.
- If $p \nmid N$, then A_p is assumed to be $\mathcal{K}_p$-invariant.
- Let $\lambda : \mathbf{I}_f / \mathbb{Q}_+^\times \to \mathbb{C}^\times$ be unramified outside T.
- Let $N = \prod_{p \in S} p^{\nu_p}$, $M = \prod_{p \in S} p^{\mu_p}$, $R = \prod_{p \in T} p^{\nu_p}$, where if $p|N$, then $\nu_p > \mu_p \geq 0, \nu_p \geq 2$, and A_p is $\mathcal{K}_1(p^{\nu_p})$-invariant. And if $p|R$, then $\nu_p \geq \mathfrak{c}_p(\lambda)$.
- Let $y \in \mathbb{Z}$, and define $t = 1/NR, t' = 1/MR \in \mathbf{I}_f$.

⌟

Def. (22.4.4.3) [Eisenstein Series]. For $\varphi \in \mathscr{S}(\mathbf{A}_f^2)$, define the Eisenstein series

$$E_{k,s}(\varphi)(\tau, g) = \sum_{0 \neq \underline{m} \in \mathbb{Q}^2} \frac{(g\varphi)(\underline{m})}{(m_1 + m_2\tau)^k |m_1 + m_2\tau|^{2s}}.$$

And $E_k(\varphi) = E_{k,0}(\varphi, 1)$. ⌟

Def. (22.4.4.4). Denote $\varphi = \varphi_{t,t'}, \varphi' = \varphi'_{t,t'} \in \mathscr{S}(\mathbf{A}_f^2)$ s.t. the local components are given by (22.4.4.1)

$$\begin{cases} \phi_p^0 & , p \nmid NR \\ \phi_p^{1,t_p}, (\phi_p^{1,t'_p})^{\mathrm{tr}} & , p|R \\ \phi_p^{1,t_p}, \phi_p^{2,t'_p} & , p|N \end{cases}$$

⌟

Def. (22.4.4.5) [Inner Products]. ⌟

Thm. (22.4.4.6) [Rankin-Selberg Equation]. ?

$$\langle E_{l,s}(\varphi)E_k(\varphi') \otimes \overline{\lambda}, F \rangle = \frac{i^{k-1}\Gamma(k+l+s-1)}{2^{k+2l+2s-4}(k-1)!} \cdot \frac{N^{l+2s-2}R^{k+l+2s}}{\# GL(2, \mathbb{Z}/(R))} \prod_{p|R} \lambda_p(MNt_pt'_p) \prod_{p|N} (1 - \frac{1}{p^2})^{-1}$$
$$\times L_{NR}(\pi \otimes \lambda; l+k+s-1)\Big(L_N(\pi; l+s, \frac{y}{M}) + (-1)^k \lambda(-1) L_N(\pi; l+s, -\frac{y}{M})\Big)$$

⌟

Proof: Cf. [Scholl, P446]? □

Cor. (22.4.4.7). If $k = l = 1, s = 0$, then

$$\langle E_1(\varphi)E_1(\varphi') \otimes \lambda, F \rangle = 2N^{-1} \prod_{p|N} (1 - \frac{1}{p^2})^{-1} \cdot \frac{R^2}{\# GL(2, \mathbb{Z}/(R))} \prod_{p|R} \lambda_p(MNt_pt'_p)^{-1}$$
$$\times L_{NR}(\pi \otimes \lambda; 1)\Big(L_N(\pi; 1, \frac{y}{M}) - \lambda(-1) L_N(\pi; 1, -\frac{y}{M})\Big)$$

⌟

5 Euler System for Elliptic Curves(Kato)

Notation (22.4.5.1).

- Fix $p \in \mathbf{P}$.
- Fix $N \in \mathbb{Z}_+$ not divisible by p, and fix $d, d' \in \mathbb{Z}_{\geq 2}$ prime to $6Np$.
- Denote
$$\mathcal{R}'_p = \mathcal{R}(Npdd'), \quad \mathcal{R}_p = \mathcal{R}'_p \times p^{\mathbb{Z}_+}.$$

⌟

General Procedure to produce Euler system for Modular Curves

Def. (22.4.5.2) [Setup]. Suppose for each $r \in \mathcal{R}_p$, there are points $z_r, z'_r \in \mathcal{E}^{\mathrm{uni}}(Y(Nr)) \cong (\mathbb{Z}/(Nr))^2$ satisfying:

- If $r, rs \in \mathcal{R}_p$, then $sz_{rs} = z_r, sz'_{rs} = z'_r$. So we have inverse limits
$$(z_r)_r, (z'_r)_r \in \varprojlim_{r \in \mathcal{R}_p} \mathcal{E}^{\mathrm{uni}}[Nr] \cong \mathbb{Z}_p^2 \times \prod_{\ell \nmid NpDD'} \mathbb{Z}/(\ell).$$
In particular, there exists $e \in \mathbb{Z}_p^*$ s.t. if $r = r_0 p^m \in \mathcal{R}_p$, the Weil pairing
$$e_{Nr}(z_r, z'_r) = \zeta_{p^m}^{er_0^{-1}} \times (\text{prime to } p \text{ roots of } 1).?$$
- for any $r \in \mathcal{R}_p$, the points Nz_r, Nz'_r generate $\mathcal{E}^{\mathrm{uni}}[r]$.
- If $r = p^m$, then the orders of z_r, z'_r are not powers of p.

⌟

Prop. (22.4.5.3). By(22.4.1.2), item3 in the setup(22.4.5.2) ensures that z_r, z'_r doesn't meet the zero section of $\mathcal{E}^{\mathrm{uni}}/Y(Nr)$ in any characteristic. So $\vartheta_d(z_r), \vartheta_d(z'_r)$ actually belongs to $\mathcal{O}^*(Y(Nr))$.

Thus for $r \in \mathcal{R}_p$ we can define
$$\widetilde{\sigma}_r = \{\vartheta_d(z_r), \vartheta_d(z'_r)\} \in K_2(Y(Nr)),$$
$$\sigma_r = \mathrm{Nm}_{Y(Nr)/Y(N)\otimes\mathbb{Q}(\mu_r)} \widetilde{\sigma}_r \in K_2(Y(N) \otimes \mathbb{Q}(\mu_r)).$$
Then they satisfy:

- For $r \in \mathcal{R}_p$, $\mathrm{Nm}_{\mathbb{Q}(\mu_{rp})/\mathbb{Q}(\mu_r)} \sigma_{rp} = \sigma_r$.
- If $\ell \in \mathbf{P}, r, r\ell \in \mathcal{R}_p$, then
$$\mathrm{Nm}_{\mathbb{Q}(\mu_{r\ell})/\mathbb{Q}(\mu_r)} \sigma_{r\ell} = (1 - T_\ell \langle \ell \rangle_* \otimes \mathrm{Frob}_\ell^{-1} + \ell \langle \ell \rangle_* \otimes \mathrm{Frob}_\ell^{-2})\sigma_r.$$

⌟

Proof: If $\ell \nmid Nr$, then
$$\mathrm{Nm}_{Y(Nr)/Y(N)_{\mathbb{Q}(\mu_r)}} \circ T_{\ell, Y(Nr)} = (T_{\ell, Y(N)} \otimes \mathrm{Frob}_\ell) \circ \mathrm{Nm}_{Y(Nr)/Y(N)_{\mathbb{Q}(\mu_r)}},$$
$$\mathrm{Nm}_{Y(Nr)/Y(N)_{\mathbb{Q}(\mu_r)}} \circ \langle \ell \rangle_{Y(Nr)*} = (\langle \ell \rangle_{Y(Nr)*} \otimes \mathrm{Frob}_\ell^{-2}) \circ \mathrm{Nm}_{Y(Nr)/Y(N)_{\mathbb{Q}(\mu_r)}},$$
because T_ℓ acts on the constant fields by Frob_ℓ, and $\langle \ell \rangle_*$ acts by Frob_ℓ^{-2}. So the theorem follows from □

Def. (22.4.5.4). Denote $\mathbb{T}_{p,N} = H^1(\overline{Y(N)}, \mathbb{Z}_p(1))$, then for $r = r_0 p^m \in \mathcal{R}_p$, there are homomorphisms

$$\begin{array}{c} \varprojlim_{n\geq m} K_2(Y(N)_{\mathbb{Q}(\mu_{r_0p^n})}) \otimes \mu_{p^n}^{-1} \\ \downarrow \text{AJ} \\ \varprojlim_{n\geq m} H^1(\mathbb{Q}(\mu_{r_0p^n}), H^1(Y(N)_{\overline{\mathbb{Q}}}, \mu_{p^n})) \\ \downarrow \text{cor} \\ \varprojlim_{n\geq m} H^1(\mathbb{Q}(\mu_{r_0p^m}), H^1(Y(N)_{\overline{\mathbb{Q}}}, \mu_{p^n})) \\ \| \\ H^1(\mathbb{Q}(\mu_r), \mathbb{T}_{p,N}) \end{array}.$$

By(22.4.5.3), the family $\{\sigma_{r_0p^n} \otimes [\zeta_{p^n}]^{-1}, n \geq m\}$is an element of the first group above, so we get elements

$$\xi_r = \xi_r(Y(N); p, d, d', z, z') \in H^1(\mathbb{Q}(\mu_r), \mathbb{T}_{p,N})$$

And they satisfy:

- For each $r \in \mathcal{R}_p$, $\operatorname{cor}_{\mathbb{Q}(\mu_{rp})/\mathbb{Q}(\mu_r)} \xi_{rp} = \xi_r$.
- If $\ell \in \mathbf{P}, r, r\ell \in \mathcal{R}_p$, then

$$\operatorname{cor}_{\mathbb{Q}(\mu_{r\ell})/\mathbb{Q}(\mu_r)} \xi_{r\ell} = (1 - \ell^{-1} T_\ell \langle \ell \rangle_* \operatorname{Frob}_\ell^{-1} + \ell^{-1} \langle \ell \rangle_* \operatorname{Frob}_\ell^{-2}) \xi_r.$$

⌟

Proof: The operators T_ℓ and $\langle \ell \rangle$ acts functorially on the cohomology groups, and Frob_ℓ acts as ℓ on μ_{p^n}, so by the twisting, we get the desired formula. □

Prop. (22.4.5.5). For any $N \in \mathbb{Z}_{\geq 3}$, in $\Omega_{Y(N)^{\mathrm{ord}}/\mathbb{Z}} \cong \Omega^1_{Y(N)^{\mathrm{ord}}/\mathbb{Z}[\mu_N]} \otimes \Omega^1_{Z[\mu_N]/\mathbb{Z}}$,

$$\operatorname{dlog}\{\vartheta_d(z), \vartheta_{d'}(z')\} = \frac{1}{N} \mathrm{KS}_{Y(N)}({}_d \operatorname{Eis}(z) \cdot {}_{d'} \operatorname{Eis}(z')) \otimes \mathrm{d} \log e_N(z, z').$$

⌟

Proof: By q-expansion principle, it suffices to check this at cusps. If $z = \zeta_N^{a_1} q^{a_2/N}, z' = \zeta_N^{b_1} q^{b_2/N}$, then $e_N(z, z') = \zeta_N^{a_2b_1 - a_1b_2}$, and $\Omega^1_{Z[\mu_N]/\mathbb{Z}}$ is generated by $\operatorname{dlog}(\zeta_N)$ and killed by N, so the assertion follows immediately from the description of KS(20.2.5.4) and(22.4.1.6). □

Prop. (22.4.5.6). For any $r = r_0 p^m \in \mathcal{R}_p$, define

$$\widetilde{\omega_r} = \frac{1}{Nr} \mathrm{KS}_{Y(Nr)}({}_d \operatorname{Eis}(z_r) \cdot {}_d \operatorname{Eis}(z'_r)) \in H^0(X(Nr), \Omega^1(\log \mathrm{cusp})),$$

$$\omega_r = \operatorname{tr}_{X(Nr)/X(N)_{\mathbb{Q}(\mu_r)}} \in H^0(X(N)_{\mathbb{Q}(\mu_r)}, \Omega^1(\log \mathrm{cusp})).$$

Then

$$\exp_p^* \xi_r = \frac{e}{r} \omega_r \text{(22.4.5.2)(22.4.5.4)}.$$

⌟

Proof: It follows from(22.4.5.5) that

$$\operatorname{dlog}\widetilde{\sigma}_r = \widetilde{\omega}_r \otimes \operatorname{dlog} e_{Nr}(z_r, z_r')(22.4.5.3) \in H^0(X(Nr)^{\mathrm{ord}}, \Omega_{X(Nr)/\mathbb{Z}}(\log \mathrm{cusp})),$$

so after taking p-adic completion, by(22.4.5.2),

$$\operatorname{dlog}\widetilde{\sigma}_r = \frac{e}{r_0}\widetilde{\omega}_r \otimes \operatorname{dlog}(\zeta_{p^m}) \in H^0(X(Nr)^{\mathrm{ord}}, \Omega_{X(Nr)_{\mathbb{Z}_p}/\mathbb{Z}}(\log \mathrm{cusp})).$$

Taking traces to $X(N)_{\mathbb{Q}(\mu_r)}$, and use the compatibility(10.1.4.12), then

$$\operatorname{dlog}\sigma_r = \frac{e}{r_0}\omega_r \otimes \operatorname{dlog}(\zeta_{p^m}).$$

Then it follows from Kato's explicit reciprocity law(22.4.3.7),

$$\exp_p^* \xi_r = \lim_{n\to\infty} \frac{e}{r_0 p^n} \operatorname{tr}_{\mathbb{Z}_p[\mu_{p^n}]/\mathbb{Z}_p[\mu_{p^m}]}(\omega_{r_0 p^n}).$$

But by(22.4.2.3),

$$\operatorname{tr}_{Y(Nr_0p^n)/Y(Nr_0p^m)} \widetilde{\omega}_{r_0p^n} = p^{n-m}\widetilde{\omega}_{r_0p^m},$$

so

$$\operatorname{tr}_{\mathbb{Z}_p[\mu_{p^n}]/\mathbb{Z}_p[\mu_{p^m}]}(\omega_{r_0p^n}) = p^{n-m}\omega_r,$$

which implies the desired equation. □

Elliptic Curves

Def. (22.4.5.7) [Setup].

- Suppose $E \in \mathcal{E}\mathrm{ll}/\mathbb{Q}$ has with conductor N_E and a Weil parametrization $\varphi_E : X_0(N_E) \to E$.
- Let ω_E be a differential on $E/\mathbb{Q}$ s.t. $\varphi_E^*\omega_E$ is a newform on $X_0(N_E)$.?
- Let Ω_E^+, Ω_E^- be the real and imaginary periods of ω_E.?
- Let $N \in \mathbb{Z}_+, N_E|N$, and $p \in \mathbf{P}$ be prime to $2N$.

⌟

Prop. (22.4.5.8). Situation as in(22.4.5.7), there are maps

$$f : H^1(X(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1)) \to H^1(Y(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1)) = \mathbb{T}_{p,N}$$

and

$$H^1(X(N)_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1)) \xrightarrow{\varphi_{E,N*}} H^1(E_{\overline{\mathbb{Q}}}, \mathbb{Z}_p(1)) = T_p(E).$$

By the proof of the Manin-Drinfeld theorem?, there is an idempotent Π_N^{cusp} in the Hecke algebra with rational coefficients s.t. for any p, it induces a left inverse to f as above. Thus for some $h_E \in \mathbb{Z}_+$ independent of p, we can define a map

$$h_E\varphi_{E,N*} \circ \Pi_{N,*}^{\mathrm{cusp}} : \mathbb{T}_{p,N} \to T_p(E).$$

⌟

Prop. (22.4.5.9) [Associated Euler System for Elliptic Curves]. For $r \in \mathcal{R}_p$(22.4.5.2), define

$$\xi_r(E) = (h_E\varphi_{E,N*} \circ \Pi_{N*}^{\text{cusp}})\xi_r(Y(N)) \in H^1(\mathbb{Q}(\mu_r), T_p(E))(22.4.5.4),$$

then $\{\xi_r(E)\}_r$ is an Euler system for $(T_p(E), \mathcal{K}, Ndd'r)$(22.1.3.2). ⌟

Proof: This follows from(22.4.5.4) and the fact $\langle \ell \rangle = 1, T_\ell = a_\ell$ on $T_p(E)$ for $\ell \in \mathbf{P} \cap \mathcal{R}_p$ by definition and the fact $f_E \in S_2(\Gamma_0(N))$.? □

Prop. (22.4.5.10). On differentials, Π_N^{cusp} is identity on cusp forms and annihilates Eisenstein forms?. Denote

$$\omega_r^{\text{cusp}} = \Pi_N^{\text{cusp}}(\omega_r) \in H^0(X(N)_{\mathbb{Q}(\mu_r)}, \Omega^1).$$

Then it follows from(22.4.5.6) and the functoriality of $\exp_p^*$ that

$$\exp_p^* \xi_r(E) = \frac{eh_E}{r}\varphi_{E,N*}(\omega_r^{\text{cusp}})(22.4.5.8).$$

⌟

The Calculation

Notation (22.4.5.11).

- Use the setup(22.4.4.2), where M, N is defined in(22.4.5.12),$R = r = r_0 p^m$ is any number in $\mathcal{R}_p$, and $\lambda : \mathbf{I}_f / \mathbb{Q}_+^\times \to \mathbb{C}^\times$ is a character with conductor dividing r.
- In particular, by(22.4.4.2)(22.4.4.4), there are elements $t, t' \in \mathbf{I}_f$, and $\varphi, \varphi' \in \mathscr{S}(\mathbf{A}_f^2)$.
- Let $\varepsilon = \lambda(-1) \in \{\pm 1\}$.
- Fix $d, d' \in \mathbb{Z}_{\geq 2}$ with $(dd', 6pN_E) = 1$, $d \equiv d' \equiv 1 (\text{mod } M)$.
- Denote
$$\delta \in \mathbf{I}_f : \delta_p = \begin{cases} d & , p | Nr \\ 1 & , \text{otherwise} \end{cases}, \quad {}_d\varphi = d^2\varphi - d[\delta]\varphi,$$
and similarly define δ' and ${}_{d'}\varphi'$.

⌟

Prop. (22.4.5.12). For any $\alpha \in \mathbb{Q}$,

$$L_{MN_E}(E, 1; \alpha) - \varepsilon L_{MN_E}(E, 1; -\alpha)$$

is a rational multiple of $\Omega_E^{-\varepsilon}$, and one can find α with denominator prime to any integer for which the expression is non-zero, by [Shimura, On the periods of modular forms]?.

Then we can find y/M.?Cf.[Scholl, P454].

And also define

$$N = \prod_{p | MN_E} p^{\nu_p}, \quad \nu_p = \max(2, v_p(N_E), v_p(M) + 1).$$

⌟

Prop. (22.4.5.13) [The function φ]. Choose $z_r \in \mathcal{E}^{\mathrm{uni}}(Y(Nr))$ to be the point which in complex coordinates is

$$\frac{1}{Nr} \in (\frac{1}{Nr}\mathbb{Z} + \frac{\tau}{Nr}\mathbb{Z})/(\mathbb{Z}+\tau\mathbb{Z}) \cong (\mathbb{Z}/(Nr))^2.$$

Then for $\ell \in \mathbf{P}, r, r\ell \in \mathcal{R}_p$, $\ell z_{r\ell} = z_r$, and

$$_d\operatorname{Eis}(z_r) = E_1(_d\varphi)\mathrm{d}u.$$

⌟

Proof: **?** Calculate using(22.4.4.3) and(22.4.1.5) and the definition of φ(22.4.4.4). □

Prop. (22.4.5.14) [The function φ']. There exists f.m. constants $b_j \in N^{-1}\mathbb{Z}$ independent of r and points $z'_{r,j} \in \mathcal{E}^{\mathrm{uni}}(Y(Nr))$, s.t.

$$\sum_j b_j \cdot {}_{d'}\operatorname{Eis}(z'_{r,j}) = E_1(_{d'}\varphi')\mathrm{d}u.$$

Moreover, for $\ell \in \mathbf{P}, r, r\ell \in \mathcal{R}_p$, $\ell z_{r\ell,j} = z_{r,j}$, and $z'_{r,j} - z'_{r,i}$ are N-torsion. And in complex coordinates,

$$Nz'_{r,j} = (-Nt'(\mathrm{mod}\ \widehat{\mathbb{Z}}))\tau \in (\frac{1}{r}\mathbb{Z} + \frac{1}{r}\tau)/(\mathbb{Z}+\tau\mathbb{Z}) \cong (\mathbb{Z}/(r))^2.$$

So

$$e_{Nr}(z_r, z'_{r,j}) = \zeta_{p^m}^{-(Mr_0)^{-1}} \times (\text{prime to } p \text{ roots of } 1),$$

so $e_{z,z'_j} = -M^{-1}$(22.4.5.2). ⌟

Proof: Cf.[Scholl, P456]**?**. □

Thm. (22.4.5.15)[Final Construction and Calculation]. Let $\xi_{r,j}(E)$ be the Euler system for $T_p(E)$ associated to $(z_r, z_{r,j})$(22.4.5.9) in the setup(22.4.5.7), then define a new Euler system

$$c_r = \sum_j b_j \xi_{r,j}(E) \in H^1(\mathbb{Q}(\mu_r), T_p(E)).$$

Then this Euler system satisfies the requirement of(22.4.5.16). ⌟

Proof: Let $\widetilde{\omega}_{r,j}$ be the differential associated to $(z_r, z_{r,j})$(22.4.5.6), then because the Kodaira-Spencer map takes $(\mathrm{d}\log t)^2$ to $\mathrm{d}\log q$, so it takes $\mathrm{d}u^2$ to $(2\pi\,\mathrm{i})^{-1}\mathrm{d}\tau$. Thus

$$\sum_j b_j\widetilde{\omega}_{r,j} = \frac{(2\pi\,\mathrm{i})^{-1}}{Nr}E_1(_d\varphi)E_1(_{d'}\varphi')\mathrm{d}\tau.$$

Then for any character $\lambda : \operatorname{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q}) \cong (\mathbb{Z}/(r))^* \to \mathbb{C}^\times$,

$$\sum_{\gamma\in\operatorname{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q})} \lambda(\gamma)\exp_p^* c_r^\gamma = \sum_j b_j \sum_{\gamma\in\operatorname{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q})} \lambda(\gamma)\exp_p^*\xi_{r,j}(E)^\gamma$$

$$\text{(22.4.5.10)} = \sum_j b_j \sum_{x\in(\mathbb{Z}/(r))^*} \lambda(x)\frac{-M^{-1}h_E}{r}\iota_x\varphi_{E,N*}(\omega_{r,j}^{\mathrm{cusp}})$$

where $\iota_x : \mathbb{Q}(\mu_r) \hookrightarrow \mathbb{C}$ is the injection that maps ζ_r to $e^{2\pi \mathrm{i}\, x/r}$. Then it equals

$$\begin{aligned}
&\frac{-M^{-1}h_E}{r}\sum_j b_j \frac{\int_{E^{\mathrm{an}}}\sum_{x\in(\mathbb{Z}/(r))^*}\lambda(x)\iota_x\varphi_{E,N*}(\omega^{\mathrm{cusp}}_{r,j})\wedge\overline{\omega}_E}{\int_{E^{\mathrm{an}}}\omega_E\wedge\overline{\omega}_E}\omega_E\\
&=\frac{-h_E}{Mr\Omega_E^+\Omega_E^-}\Big(\sum_j b_j\int_{Y(N)^{\mathrm{an}}\times(\mathbb{Z}/(r))^*}\lambda(x)\iota_x\omega^{\mathrm{cusp}}_{r,j}\wedge\varphi^*_{E,N}\overline{\omega}_E\Big)\omega_E\\
&=\frac{-h_E}{Mr\Omega_E^+\Omega_E^-}\Big(\sum_j b_j\int_{Y(N)^{\mathrm{an}}\times(\mathbb{Z}/(r))^*}\lambda(x)\iota_x\omega_{r,j}\wedge\varphi^*_{E,N}\overline{\omega}_E\Big)\omega_E\\
&=\frac{-h_E}{Mr\Omega_E^+\Omega_E^-}\Big(\sum_j b_j\int_{Y(Nr)}(\lambda\circ e_{Nr})\widetilde{\omega}_r\wedge\varphi^*_{E,N}\overline{\omega}_E\Big)\omega_E\\
?&=\frac{-h_E\#\,\mathrm{GL}(2,\mathbb{Z}/(Nr))}{MNr^2\Omega_E^+\Omega_E^-}\langle E_1({}_d\varphi)E_1({}_{d'}\varphi')\otimes\lambda, F\rangle\omega_E
\end{aligned}$$

where $e_{Nr} : Y_{Nr}(\mathbb{C}) \to \mu_N(\mathbb{C})$ is the Weil pairing.

Using(22.4.4.7) and the facts $\mathfrak{c}(\lambda)|r$ and $d \equiv d' \equiv 1(\mathrm{mod}\ \ M)$, it equals?

$$\frac{C_{E,M}}{\Omega_E^+\Omega_E^-}DD'(D-\chi^{-1}(D))(D'-\chi^{-1}(D'))L_{rMN_E}(E,\chi;1)\Big(L_{MN_E}(\pi;1,\frac{y}{M})-\lambda(-1)L_{MN_E}(\pi;1,-\frac{y}{M})\Big)\omega_E$$

Where $C_{E,M}$ only depends on E and M.(Notice N only depends on E and M(22.4.5.12)).

Then by the choice of y/M(22.4.5.12), depending on $\lambda(-1) = \pm 1$, it equals

$$C^{\pm}_{E,M}DD'(D-\chi^{-1}(D))(D'-\chi^{-1}(D'))\frac{L_{rMN_E}(E,\chi;1)}{\Omega_E^{\pm}}\omega_E,$$

where $C^{\pm}_{E,M}$ only depends on E and M. □

Conclusions

Thm. (22.4.5.16) [Kato]. Situation as in(22.4.5.7), then there exists $M \in \mathbb{Z}_+$ prime to p s.t. for any $d, d' \in \mathbb{Z}_{\geq 2}$ with $(dd', 6pN_E) = 1$, $M|d-1, M|d'-1$, there is an Euler system

$$\overline{\mathbf{c}} = \{\overline{\mathbf{c}}_r(E,p,d,d') \in H^1(\mathbb{Q}(\mu_r), T_p(E)), \quad r = r_0p^m, m \geq 1, r_0 \in \mathcal{R}(pMN_E)\}.$$

satisfying: For any $r \in \mathcal{R}_p$ and $\chi : \mathrm{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q}) \cong (\mathbb{Z}/(r))^* \to \mathbb{C}^*$, with $\chi(-1) = \pm 1$,

$$\sum_{\gamma\in\mathrm{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q})}\chi(\gamma)\exp_p^*\overline{\mathbf{c}}_r^{\gamma} = C_E^{\pm}DD'(D-\chi^{-1}(D))(D'-\chi^{-1}(D'))L_{rMN_E}(E,\chi;1)/\Omega_E^{\pm}.$$

⌟

Proof: This follows from(22.4.5.15). □

22.5 Iwasawa Theory for Elliptic Curves

References are [Coates] and [Greenberg].

1 Mazur's Control Theorem

Thm. (22.5.1.1) [Mazur's Control Theorem]. Suppose $p \in$,$F \in$ `NField` and $F_\infty = \cup_{n\in\mathbb{N}} F_n$ is an $\mathbb{Z}_p$-extension, $E \in \mathcal{E}\mathrm{ll}/F$ has good ordinary reduction at all primes over p, then for $n \in \mathbb{N}$, then the natural maps

$$\mathrm{Sel}^{p^\infty}(E/F_n) \to \mathrm{Sel}^{p^\infty}(E/F_\infty)^{\mathrm{Gal}(F_\infty/F_n)}$$

has kernels and cokernels of bounded orders as $n \to \infty$. ⌟

Proof: □

23 Kudla's Program

23.1 Kudla's Program

1 Modularity Conjecture

Siegel Modular Forms

Modularity Conjecture

Thm. (23.1.1.1) [Modularity Conjecture, Kudla]. ⌟

Remark (23.1.1.2). This theorem is proven by [Gross-Kohen-Zagier1987] for modular curves, and [Hirzebruch-Zagier1976] for Hilbert modular surfaces, and [Borcherds1999] for Shimura varieties of orthogonal type. ⌟

Proof: □

W. Zhang's Work

References are [Wei Zhang's thesis].

23.2 Arithmetic Siegel-Weil Formula

References are [ChaoLi's notes].

1 Represented by Quadratic Forms

Thm. (23.2.1.1) [Jacobi]. For $n \in \mathbb{Z}_+$, let $r(n) = \#\{(x,y) \in \mathbb{Z} | x^2 + y^2 = n\}$, then $r(n) \neq 0$ iff $2 | v_p(n)$ for any $p \equiv 3 (\mathrm{mod}\ 4)$.

Moreover,

$$r(n) = 4\Big(\#\{d \in \mathbb{Z}_+, d|n, d \equiv 1 (\mathrm{mod}\ 4)\} - \#\{d \in \mathbb{Z}_+, d|n, d \equiv 3 (\mathrm{mod}\ 4)\}\Big).$$

⌟

Proof: It is clear that

$$\sum_{n \in \mathbb{Z}_+} r(n) q^n = \theta^2 (20.4.1.3).$$

□

23.3 Kudla-Rapoport Conjecture

1 Global Kudla-Rapoport Conjecture

24 Computational Number Theory

24.1 Computational Number Theory

References are [Princeton Companion] and [Pi and the AGM. A study in Analytic Number theory and computational complexity].

1 Primality Testing

Algo. (24.1.1.1) [AKS Primality Proving]. Consider the following algorithm:

Input: An integer $n \in \mathbb{Z}_{\geq 2}$
Output: `PRIME` or `COMPOSITE`

1. **if** $n = a^b$ *for some* $a \in \mathbb{Z}_+, b \in \mathbb{Z}_{\geq 2}$ **then return** `COMPOSITE`;
2. `Find` the smallest number r s.t. $\mathrm{ord}_r(n) > \log^2 n$;
3. **if** $1 < \gcd(a, n) < n$ *for some* $a \leq r$ **then return** `COMPOSITE`;
4. **if** $n \leq r$ **then return** `PRIME`;
5. **for** $a \leftarrow 1$ **to** $\lfloor \sqrt{\varphi(r) \log n} \rfloor$ **do**
   if $(X + a)^n \not\equiv X^n + a (\mathrm{mod}\ \ (X^r - 1, n))$ **then return** `COMPOSITE`;
6. **return** `PRIME`;

Then for any input $n \in \mathbb{Z}_+$, this algorithm returns `PRIME` iff $n \in$ `Prime`. And its asymptotic time complexity is $\widetilde{O}(\log^{15/2} n)$.

In particular, deciding the language `Prime` $\subset \mathbb{N}$ is in the class P(2.7.4.1). ⌟

Remark (24.1.1.2) [Lenstra and Pomerance, Primality testing with gaussian periods]. has an improvement that has ⌟

Proof: To prove the algorithm is correct: Notice if n is prime, then it can only return prime. And the converse is proved in(24.1.1.3).

To analyze the asymptotic time complexity, we use [Modern Computer Algebra].

The first step of the algorithm takes asymptotic time $\widetilde{O}(\log^3 n)$.

For the second step, use(21.4.11.4). To find such an r, we check for each $r < \log^{3+\varepsilon}$ and each $k < \log^2 n$ whether $r | n^k - 1$. For each r, the complexity is $\widetilde{O}(\log^2 n \log r)$, so the asymptotic complexity is $\widetilde{O}(\log^5 n)$.

The third step takes asymptotic time $O(\log^6 n)$.

The fourth step takes asymptotic time $O(\log n)$.

In step 5, we need to verify $\lfloor\sqrt{\varphi(r)\log n}\rfloor$ equations, each equation requires $O(\log n)$ multiplications of degree r polynomials with coefficients of size $O(\log n)$. So the asymptotic time is

$$\widetilde{O}(r\log^2 n\sqrt{\varphi(r)\log n}) \le \widetilde{O}(r^{3/2}\log^3 n) \le \widetilde{O}(\log^{15/2} n).$$

Thus the total asymptotic time is $\widetilde{O}(\log^{15/2} n)$. □

Lemma (24.1.1.3). If the AKS algorithm in(24.1.1.1) returns `PRIME`, then n is a prime. ⌟

Proof: If it returns at step 4, then step3 implies that n is a prime. So we assume that it returns at step6. Since $\operatorname{ord}_r(n) > 1$, there exists $p|n$ s.t. $\operatorname{ord}_r(p) > 1$. By step3, $p > r$ and $(r, n) = 1$.

Let G be the subgroup of $(\mathbb{Z}/r)^*$ generated by n and p, with $\#G > \log^2 n$. And denote $\zeta = \zeta_{\operatorname{ord}_r(p)}$ and let $\mathcal{G}$ be the subgroup of $\mathbb{F}_p(\zeta)$ generated by $\zeta, \zeta+1, \ldots, \zeta + \lfloor\sqrt{\varphi(r)\log n}\rfloor$. Then

$$\begin{aligned}
\#\mathcal{G} &\overset{(24.1.1.4)}{\geq} \binom{\#G + \lfloor\sqrt{\varphi(r)\log n}\rfloor}{\#G - 1} \\
(\because \#G > \sqrt{\#G}\log n) &\geq \binom{\lfloor\sqrt{\varphi(r)\log n}\rfloor + 1 + \lfloor\sqrt{\#G\log n}\rfloor}{\lfloor\sqrt{\#G\log n}\rfloor} \\
&\geq \binom{2\lfloor\sqrt{\#G\log n}\rfloor + 1}{\lfloor\sqrt{\#G\log n}\rfloor} \\
(11.6.1.14) &> 2^{\lfloor\sqrt{\#G\log n}\rfloor + 1} \\
&\geq n^{\sqrt{\#G}}.
\end{aligned}$$

But then by(24.1.1.4), $n \in p^{\mathbb{Z}_+}$. So in view of step1, $n = p \in$ `Prime`. □

Lemma (24.1.1.4). Let $G, \mathcal{G}$ be the group defined in the proof of(24.1.1.3), then

$$\#\mathcal{G} \geq \binom{\#G + \sqrt{\varphi(r)\log n}}{\#G - 1}.$$

And if $n \notin p^{\mathbb{Z}_+}$, then $\#\mathcal{G} \leq n^{\sqrt{\#G}}$. ⌟

Proof: By the hypothesis, n passed step4, so any $0 \le a \le \sqrt{\varphi(r)\log n}$,

$$(X+a)^n \equiv X^n + a(\bmod\ X^r - 1, p),$$

so

$$(X+a)^{\frac{n}{p}} \equiv X^{\frac{n}{p}} + a(\bmod\ X^r - 1, p).$$

More generally, for any $m \in I = \{(\frac{n}{p})^i p^j : i, j \in \mathbb{N}\}$ and any polynomial

$$f(X) \in P = \{\prod_{a=0}^{\lfloor\sqrt{\#G\log n}\rfloor} (X+a)^{e_a} : e_a \in \mathbb{N}\},$$

we have

$$f(X)^m \equiv f(X^m)(\bmod\ X^r - 1, p).$$

Then we claim that any two polynomials in P with degree$< \#G$ will be distinct elements in $\mathbb{F}_p(\zeta)$: If $\overline{f} = \overline{g}$, then for each $m \in G$, $f(\zeta^m) \equiv g(\zeta^m)$, so f and g are equal on $\#G$ values. This forces $f \equiv g(\text{mod } p)$. But this is not possible as $i \not\equiv j(\text{mod } p)$ for $i, j \leq \lfloor\sqrt{\#G \log n}\rfloor < \sqrt{r \log n} < r < p$.

Then by combinatorics, $\#\mathcal{G} \geq \binom{\#G+\sqrt{\varphi(r)\log n}}{\#G-1}$.

For the upper bound, consider the subset $I' = \{(\frac{n}{p})^i p^j : 0 \leq i, j \leq \sqrt{\#G}\}$. If $n \notin p^{\mathbb{Z}_+}$, then $\#I' > \#G$, so there are two elements $m_1, m_2 \in I'$ s.t. $r | m_1 - m_2$. Then $f(\zeta)^{m_1} = f(\zeta^{m_1}) = f(\zeta^{m_2}) = f(\zeta)^{m_2}$ for any $f(X) \in P$. Then $f(\zeta)$ is a root of the polynomial $X^{m_1} - X^{m_2}$, which has degree$\leq n^{\sqrt{\#G}}$. In view of the fact $\mathcal{G}$ is the values of polynomials in P at ζ, we have $\#\mathcal{G} \leq n^{\sqrt{\#G}}$. □

Def. (24.1.1.5) [Elliptic Curve Primality Proving(ECPP)]. Cf.[Sutherland]L12. ⌟

2 Factorizing Integers

Algo. (24.1.2.1) [Buhler-Lenstra-Pomerance]. There is an algorithm to factor a n-bit number N in $O(e^{cn^{1/3}\log^{2/3} n})$ times. ⌟

3 Others

Remark (24.1.3.1). There are not yet a polynomial algorithm that gives for a prime $p \in \mathbf{P}$ a primitive root $a \in (\mathbb{Z}/(p))^*$. ⌟

25 Combinatorics

25.1 Combinatorics

1 Polytopes

Def. (25.1.1.1) [Polytopes]. A n-**polytope** is a compact subset of $\mathbb{R}^n$ for some $n \in \mathbb{Z}$ with boundaries given by polytopes of smaller dimensions. A **polygon** is a 2-polytope. A **polyhedron** is a 3-polytope. ⌟

Def. (25.1.1.2) [Tetrahedra]. A **tetrahedron** is an 3-simplex in $\mathbb{R}^3$. ⌟

Def. (25.1.1.3) [Orthohedra]. An **orthohedron** is a tetrahedron isomorphic to the convex hull of the four points

$$\{(0,0,0),(x,0,0),(x,y,0),(x,y,z)\} \in \mathbb{R}^3.$$

⌟

Prop. (25.1.1.4) [Dihedral Angles of Orthohedra].

- Each orthohedron has dihedral angles $(\alpha,\beta,\gamma,\pi/2,\pi/2,\pi/2)$.
- A rectangular solid can be cut into 6 orthohedra sharing a common diagonal. And for any $\alpha,\beta,\gamma \in (0,\pi), \alpha+\beta+\gamma=\pi$, there is a rectangular solid that can be cut into 6 orthohedra s.t. the dihedral angles along the diagonal are $(\alpha,\beta,\gamma,\alpha,\beta,\gamma)$.

⌟

Proof: Only 2 needs a proof, and this is verified by brutal force calculations. □

2 Hilbert's 3rd Problem

Cf.[Sch13b].

Def. (25.1.2.1) [Scissors Congruence]. A **dissection of a polytope** P is an expression $P = \cup_i^n P_i$ s.t. the interiors of P_i are disjoint.

Two polytopes P, Q are called **scissors-congruent** if there are dissections $P = \cup_i^n P_i, Q = \cup_i^n Q_i$ s.t. $P_i \cong Q_i$ for $1 \le i \le n$. Scissors congruence relations are denoted by $\sim_s$. ⌟

Thm. (25.1.2.2) [Wallace-Bolyai-Gerwien]. Any two polygons P, Q in $\mathbb{R}^2$ are scissors-congruent. ⌟

Proof: Find a line l that is not parallel to any line generated by vertices of P and Q, cut P, Q through lines parallel to l and passing through some vertices of O, Q. Then we get some trapezoids. Then we cut them into right triangles.

Now we transform any right triangle P with vertices $\{A = (-0, 0), B = (0, 2b), C = (0, c)\}$ to a triangle triangle of height 2: Now consider another right triangle with vertices $\{A = (-0, 0), X = (0, 2), Y = (0, bc)\}$. Then $BY//CX$, thus BYC and BYX are triangles of the same base and height.

Then $BYC \sim_s BYX$: cut them into parallelograms with the same base and height, then it is easy to see any two such parallelograms are scissor-congruent.

Now all the triangles has a side of length2, we can transform them into rectangles with a side of length1. Then clearly P, Q are transformed together. □

Thm. (25.1.2.3) [Zylev]. If P, A, B are polytopes, $A \subset P, B \subset P$, $P\backslash A \sim_s P\backslash B$, then $A \sim_s B$. ⌟

Proof: Let

$$F = A \coprod \coprod_{k=1}^{n} P_k = B \coprod \coprod_{k=1}^{n} Q_k, P_k \sim_s Q_k$$

We can dissect them even further s.t. $\mathrm{Vol}(P_k) < \frac{1}{2}\mathrm{Vol}(A)$. Then we use induction on n to show that $A \sim_s B$: $n = 0$ is trivial. For $n > 0$, because of the volume bound, $\mathrm{Vol}(A\backslash Q_n) > \mathrm{Vol}(Q_n)$, thus we can find disjoint $T_1, \ldots, T_n \subset A\backslash Q_n$ s.t. $T_k \sim_s P_k \cap Q_n$. Now define

$$F' = F\backslash Q, P_k' = (P_k\backslash Q_n) \cup T_k \sim_s P_k, \quad A' = F' \backslash \bigcup_{k=1}^{n-1} P_k' = (A\backslash \bigcup_{k=1}^{n-1} T_k) \bigcup_{k=1}^{n-1} Q_k$$

Then by induction, $A' \sim_s B' = B$. But $A' \sim_s A$ by changing T_k with Q_k. □

Dehn-Sydler Theorem

Prop. (25.1.2.4) [Tetrahedra]. Any polyhedron has a dissection into tetrahedra. ⌟

Proof: By choose a sufficiently small lattice dissection of $\mathbb{R}^3$, it suffices to consider three cases:

- A cube.
- A cube cut by one hypersurfaces.
- A cube cut by two hypersurfaces.
- A cube containing a single vertex.

All cases are straightforward. □

Def. (25.1.2.5) [Dehn Invariants]. For a polyhedron P, define the **Dehn invariant** of P as

$$\Delta(P) = \sum_i l_i[\alpha_i] \in \mathbb{R} \otimes (\mathbb{R}/\mathbb{Z}\pi)$$

where the sum is over all edges e_i, of P, $l_i = l(e_i)$, and α_i is the dihedral angles of e_i. ⌟

Thm. (25.1.2.6) [Dehn]. If two polyhedra in $\mathbb{R}^3$ are scissors-congruent, then they have the same volume and Dehn invariants. ⌟

Proof: The volumes are the same by the invariance properties of Lebesgue measure. To show the Dehn invariants are the same, notice the dissections of a polytope P may create new edges, but the sum of angles around a new edge is 2π for if it is contained in the interior of P, or π if it is in the surface of P. □

Def. (25.1.2.7) [Simple Prisms]. A **simple prism** is a polyhedron that is isomorphic to an affine translate of $T \times I \subset \mathbb{R}^2 \times \mathbb{R}$, where $T \subset \mathbb{R}^2$ is a triangle. ⌟

Prop. (25.1.2.8). A simple prism P is scissors-congruent to $[0,1]^2 \times [0, \mathrm{Vol}(P)]$. ⌟

Proof: Place the three edges P_1Q_1, P_2Q_1, P_3Q_3 that is the image of Vertices$(T) \times I$ vertically, and they have length l. Then we can talk about the **heights** of P_i, Q_i. Suppose $h(P_1) \geq h(P_2) \geq h(P_3)$. If $h(P_3) \geq h(Q_1)$, then we can cut P along height $h(Q_1)$ make P scissors-congruent to a perfect simple prism $P' = T' \times I'$. If $h(P_3) < h(Q_1)$, then we can cut P along the plane $P_2P_3Q_1$ to make $P \sim_s P'$, where for P', $h(P_3') - h(Q_1')$ is larger. And if this process goes on, every 2 transform makes $h(P_3) - h(Q_1)$ bigger by at least l, so eventually $h(P_3) \geq h(Q_1)$, and we can transform it to a perfect simple prism.

Now if $P = T \times I$ is a perfect simple prism, (25.1.2.2) shows T is scissors equivalent to $[0,1] \times [0, \mathrm{Vol}(T)]$, and then it suffices to show $[0, \mathrm{Vol}(T)] \times I$ is scissors equivalent to $[0, \mathrm{Vol}(P)]$, which is by(25.1.2.2) again. □

Def. (25.1.2.9) [pseudo-prisms]. A **pseudo-prisms** is a convex polyhedra $(OPQRS)$, where

- OPQ is is an isosceles with $OP = PQ$,
- PR, QS is orthogonal to the plane OPQ,
- $l(QS) = 2l(PR)$.

Notice a pseudo-prism $(OPQRS)$ is scissors-congruent to the perfect simple prism $OPQ \times PR$. ⌟

Def. (25.1.2.10). Denote

- $\mathcal{P}$ the free Abelian group generated by isomorphism classes of all polyhedra.
- $\mathcal{E}$ the subgroup of $\mathcal{P}$ generated by the dissection relations.
- $\mathcal{F}$ is the subgroup of $\mathcal{P}$ generated by $\mathcal{E}$ and all the simple prisms(25.1.2.7).
- $\mathcal{V} = \mathcal{P}/\mathcal{F}$.

Then clearly two polyhedra P, Q are scissors-congruent iff $[P] = [Q] \in \mathcal{P}/\mathcal{E}$. ⌟

Prop. (25.1.2.11)[$\mathbb{R}$-Structures]. $\mathbb{R}$ acts on the set of polyhedra by scaling, and this action is additive and multiplicative, and stablizes $\mathcal{F}$, thus inducing an $\mathbb{R}$-structure on $\mathcal{V}$. ⌟

Proof: By(25.1.2.4), $\mathcal{P}$ is generated by tetrahedra. So it suffices to show that for $\lambda_1, \lambda_2 \in \mathbb{R}_+$ and a tetrahedron T, $[\lambda_1 T] + [\lambda_2 T] - [(\lambda_1 + \lambda_2)T] \in \mathcal{F}$. For this, use geometry, notice $(\lambda_1 + \lambda_2)T \backslash (\lambda_1 T \cup \lambda_2 T)$ consists of two simple prisms, where these two smaller tetrahedra aligned along an edge of T. □

Prop. (25.1.2.12) [Orthohedra]. $\mathcal{V}$ is generated by orthohedra(25.1.1.3). ⌟

Proof: By(25.1.2.4), it suffices to show that for any tetrahedron T, $[T]$ is a linear combinations of orthohedra. For this, take the center I of the inscribed circle of T, and take its projections I_1, I_2, I_3, I_4 to the faces of T, then they form 24 orthohedra(may be degenerate ones). Thus T is a linear combinations of those non-degenerate orthohedra. □

Prop. (25.1.2.13). A simple primes P has Dehn invariant $\Delta(P) = 0$(25.1.2.14) and(25.1.2.8), so by(25.1.2.8) again, Δ factors through $\Delta : \mathcal{V} \to \mathbb{R} \otimes (\mathbb{R}/\mathbb{Z}\pi)$, which is $\mathbb{R}$-linear with $\mathbb{R}$-structure on $\mathcal{V}$ given in(25.1.2.11). ⌟

Thm. (25.1.2.14) [Dehn-Sydler]. Two polyhedra in $\mathbb{R}^3$ are scissors-congruent iff they have the same volume and Dehn invariants. ⌟

Proof: One direction is shown in(25.1.2.6). For the other, it suffices to show this map $\Delta : \mathcal{V} = \mathcal{P}/\mathcal{F} \to \mathbb{R}\otimes(\mathbb{R}/\mathbb{Z}\pi)$(25.1.2.13) is injective, because in this way, if two polyhedra has the same volume and Dehn invariants, then they are scissors equivalent to two prisms with the same volume, hence scissors-congruent, by(25.1.2.8).

Take a good function $\varphi : \mathbb{R} \to \mathcal{V}$(25.1.2.24). φ vanishes on $\mathbb{Z}\pi$, thus extends to an $\mathbb{R}$-linear map $\Phi : \mathbb{R} \otimes (\mathbb{R}/\mathbb{Z}\pi) \to \mathcal{V}$, and for an orthohedron T, $\Phi(\Delta([T])) = [T]$ by(25.1.2.15), and orthohedra generate $\mathcal{V}$ by(25.1.2.12), so $\Phi \circ \Delta = \mathrm{id}_{\mathcal{V}}$. Thus Δ is injective. □

Homological Arguments

Def. (25.1.2.15) [Good Functions]. A map $\varphi : \mathbb{R} \to \mathcal{V}$ is called a **good function** if
- φ is additive and $\varphi(\pi) = 0$.
- For any orthohedron T, $[T] = \sum_{i=1}^{6} l_i\varphi(\alpha_i)$, where the notation is the same as in(25.1.2.5).

⌟

Def. (25.1.2.16) [$T(a, b)$]. For $a, b \in (0, 1)$, define $a' = \sqrt{a^{-1} - 1}, b' = \sqrt{b^{-1} - 1}$, and define $T(a, b)$ to be the orthohedron with vertices

$$\{(0, 0, 0), (a', 0, 0), (a', a'b', 0), (a', a'b', b')\} \in \mathbb{R}^3.$$

Notice $T(a, b) \cong T(b, a)$.

The order of the vertices is also important. It is always assumed to be written in this order. ⌟

Prop. (25.1.2.17). For $\alpha, \beta \in \mathbb{R}$, $T(\sin^2(\alpha), \sin^2(\beta))$ has three edges with dihedral angle $\pi/2$, and three edges with lengths $\cot(\alpha), \cot(\beta), \cot(\gamma)$ and dihedral angles $(\alpha, \beta, \pi/2 - \gamma)$ resp., where $\sin^2(\gamma) = ab, \gamma \in (0, \pi/2)$. In particular,

$$\Delta(T(\sin^2(\alpha), \sin^2(\beta))) = \cot(\alpha) \otimes \alpha + \cot(\beta) \otimes \beta + \cot(\gamma) \otimes (\pi/2 - \gamma).$$

⌟

Proof: Brutal force calculation. □

Prop. (25.1.2.18). For $a, b, c \in \mathbb{R}_+$,

$$a[T(\frac{a+b}{a+b+c}, \frac{a}{a+b})] + b[T(\frac{a+b}{a+b+c}, \frac{b}{a+b})] = a[T(\frac{a+c}{a+b+c}, \frac{a}{a+c})] + c[T(\frac{a+c}{a+b+c}, \frac{c}{a+c})]$$

⌟

Proof: This follows from the different ways of cutting the tetrahedron with vertices

$$\{O = (0, 0, 0), X = (\sqrt{bc}, 0, 0), Y = (0, \sqrt{ac}, 0), Z = (0, 0, \sqrt{ab})\} \in \mathbb{R}^3.$$

In fact, for this tetrahedron, the plane orthogonal to YZ passing through X cut this to two orthohedra, and similar does the plane orthogonal to XZ passing through Y. These two cutting give the assertion above. □

Def. (25.1.2.19) [Homological Functions]. A **homological function** is a function $h : (0, 1) \to \mathcal{V}$ s.t.
- For $a, b \in (0, 1), [T(a, b)] = h(a) + h(b) - h(ab)$.

- If $a, b \in (0,1), a+b=1$, then $ah(a)+bh(b)=0$.

⌟

Prop. (25.1.2.20). For $V \in \mathcal{V}\mathrm{ect}/\mathbb{R}$, if $g : \mathbb{R}_+ \to V$, define $\delta(g)(a,b) = g(a)+g(b)-g(ab)$. And if $F : \mathbb{R}_+^2 \to V$, define $\delta(F)(a,b,c) = F(a,b) - F(a,c) + F(ab,c) - F(ac,b)$.

Then if $F : (0,1) \to V$ is symmetric and $\delta(F) = 0$, then $F = \delta(f)$ for some $f : (0,1) \to V$. ⌟

Proof: Cf.[Sch13b]. □

Prop. (25.1.2.21). Let $G : \mathbb{R}_+^2 \to V$ be a symmetric function satisfying

- $G(\lambda a, \lambda b) = \lambda G(a,b), \lambda, a, b \in \mathbb{R}_+$,
- $G(a,b) + G(a+b,c) = G(a,c) + G(a+c,b)$.

Then there exists a homomorphism $g : \mathbb{R}_+^\times \to V$ s.t. when $a+b=1$,

$$G(a,b) = ag(a) + bg(b).$$

⌟

Proof: Cf.[Sch13b]. □

Prop. (25.1.2.22)[Sydler]. Let $F : (0,1)^2 \to \mathcal{V} : (a,b) \mapsto [T(a,b)]$, then F is symmetric, and $\delta(F) = 0$. ⌟

Proof: We check that $[T(a,b)] + [T(ab,c)] = [T(a,c)] + [T(ac,b)]$. This is done by geometry:

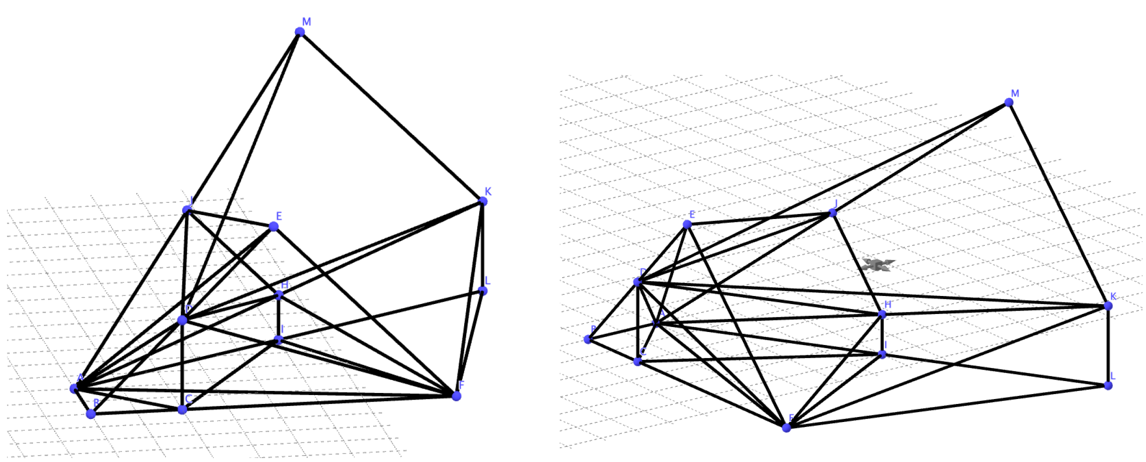
Put $T(a,b), T(a,c)$ together: $T(a,b) \cong ABCD, T(a,c) \cong ABEF$, where BDE is collinear. Let H be the center of the sphere S passing through $ACDEF$, and the projection of H on the planes ABC, ABD is denoted by I, J resp. Let K, L, M be the intersection of AH, AI, AJ with the sphere S resp.

Then it can be verified that $T(ab,c) \cong ANMK, T(ac,b) \cong AFLK$. Let $P = ABDFHI + ADHJ$, then

$$P - (AICHD) - (FICHD) + (DJMHK) = T(a,b) + T(ab,c).$$

$$P + (DJEHF) - (AJEHF) + (FILHK) = T(a,c) + T(ac,b).$$

□



Cor. (25.1.2.23). Homological functions(25.1.2.19) exist. ⌟

Proof: By(25.1.2.20), there exists $f : (0,1) \to \mathcal{V}$ s.t. $F(a,b) = [T(a,b)] = f(a) + f(b) - f(ab)$. Then we want to find $h = f - g$, where $g : (0,1) \to \mathcal{V}$ is a homomorphism s.t. when $a + b = 1$, $ah(a) + bh(b) = 1$, which is equivalent to

$$ag(a) + bg(b) = af(a) + bf(b).$$

Let

$$G : \mathbb{R}_+^2 \to \mathcal{V} : (a,b) \mapsto af(\frac{a}{a+b}) + bf(\frac{b}{a+b}),$$

then $G(\lambda a, \lambda b) = \lambda G(a,b), \lambda, a, b \in \mathbb{R}_+$, and $G(a,b) + G(a+b,c) = G(a,c) + G(a+c,b)$. In fact, this boils down to(25.1.2.18). Thus by(25.1.2.21), we truly can find such a function g. □

Prop. (25.1.2.24). Good functions(25.1.2.15) exist. ⌟

Proof: Take a homological function h(25.1.2.23), define $\varphi : \mathbb{R} \to \mathcal{V}$:

$$\varphi(\frac{n\pi}{2}) = 0, \quad n \in \mathbb{Z}, \quad \varphi(\alpha) = \tan(\alpha)h(\sin^2(\alpha)).$$

We show this is a good function:

Firstly we show:

Lemma (25.1.2.25). $\varphi(\pi/2 - \alpha) = -\varphi(\alpha), \varphi(\alpha + \pi/2) = \varphi(\alpha)$. ⌟

Proof: If $\alpha = n\pi/2$, the assertion holds. So we assume $\alpha \neq n\pi/2$ and let $\beta = \pi/2 - \alpha, a = \sin^2(\alpha), b = \sin^2(\beta)$, then $a + b = 1$, so by definition(25.1.2.19),

$$\begin{aligned} 0 = 2ah(a) + abh(b) &= 2\sin^2(\alpha)\cot(\alpha)\varphi(\alpha) + 2\sin^2(\beta)\cot(\beta)\varphi(\beta) \\ &= \sin(2\alpha)\varphi(\alpha) + \sin(2\beta)\varphi(\beta) = \sin(2\alpha)(\varphi(\alpha) + \varphi(\beta)) \end{aligned}$$

So the assertion holds as $\sin(2\alpha) \neq 0$.

The second equality follows from the first. □

Next, we show $[T] = \sum_{i=1}^6 l_i\varphi(\alpha_i)$ for a orthohedron T: By scaling, it suffices to prove for T of the form $T(\sin^2(\alpha), \sin^2(\beta))$(25.1.2.16). Thus by(25.1.2.19) and(25.1.2.17),

$$\begin{aligned} [T(\sin^2(\alpha), \sin^2(\beta))] &= h(\sin^2(\alpha)) + h(\sin^2(\beta)) - h(\sin^2(\alpha)\sin^2(\beta)) \\ &= \cot(\alpha)\varphi(\alpha) + \cot(\beta)\varphi(\beta) + \cot(\gamma)\varphi(\pi/2 - \gamma) = \sum_{i=1}^6 l_i\varphi_i(\alpha_i) \end{aligned}$$

Finally, to show additivity of φ, notice by the lemma above, it suffices to show $\varphi(\alpha) + \varphi(\beta) = \varphi(\alpha + \beta)$ for $\alpha, \beta \in (0, \pi/2)$. In this case, let $\gamma = \pi - \alpha - \beta \in (0, 2\pi)$, then use(25.1.1.4) to find a rectangular solid that cuts along a diagonal to 6 orthohedra T_i s.t. the dihedral angles along the diagonals are $(\alpha, \beta, \gamma, \alpha, \beta, \gamma)$. Then

$$0 = [R] = \sum_{k=1}^6 [T_i] = 2l(\varphi(\alpha) + \varphi(\beta) + \varphi(\gamma)) + \sum_{k=1}^6 l_k(\varphi(\theta_{k1}) + \varphi(\theta_{k2}))$$

where l is the length of the diagonal, θ_{k_i} are the dihedral angles along the edges of the rectangular solid that is connected to the diagonal, and $\theta_{k_1} + \theta_{k_2} = \pi/2$. Thus by the lemma above, $\varphi(\alpha) + \varphi(\beta) = -\varphi(\gamma) = \varphi(\alpha + \beta)$. □

3 Combinatorial Geometry

Convex Polygons

Prop. (25.1.3.1). For $n \in \mathbb{Z}_{\geq 4}$ and any n points in $\mathbb{R}^2$ in general position, they form a convex n-gon iff any 4 points of them form a convex quadrilateral. ⌟

Proof: We use induction on n. $n = 4$ is trivial. For $n \geq 5$, let the points by $\{P_1, \ldots, P_n\}$, then by induction hypothesis, any $n-1$ points of them form a convex $(n-1)$-gon. So for any $1 \leq k \leq n$, $\{X_1, \ldots, \widehat{X_k}, \ldots X_n\}$ is a convex $(n-1)$-gon, and X_k is not contained in any sub-$(n-2)$-gon of $X_1 \ldots \widehat{X_k} \ldots X_{n-1}$. But any convex $(n-1)$ is a sum of its sub-$(n-2)$-gons, because we can use equations of the form $a_1P_1 + a_2P_2 = a_3P_3 + a_4P_4, a_i > 0$ to eliminate some P_i. Because k is arbitrary, this means $P_1 \ldots P_n$ is convex. □

Thm. (25.1.3.2) [Erdös-Szekeres]. For any $n \in \mathbb{Z}_{\geq 2}$, there exists a minimal positive integer $N(n)$ s.t. for any $ES(n)$ points in $\mathbb{R}^2$ in general position, there exists a subset of n points forming a convex n-gon. Moreover,

$$2^{n-2} + 1 \leq ES(n) \leq \binom{2n-4}{n-2} + 1.$$

⌟

Proof: We first prove that $ES(4) = 5$: Given 5 points in $\mathbb{R}^2$ in general position, we need to find 4 points that form a convex quadrilateral. If the convex hull of these 5 points is a quadrilateral or a pentagon, we are done, and if the convex hull is a triangle ABC, and D, E are inside ABC, then suppose BC lies in the same side of the line $\overline{DE}$, then $BDEC$ form a convex quadrilateral.

For general n, in fact $ES(n) \leq R(4, 2; 5, n)$(25.4.2.1), because for $R(4, 2; 5, n)$ many points $X \subset \mathbb{R}^2$, divide the 4-subsets of X into two classes depending on either they form a convex quadrilateral or not, then either there exists a 5-subset whose 4-subsets are all non-convex, or there exists an n-subset whose 4-subsets are all convex. The first case is not possible by the fact $ES(4) = 5$, so the second case is true. Thus we get a convex n-gon by(25.1.3.1).

For the lower bound, it suffices to construct 2^{n-2} points with no n points forming a convex n-gon: Cf.[Art of Counting, Erdös]P680.?

For the upper bound for $ES(n)$, Cf. [Erdös-Szekers](or [Holmsen-Mojarrad-Pach-Tardos], where they proved that $ES(n) \leq 2^{n+O(\sqrt{n \log n})}$). □

Conj. (25.1.3.3) [Erdös-Szekeres]. For any $n \in \mathbb{Z}_{\geq 2}$, $ES(n) = 2^{n-2} + 1$. ⌟

Proof: □

Remark (25.1.3.4). This conjecture has been proven for $n \leq 6$. ⌟

Crossing Numbers of Graphs

Thm. (25.1.3.5) [Leighton]. For any simple graph G with n vertices and $e \geq 4n$ edges drawn in $\mathbb{R}^2$, $\mathrm{Cr}(G)$(the number of crossing of G) is at least $e^3/(100n^2)$. ⌟

Proof: Cf.[Ajtai, M.; Chvátal, V.; Newborn, M. M.; Szemerédi, E. Crossing-free subgraphs]. □

Incidences

Thm. (25.1.3.6) [Szemérédi-Trotter]. There exists $C \in \mathbb{R}_+$ s.t. if $n, t \in \mathbb{Z}_+$, then for any $\mathscr{P} \subset \mathbb{R}^2, \#\mathscr{P} = n$ and a family $\mathscr{L}$ of lines in $\mathbb{R}^2$ s.t. $\#\mathscr{L} = t$, the numbers of incidences $\#I(\mathscr{P}, \mathscr{L})$ between points in $\mathscr{P}$ and lines in $\mathscr{L}$ is$\leq 22(nt)^{2/3} + 4n + t$. ⌟

Proof: We may assume that any line in $\mathscr{L}$ is incident to at least one point in $\mathscr{P}$. Draw a graph G in $\mathbb{R}^2$ with $V(G) = \mathscr{P}$, and join two points with a straight segment if they are consecutive points on one of the lines in $\mathscr{L}$. Then G is a simple graph, and the crossing number of G is at most t^2. Also $\#I(\mathscr{P}, \mathscr{L}) = t + E(G)$.

Then it follows from(25.1.3.5) that either $4n > \#I(\mathscr{P}, \mathscr{L}) - t$, or $t^2 \geq \mathrm{Cr}(G) \geq (\#I(\mathscr{P}, \mathscr{L}) - t)^3/(100n^2)$, from these the assertion follows. □

Cor. (25.1.3.7). There exists $C \in \mathbb{R}_+$ s.t. if $n \in \mathbb{Z}_+$ and $\mathscr{P} \subset \mathbb{R}^2$ is a set of n points, and $\mathscr{L}$ is family of lines determined by $\mathscr{P}$, then there exists a point $P \in \mathscr{P}$ belong to at most Cn lines in $\mathscr{L}$. ⌟

Proof: Cf.[S-T83]. □

Thm. (25.1.3.8) [Szemérédi-Trotter]. There exists $C \in \mathbb{R}_+$ s.t. if $n, k \in \mathbb{Z}_+, 2 \leq k \leq 10\sqrt{n} + 1$, $\mathscr{P} \subset \mathbb{R}^2, \#\mathscr{P} = n$, and $\mathscr{L}$ is a family of lines in $\mathbb{R}^2$ each containing at least k points from $\mathscr{P}$, then $\#\mathscr{L} \leq 100n^2/(k-1)^3$.

(The constant C can be taken to be 3 by [Clarkson et al. Combinatorial complexity bounds for arrangements of curves and surfaces].) ⌟

Proof: Let $t = \mathscr{L}$. Draw a graph G in $\mathbb{R}^2$ with $V(G) = \mathscr{P}$, and join two points with a straight segment if they are consecutive points on one of the lines in $\mathscr{L}$. Then G is a simple graph, and the crossing number of G is at most t^2. Also $E(G) \geq t(k-1)$.

Then it follows from(25.1.3.5) that either $4n > t(k-1)$, or $t^2 \geq \mathrm{Cr}(G) \geq t^3(k-1)^3/(100n^2)$, from these the assertion follows. □

Remark (25.1.3.9). The assertion is tight for $2 \leq k \leq \sqrt{n}$: Take $\mathscr{P}$ to be the $\sqrt{n} \times \sqrt{n}$ integer grid. Cf.[Beck, On the lattice property of the plane and some problems of Dirac, Motzkin, and Erdös in combinatorial geometry]?. ⌟

Distance Problems

Thm. (25.1.3.10) [Erdös/Guth-Katz]. For $n \in \mathbb{Z}_{\geq 2}$, let $f(n)$ be the minimal number of distinct distances generated by n distinct points in $\mathbb{R}^2$, then

$$f(n) = \Theta(\frac{n}{\log n}).$$

⌟

Proof: Consider the points (x, y) where $1 \leq x, y \leq \sqrt{n}$, then the distances between them are all of the form $\sqrt{a^2 + b^2}$, where $1 \leq a^2 + b^2 < 2n$. Then by(21.4.1.4), there are $O(\frac{n}{\log n})$ many points.

Conversely, Cf.[Guth-Katz]? □

Thm. (25.1.3.11) [Solymosi]. There exists $C \in \mathbb{R}_+$ s.t. for any $n \in \mathbb{Z}_{\geq 2}$ and any n distinct points in $\mathbb{R}^2$, one of them determine at least $Cn^{6/7}$ different distances from the others. ⌟

Proof: Cf.[Solymosi, Distinct distances in the plane]. □

Conj. (25.1.3.12) [Erdös]. For $n \in \mathbb{Z}_{\geq 2}$, the number of distinct distances determined by the vertices of a convex n-gon in $\mathbb{R}^2$ is at least $\lfloor \frac{n}{2} \rfloor$, with equality iff this is a regular n-gon. ⌟

Proof: □

Thm. (25.1.3.13) [Erdös/Spencer-Szemérredi-Trotter]. For $n \in \mathbb{Z}_{\geq 3}$ and $r \in \mathbb{R}_+$, let $U(n)$ be the maximal number of times the unit distance occur among n points in $\mathbb{R}^2$, then there exists $C \in \mathbb{R}_+$ s.t.

$$n^{1+C/\log\log n} < U(n) < \min(n^{3/2}, 6n^{5/4}).$$

⌟

Proof: To prove $U(n) < n^{3/2}$: This is clearly true for $n \leq 3$, so we assume $n \geq 4$. Given n points $\{P_1, \ldots, P_n\}$, and for $1 \leq i \leq n$, suppose there are x_i points with distance r from P_i. We may assume that $x_1 \geq x_2 \geq \ldots \geq x_n$. Then for any $i \neq j$, the x_i points at distance r from P_i can contain at most two points with distance r from P_j, so for each $1 \leq j \leq n$,

$$\sum_{i=1}^{j} (x_i - 2i + 2) \leq n.$$

Denote $\lfloor \sqrt{n} \rfloor = a, \{\sqrt{n}\} = \varepsilon$, then

$$x_1 + x_2 + \ldots + x_a \leq n + a(a-1) = 2n - 2\varepsilon\sqrt{n} + \varepsilon^2 - \sqrt{n} + \varepsilon < 2n - 2\varepsilon\sqrt{n}.$$

Thus $x_a < \frac{1}{a}(2n - 2\varepsilon\sqrt{n}) = 2\sqrt{n}$, and

$$\sum x_i < 2n - 2\varepsilon\sqrt{n} + (n-a)2\sqrt{n} = 2n^{3/2}.$$

To prove $U(n) < 6n^{5/4}$: Let U be the number of times the unit distance occur. Draw a graph G in $\mathbb{R}^2$ with vertices the given points, and two points are connected by an arc in unit circle if they are consecutive points on the unit circle centered at one of the points. Then G is a multigraph. Noticing two points are connected by at most two arcs, so minimally delete arcs so that each pair is connected by at most one arc, we get a graph G satisfies $E(G) \geq U - n/2$ and $\mathrm{Cr}(G) \leq 2n^2$. Then by(25.1.3.5), either $U - n/2 \leq E(G) < 4n$, or $2n^2 \geq \mathrm{Cr}(G) \geq (U - n/2)^3/(100n^2)$, from these the assertion follows.

For the lower bound, consider the set of points $(x, y), 0 \leq x, y \leq \sqrt{n}$.**?** Cf.[Erd46]. □

Prop. (25.1.3.14). For $n \geq 3$, let $a_{\min}(n)$ and $a_{\max}(n)$ be the maximal number of times the minimal and maximal distance of distinct n points in $\mathbb{R}^2$ can be achieved, then

$$a_{\max}(n) = n, \quad a_{\min}(n) \leq 3n - 6, \quad |3n - a_{\min}(n)| = \Theta(\sqrt{n}).$$

⌟

Proof: For $a_{\max}(n)$, notice $a_{\max}(n) \geq n$ because it can easily achieve n times. To prove $a_{\max}(n) \leq n$, we use induction on n: if the given points are $\{P_1, \ldots, P_n\}$, and $d(P_1, P_2)$ and $d(P_3, P_4)$ are both maximal, then by an easy argument, $P_1P_2 \cap P_3P_4 \neq \varnothing$. Now connect any two points with maximal distance, and consider two cases: if each point is connected to at most 2 points, then there are at most n edges; and if some point P_1 is connected to 3 points P_2, P_3, P_4, where $\angle P_2P_1P_4$ is acute, and P_3 are between P_2, P_4, then it is clear P_3 cannot connect to any other P_i, so we can omit P_3 and use induction on n.

For $a_{\min}(n)$, we first prove that $a_{\min}(n) \leq 3n-6$?: Connect two points if they has minimal distance, then clearly these edges don't intersect. Thus the resulting graph is planer, and then has at most $3n-6$ edges by Euler's theorem(25.2.6.3).

To show $|3n - a_{\min}(n)| = \Theta(\sqrt{n})$, use triangular constellation?. □

Conj. (25.1.3.15) [Borsuk]. For $k \in \mathbb{Z}_+$, each subset $S \subset \mathbb{R}^k$ of diameter 1 can be decomposed into $k+1$ subsets s.t. each subset has diameter< 1. ⌟

Proof:

□

Rational Distances

References are [Sol00], [A-E45] and [Erd45a].

Def. (25.1.3.16) [Integral Sets]. An **integral set** in $\mathbb{R}^2$ is a point set s.t. the distances between the elements in S are all integers. ⌟

Prop. (25.1.3.17) [Anning-Erdös]. For any $n \in \mathbb{Z}_+$, we can a planer integral set of cardinality n in general position. ⌟

Proof: let $\alpha = \arcsin(3/5)$, then α/π is non-rational Consider the n points $P_k = e^{\mathrm{i}k\alpha}, 0 \leq k \leq n-1$, then it is clear that all the distances between the points are rational. Thus by scaling, we can find n points with integral distances. □

Lemma (25.1.3.18). If a triangle T has integer side-lengths $a \leq b \leq c$, then the minimal height m of it is at least $\sqrt{a - \frac{1}{4}}$. ⌟

Proof: As $a, b, c \in \mathbb{Z}_+$, $a + b \geq c + 1$. The minimal height m corresponds to the side with length c, so it follows from heron's formula? that

$$m^2 = a^2 - (\frac{c^2 + a^2 - b^2}{2c})^2.$$

Clearly larger c gives smaller height, so we may assume $c = a + b - 1$. Then

$$\frac{c^2 + a^2 - b^2}{c} = c + \frac{a+b}{c}(a-b) \leq c + a - b = 2a - 1.$$

And the assertion follows. □

Lemma (25.1.3.19) [Erdös]. In a planer integral set H, if there exists two point-pairs (A, B) and (C, D) in general position(i.e. the lines AB and CD are distinct, and the bisector lines are distinct), then $\#H \leq 4d(A, B) \cdot d(C, D)$. ⌟

Proof: This is because for any $d \in \mathbb{Z}$, the set $\{d(P, A) - d(P, B) = d\}$ is a hyperbola, and similar for C, D. The condition implies that the hyperbolas for any two such distance pairs are different, so they intersect at at most 2 points. So there are at most $4d(A, B) \cdot d(C, D)$ many points. □

Prop. (25.1.3.20) [Annin-Erdös/Solymosi]. If H is a planer infinite integral set, then the points of H lie on a line.

In fact, if A, B are two points in a planer integral set H with $d(A, B) = d > 1$, and $\#H \geq d^3$, then there are at most $2d - 1$ points of H not on the line AB. ⌟

Proof: The first assertion follows from(25.1.3.19). For the second assertion, Cf.[Sol00]P339**?**. □

Cor. (25.1.3.21) [Minimal distances of Integral Sets]. If H is a planer integral set in general position and $\#H \geq 4$, then the minimal distance between points in H is at least $(\#H+1)^{1/3}$. ⌟

Proof: If there are two points A, B with $d(A,B) = 1$, then by triangular inequality, any other points must be in equal distances with A and B. So it follows from(25.1.3.18) that there are at most points.

In other cases, it follows from the proposition that $\#H \leq d(A,B)^3 - 1$. □

Conj. (25.1.3.22) [Erdös-Ulam]. There doesn't exists a dense subset $S \subset \mathbb{R}^2$ s.t. all the distances between points in S are rational. ⌟

Proof: It follows from `https://terrytao.wordpress.com/2014/12/20/the-erdos-ulam-problem-varieties-of-general-type-and-the-bombieri-lang-conjecture/#more-7930` that this conjecture is a consequence of the Bombieri-Lang conjecture(15.14.8.1).**?** □

Lemma (25.1.3.23). If H is a planer integral set with $\#H \geq 4$ with diameter Δ and having at most $n/2$ colinear points, then there exists two point-pairs (A,B) and (C,D) in general position(as in(25.1.3.19)) s.t. $d(A,B), d(C,D) \leq 12\Delta/\sqrt{n}$. ⌟

Proof: Call a point $P \in H$ single if there is at most one other point in H with distance smaller than $12\Delta/\sqrt{n}$ with P. Then a method of volume counting implies that there are less than $n/2$ single points.

Remove all the single points, then in the remaining set H', any point P has two points $Q_1, Q_2 \in H'$ s.t. $d(P, Q_i) \leq 12\Delta/\sqrt{n}$. **?** Then we can find two point-pairs in general position.**?** □

Thm. (25.1.3.24) [Minimal Diameters of Integral Sets]. There exists $c \in \mathbb{R}_+$ s.t. for any $n \in \mathbb{Z}_+$, any planer integral set with cardinality n has diameter at least cn. ⌟

Proof: If there are more than $n/2$ points in a single line, then the diameter is at least $n/2$. Suppose this is not the case, then it follows from(25.1.3.23) that

$$n \leq 4\left(\frac{\Delta}{\sqrt{n}}\right)^2,$$

and the assertion follows. □

4 Probabilistic Methods

References are [The probabilistic method, Alon-Spencer].

25.2 Graph Theory I

References are [Die17].

Notation (25.2.0.1).

- For simplicity, we usually use graph to denote a simple graph(25.2.1.1)(unless specified otherwise), and a multi-graph to denote a graph with (possibly)multi-edges or loops.
- For a multi-graph G,
  - let $V(G)$ denote the set of vertices of G,
  - let $E(G)$ denote the set of edges of G,
  - let $\overrightarrow{E}(G)$ denote the set of triples (e, x, y) where $e \in E(G)$, and $e \cap V(G) = \{x, y\}$,
  - let $v(G)$ denote the number of vertices,
  - let $e(G)$ denote the number of edges,
  - let $\chi(G) = v(G) - e(G)$ denote the Euler characteristic of G,
  - for $v \in V(G)$, let $\deg(v)$ denote the set of vertices of G,
  - let $d(G)$(or $t(G)$) denote the average degree of vertices in G, which equals $2e(G)/v(G)$ when G is finite,
  - let $\delta(G)$ denote the minimum degree of vertices of G,
  - let $\Delta(G)$ denote the maximum degree of vertices of G,
  - for $U \subset V(G)$, let $N(U)$ denote the set of vertices connected to U, and let $E(U)$ denote the set of edges adjacent to U.
  - let $\omega(G)$ denote the maximal cardinality of a clique in G(25.2.5.1),
  - let $\alpha(G)$ denote the maximal cardinality of an independent subset of G,
  - for two disjoint non-empty subset $X, Y \subset V(G)$, let $e(X, Y)$ denote the number of edges between vertices in X and vertices in Y, and $d(X, Y) = \frac{e(X,Y)}{\#X\#Y}$ the density between X and Y.
  - for $U \subset G$, $G(U)$ is the induced subgraph on U,
  - let $\gamma(G)$ denote the chromatic number of G,
  - let $\kappa(G)$ denote the number of spanning trees of G,
  - let $g(G)$ denote the girth of G,
  - let $h(G)$ denote the expanding constant of G(25.3.9.1).

⌟

1 Basics

Def. (25.2.1.1) [Graphs]. A **graph** X is a CW-complex of dimension≤ 1 with a given presentation $(X^0, X^1 = X)$(4.13.3.1). the elements in the set of X^0 are called **vertices** of X, and the 1-cells are called **edges** of X.

A **simple graph** is a graph without loops and multi-edges.

For a graph X, a **subgraph** is a sub CW-complex of X. And if $V' \subset V(X)$ is a subset, the **induced subgraph** of X is defined to be the subgraph $X' \subset V(X)$ whose vertices are just V', and two vertices in V' are connected by an edge iff they are connected by an edge in X. ⌟

Def. (25.2.1.2)[Claws]. A **claw graph** is any graph isomorphic to the graph $G = (V(G), E(G))$ where $V(G) = \{1, 2, 3, 4\}, E(G) = \{12, 13, 14\}$. ⌟

Degrees of Vertices

Def. (25.2.1.3) [Complete Graphs]. A **complete graph** is a simple graph that each two vertices is connected by an edge. For $r \in \mathbb{Z}_+$, a complete graph of size r is denoted by K^r. ⌟

Def. (25.2.1.4) [Complement Graph]. For $G \in \mathtt{Graph}^{\mathtt{simple}}$ the **complement graph** $G^c \in \mathtt{Graph}^{\mathtt{simple}}$ is a simple graph s.t. $V(G^c) = V(G)$, and two distinct vertices in G^c are adjacent if they are not adjacent in G. ⌟

Def. (25.2.1.5) [Kernels]. For any oriented graph $H \in \mathtt{Graph}$, a **kernel of graph** of H is an independent set $U \subset V(H)$ s.t. for any $v \in V(H) \setminus U$, there exists an edge $vu \in \overrightarrow{E}(G)$ with $u \in U$. ⌟

Prop. (25.2.1.6). For any $G \in \mathtt{Graph}^{\mathrm{fin}}$ with $E(G) \neq \varnothing$, there is a subgraph H of G s.t. $2\delta(H) \geq t(H) \geq t(G)$. ⌟

Proof: If there is a vertex $v \in V(G)$ s.t. $\deg(v) < \frac{1}{2}t(G) = e(G)/v(G)$, then we delete v, and get $G_1 = G \setminus \{v\}$. Do the same for G_1, and so on. In this way, it is easy to see that $t(G)$ is increasing. Because G is finite, this process stops at some point. But because $t(\mathrm{pt}) = 0 < G$, the stopping graph H cannot be empty. And this graph H satisfies $2\delta(H) \geq t(H) \geq t(G)$. □

Def. (25.2.1.7)[Groupies]. A **groupie** in a graph G is a vertex $P \in V(G)$ s.t. if $r(P)$ is the summation of degree of vertices of points Q adjacent to P, then $r(P) \geq \frac{2e(G)}{v(G)} \deg P$. ⌟

Prop. (25.2.1.8). Any $G \in \mathtt{Graph}$ has a groupie. ⌟

Proof: For $P \in V(G)$, let $r(P)$ is the summation of degree of vertices of points Q adjacent to P. then

$$\sum_{P \in V(G)} r(P) = \sum_{Q \in V(G)} \deg(Q)^2 \geq (\sum \deg(P))^2/v(G) = t(G)^2 v(G) = t(G) \sum \deg(P).$$

So there must be some $P \in V(G)$ that $r(P) \geq t(G) \deg P$. □

Paths and Circuits

Def. (25.2.1.9) [Paths, Circuits and Cycles]. For $G \in \mathtt{Graph}$, a **walk in an (oriented)graph** of length $k \in \mathbb{Z}_{\geq 2}$ is a sequence $(v_1, e_1, \ldots, e_{k-1}, v_k)$ s.t.

- $v_j \in V(G)$ for any $j \in [k]_+$,
- $e_i = v_i v_{i+1} \in E(G)$ for $i \in [k-1]_+$.

A **simple path** is a path without repetition vertices.

A **circuit in a graph** of length $k \in \mathbb{Z}_{\geq 2}$ is a sequence $(v_1, e_1, \ldots, e_{k-1}, v_k, e_k)$ s.t.

- $v_j \in V(G)$ for any $j \in [k]_+$,
- $e_i = v_i v_{i+1} \in E(G)$ for $i \in [k-1]_+$,
- $e_k = v_k v_1 \in E(G)$.

A **simple circuit** is a circuit without repetition vertices.

A **cycle in a graph**(resp. ordered cycle) is an $\mathbb{Z}/(k) \ltimes \mathbb{Z}/(2)$(resp. $\mathbb{Z}/(k)$)-orbit of simple circuits.

The **girth** $g(G)$ of G is the minimal length of a circuit in G. ⌟

Prop. (25.2.1.10) [Minimal Degree and Large Cycles]. For any $G \in \mathtt{Graph}$, G contains a path of length $\delta(G)$. And if $\delta(G) \geq 2$, it contains a cycle of length$\geq \delta(G)+1$. ⌟

Proof: Consider the largest simple path, then the neighbourhood of the endpoints are all on this path, thus it has length$\geq \delta(G)$. And consider its neighbors on this path, we get a simple circuit. □

Def. (25.2.1.11) [Distances]. For any $G \in \mathtt{Graph}$ and $x, y \in V(G)$, the **distance between vertices** $d_G(x, y)$ is defined to be the infimum of lengths of paths in G with endpoints x and y.

The maximal distances between two vertices in G is called the **diameter of graph** of G, denoted by $\operatorname{diam}(G)$. ⌟

Def. (25.2.1.12) [Radius]. For $G \in \mathtt{Graph}$, the **radius** of G is defined to be

$$\operatorname{rad}(G) = \min_{x \in V(G)} \max_{y \in V(G)} d_G(x, y).$$

Clearly $\operatorname{rad}(G) \leq \operatorname{diam}(G) \leq 2\operatorname{rad}(G)$. ⌟

Prop. (25.2.1.13). For $G \in \mathtt{Graph}$, either $g(G) = \infty$ or $g(G) \leq 2\operatorname{diam}(G) + 1$. ⌟

Prop. (25.2.1.14) [Radius, Maximal Degrees and Sizes]. For $k, d \in \mathbb{Z}_+, G \in \mathtt{Graph}$, if $\operatorname{rad}(G) \leq k, \Delta(G) \geq d \geq 3$, then

$$v(G) \leq \frac{d}{d-2}(d-1)^k.$$

⌟

Proof: Take a central point $z \in G$ and let D_i be the set of vertices with distances i from z. Then $\#D_0 = 1$, $\#D_i \leq d(d-1)^{i-1}$ for $i \in \mathbb{Z}_+$. Thus we get the desired result by counting. □

Prop. (25.2.1.15) [Average Degree, Girth and Sizes, Alon-Hoory-Linial2002]. For $g, d \in \mathbb{Z}_+, G \in \mathtt{Graph}$, if $d(G) \geq d \geq 2$ and $g \leq g(G) < \infty$, then

$$v(G) \geq \begin{cases} 2\sum_{i=0}^{\lfloor \frac{g}{2} \rfloor - 1}(d-1)^i & ,2|g \\ 1 + d\sum_{i=0}^{\lfloor \frac{g}{2} \rfloor - 1}(d-1)^i & ,2 \nmid g \end{cases}.$$

⌟

Proof: ? □

Cor. (25.2.1.16). If $d(G) \geq 3$, then $g(G) < 2\log v(G)$. ⌟

Def. (25.2.1.17) [Large Girth Families]. For $k \in \mathbb{Z}_{\geq 3}$, a family of k-regular finite simple graphs $(X_n) \in \mathtt{Graph}^{\mathbb{Z}_+}$ is called a family of **large girth graphs** if there exists $C \in \mathbb{R}_+$ s.t. $\varinjlim v(X_n) = \infty$ and $g(X_n) \geq C\log_{k-1} v(X_n)$. ⌟

Prop. (25.2.1.18) [Large Girth and Large Connectivity Graphs]. For any $k \in \mathbb{Z}_+$, there exists a finite graph $H \in \mathtt{Graph}^{\mathtt{simple}}$ with $g(H) > k$ and $\kappa(H) > k$. ⌟

Proof: This follows from(25.3.2.9) and(25.2.4.5). □

Def. (25.2.1.19) [Prime circuits]. A **prime circuit** in an unoriented graph G is a circuit that is not a non-trivial multiple of another cycle, and doesn't contain a segment of the form $\ldots, x, y, x, \ldots$ for $x, y \in V(G)$. ⌟

Def. (25.2.1.20) [Primitive Graphs]. For a connected graph $G \in \mathtt{Graph}$, the gcd of lengths of circuits in G is called the **period of graph** G. G is called a **primitive graph** if it has period 1.

If G has period v, then it can be decomposed into $G_1 \amalg \ldots G_v$ s.t. each edge is between some G_i to G_{i+1}. ⌟

Def. (25.2.1.21) [Holes]. For a simple graph, a **hole of graph** $H \subset G$ is an induced subgraph that is isomorphic to a cycle of length≥ 4. An **antihole of a graph** is an induced subgraph of G whose complement is a graph in G^c. ⌟

Trees and Forests

Def. (25.2.1.22) [Trees]. A **tree** is a graph T s.t. $H_1(T) = 0$. A tree in a graph X is called a **maximal tree** if it contains all vertices of X. A **forest** is a graph that is a disjoint union of trees. ⌟

Prop. (25.2.1.23). Any tree T is contractible, and any vertex v is a deformation retract of T. ⌟

Proof: □

Prop. (25.2.1.24) [Maximal Trees]. Every connected graph contains a maximal tree, and any tree in a connected graph is contained in a maximal tree.

A tree T in a graph X is maximal iff $X^0 \subset T$. ⌟

Proof: Cf.[Hat02]P84. □

Prop. (25.2.1.25) [π_1 of Graphs]. For a connected graph X with a maximal tree T, $\pi_1(X)$ is a free group with basis the classes $[f_\alpha]$ corresponding to the edges $e_\alpha \in X \backslash T$. ⌟

Proof: The quotient map $X \to X/T$ is a homotopy equivalence by(4.13.6.7). And the quotient space X/T has only one vertex, thus is a wedge sum of circles corresponding to $e_\alpha \in X \backslash T$. So we are done by(4.13.4.29). □

Prop. (25.2.1.26) [Covering Spaces of Graphs]. Every covering space $\pi : \widetilde{X} \to X$ of a graph is also a graph, with vertices and edges lifts of vertices and edges of X. ⌟

Proof: Let the sets $\pi^{-1}(v)$ be vertices of $\widetilde{X}$, where v are vertices of X. And if we write X as a quotient space of $X^0 \cup_\alpha I_\alpha$, each I_α can be lifted to maps to $\widetilde{X}$, and we let these be edges of $\widetilde{X}$. The topology of $\widetilde{X}$ coming from quotient topology of this is the same as the original topology, because they has the same basis open sets, because π is a local homeomorphism. □

Def. (25.2.1.27) [Path Trees]. For $G \in \mathtt{Graph}$, the **path tree** of G at u is defined to be the universal covering of G at u consisting of simple paths at u. ⌟

Prop. (25.2.1.28) [Spencer's Lemma]. If there is a triangulation of a plane polygon P, for arbitrary 3-color numbering($\{0, 1, 2\}$) of the vertices, if the number of edges on the boundary with color $(0, 1)$ is odd, then there is a triangle with vertices of pairwise different colors. ⌟

Proof: In fact the number of those triangles with vertices of pairwise different colors is odd. In fact, the number of $(0, 1)$-edges on a triangle is odd iff its vertices has pairwise different colors. But the sum of numbers of $(0, 1)$-edges on the triangles are odd, by hypothesis, thus the result. □

Contractions and Minors

Def. (25.2.1.29)[Subdivisions and Topological Minors]. A **subdivision** of a graph X is any graph obtained from X by 'subdividing'some or all of its edges by drawing new vertices on those edges.

For graphs X, Y, if Y contains a subgraph that is isomorphic to a subdivision of X, then X is called a **topological minor graph** of Y. ⌟

Def. (25.2.1.30)[Contractions and Minors]. For any graph G, divide $V(G)$ into connected subsets $V_{\alpha_1}, \ldots, V_{\alpha_k}$, and let X be the graph with

$$V(X) = \{\alpha_1, \ldots, \alpha_k\}, \quad E(X) = \{(\alpha_i, \alpha_j) | i \neq j, E(V_{\alpha_i}, V_{\alpha_j}) \neq \varnothing\}.$$

Then X is called a **contraction graph** of G.

For graphs X, Y, if X is isomorphic to a contraction of a subgraph of Y, then X is called a **minor graph** of Y. We sometimes use the notation $X = Y/U$ to denote a minor of Y that only contracts one connected connected subset U. ⌟

Prop. (25.2.1.31). Any topological minor is a minor. And if X is a minor of a graph G with $\Delta(X) \leq 3$, then X is also a topological minor of G. ⌟

Proof: The first assertion is easy. For the last assertion, consider each V_x for $x \in X$, then it suffices to show that for any three vertices x, y, z in a connected graph, there is a vertex with separate paths to them without intersection. For this, firstly find a shortest path W from x to y. If this path contains z, then z is the vertex we want. If this path doesn't contain z, then find a shortest path W' from z to W, then the endpoint of W' is the vertex we want. □

2 Spectral Graph Theory

Def. (25.2.2.1)[Companion Matrices]. For a finite multi-graph G with $\#V(G) = n$, given an ordering of the vertices, the

- **adjacency matrix** A_G of G is defined to be the $n \times n$ matrix (a_{ij}) with $a_{ij} = \alpha(v_i, v_j)$, the number of edges between v_i and v_j.
- **valence matrix** D_G of G is defined to be the $n \times n$ diagonal matrix $\mathrm{diag}(\deg(v_1), \ldots, \deg(v_n))$.
- **Laplacian matrix** L_G of G is defined to be the $A_G - D_G$.

It is clear that M_G, D_G, L_G are all real symmetric. In particular, they have real spectrums. ⌟

Def. (25.2.2.2)[Spectrums of Graphs]. For any finite multi-graph $G \in \mathtt{Graph}$, denote

$$\lambda_0 \geq \lambda_1 \geq \ldots \lambda_{v(G)}$$

be the set of eigenvalues of M_G. And denote $\rho(G) = \max |\lambda_i(G)|$ the **spectrum radius** of G. ⌟

Prop. (25.2.2.3)[Spectra of Adjacency Matrices]. For $k, n \in \mathbb{Z}_+$, if $G \in \mathtt{Graph}$ is k-regular and $n = v(G) \leq n$, then

- $k = \lambda_0 \geq \lambda_1 \geq \ldots \geq \lambda_{n-1} \geq -k$.
- $k > \mu_1$ iff G is connected.

⌟

Proof: 1: Clearly $(1, \ldots, 1)^t$ is an eigenvector with eigenvalue k. To show that $|\lambda_i| \leq k$, just choose a coordinate with largest absolute value.

2: This is also easy by taking a maximum coordinate. □

Prop. (25.2.2.4) [Spectrum of Bipartite Graphs]. For $k, n \in \mathbb{Z}_+$, if $G \in \texttt{Graph}$ is connected, k-regular and $n = v(G) \leq n$, then the following are equivalent:

- G is bipartite.
- $\lambda_i + \lambda_{n-1-i} = 0$.
- $\mu_{n-1} = -k$.

⌟

Proof: 1 → 2: Suppose $G = G^+ \coprod G^-$. If v is an eigenvector of A_G with eigenvalue μ, then by multiplying the coordinates of v corresponding to $v \in G^-$, we get an eigenvector of A_G with eigenvalue $-\mu$.

2 → 3 follows from(25.2.2.3).

3 → 1: similarly, choose a coordinate of the eigenvector with eigenvalue $-k$. Then

$$v_x = -\frac{1}{k} \sum_{yx \in E(G)} v_y.$$

So it can be shown that $v_y = -v_x$ if $xy \in E(G)$. By this way and the fact G is connected, we get a bipartition of $V(G)$. □

L_G and Spectral Gaps

Prop. (25.2.2.5). For any finite graph $G \in \texttt{Graph}$, L_G is positive-semidefinite, as for any $\mathbf{x} \in \mathbb{R}^n$,

$$\mathbf{x}^T L_G \mathbf{x} = \sum_{1 \leq i \leq j \leq n} \alpha(v_i, v_j)(x_i - x_j)^2.$$

And if G is connected, then L_G has nullity 1, whose eigenspace is spanned by $\mathbf{x} = (1, 1, \ldots, 1)^t$. ⌟

Prop. (25.2.2.6). Let G be a finite connected multi-graph with $\#V(G) = n$ and diameter $d = d(G)$, then the smallest eigenvalue λ_1 of L_G satisfies $\lambda_1 \geq 1/(nd)$. ⌟

Proof: Let w be the unit eigenvector belong to λ_1, then there exists $i \in [n]_+$ s.t. $|w_i| \geq 1/\sqrt{n}$. We may assume that $w_1 > 1/\sqrt{n}$. Since w is orthogonal to $(1, \ldots, 1)^t$, we have $\sum w_i = 0$. So there exists some $w_k < 0$. Let $v_1, v_2, \ldots, v_k$ be a minimal path from v_1 to v_k, then $k - 1 \leq d$, and

$$\lambda_1 = \mathbf{w}^t L_G \mathbf{w} = \sum_{1 \leq i \leq j \leq n} \alpha(v_i, v_j)(w_i - w_j)^2 \geq \sum_{i=1}^{k-1} (w_i - w_{i+1})^2 \geq \frac{1}{k-1}(w_1 - w_n)^2 \geq \frac{1}{nd}.$$

□

Prop. (25.2.2.7) [Bigg]. For k-regular finite graph $G \in \texttt{Graph}$ and any cofactor M of L_G, $\det(M) = \mathrm{tree}(G)$. ⌟

Proof: Cf.[Biggs, Algebraic Graph Theory]Thm6.3.? □

Spectral Radius

Prop. (25.2.2.8). If $X \in \mathtt{Graph}$ is connected, then for any $x \in X$,

$$\rho(X) = \limsup_{s\to\infty} \sqrt[s]{t_s(x)}$$

where $t_s(x)$ is the number of closed paths starting from x. ⌟

Proof: Cf.[Discrete Groups, Expanding Graphs and Invariant Measures]Chap4.? □

Prop. (25.2.2.9). The spectrum radius of a (c,d)-regular tree is $\sqrt{c-1}+\sqrt{d-1}$. ⌟

Proof: ?Cf.[Walk generating functions and spectral measures of infinite graphs] and [Spectra of regular graphs and hypergraphs and orthogonal polynomials]. □

Thm. (25.2.2.10)[Greenberg/Cioabă]. Let X be a connected, infinite graph with $\Delta(X) < \infty$. Given $\varepsilon \in \mathbb{R}_+$, there exists $c(X,\varepsilon) \in \mathbb{R}_+, g(X,\varepsilon) \in \mathbb{Z}_+$ such that

- for any finite graph $Y \in \mathtt{Graph}^{\mathtt{simple}}$ covered by X,

$$\#\{\lambda \in \mathrm{Spec}(Y) | \lambda \geq \rho(X) - \varepsilon\} \geq c(\varepsilon, k)v(Y).$$

- for any finite graph $Y \in \mathtt{Graph}^{\mathtt{simple}}$ covered by X s.t. $g(Y) \geq g$,

$$\#\{\lambda \in \mathrm{Spec}(Y) | \lambda \leq -\rho(X) + \varepsilon\} \geq c(\varepsilon, k)v(Y).$$

⌟

Proof: Cf.[Eigenvalues of graphs and a simple proof of a theorem of Greenberg].? □

Cor. (25.2.2.11) [Alon-Boppana/Serre]. For any $\varepsilon \in \mathbb{R}_+$ and $k \in \mathbb{Z}_{\geq 3}$, there exists a $c(\varepsilon, k) \in \mathbb{R}_+$ s.t. for k-regular connected finite graph $G \in \mathtt{Graph}^{\mathtt{simple}}$,

$$\#\{\lambda \in \mathrm{Spec}(G) | \lambda \geq (2-\varepsilon)\sqrt{k-1}\} \geq c(\varepsilon, k)v(G).$$

⌟

Proof: [Sarnak, Elementary Number Theory]P26. □

3 Matching, Covering and Packing

Def. (25.2.3.1) [Matchings]. For $G \in \mathtt{Graph}$, a **matching on graph** is a subset $M \subset E(G)$ s.t. no two edges in M have a common vertex. ⌟

Def. (25.2.3.2) [Stable Matchings]. For any finite bipartite graph $G \in \mathtt{Graph}^{\mathrm{fin}}$, a **family of preferences** on $E(G)$ is a family $\{\leq_v\}_{v\in V(G)}$ where each $\leq_v$ is a linear ordering on $E(v)$.

Given a finite simple bipartite graph $G \in \mathtt{Graph}^{\mathrm{fin}}$ with a family of preferences, a **stable matching** on G is a matching M on G s.t. for any $e \in E(G)\setminus M$, $\exists f \in M$ s.t. e, f has a common vertex v and $e \leq_v f$. ⌟

Thm. (25.2.3.3) [Stabel Mapping Theorem, Gale-Shapley1962]. Any finite bipartite graph $G \in \mathtt{Graph}$ with a family of preferences has a stable matching(25.2.3.2). ⌟

Proof: ?Cf.[Diestel]P40. □

Matching Polynomials

Def. (25.2.3.4) [Matching Polynomials]. Let $G \in \texttt{Graph}$ with $n = v(G) < \infty$. For $i \in \mathbb{N}$, let m_i be the number of matchings in G consisting of i edges, then the **matching polynomial** of G is defined to be

$$\mu_G(T) = \sum_{i \in \mathbb{N}} (-1)^i m_i T^{n-2i}.$$

⌟

Thm. (25.2.3.5) [Roots of Matching Polynomials, Heilmann-Lieb/Godsil]. For any $G \in \texttt{Graph}$, the roots of the matching polynomial $\mu_G(X)$ are real, and have absolute value at most $\rho(P(G,u))$, where $P(G,u)$ is the path tree of G at u(25.2.1.27).

In particular, the roots have absolute values at most $\rho(T)$, where T is the universal cover of G, which is bounded by $2\sqrt{\Delta(G)-1}$. ⌟

Proof: Cf.[Algebraic Combinatorics, Godsil].?

For the last assertion, notice $P(G,u)$ is an induced subgroup of T, so so clearly $\rho(P(G,u)) \leq \rho(T)$. □

4 Connectivity

Def. (25.2.4.1) [s-Connected Graphs]. For $s \in \mathbb{Z}_+$, a graph $G \in \texttt{Graph}$ is called k**-connected** if it is connected after deleting any $k-1$ vertices.

The maximal $k \in \mathbb{Z}_+$ s.t. G is k-connected is denoted by $\kappa(G)$. ⌟

Def. (25.2.4.2) [Edge-Connected Graphs]. The maximal $k \in \mathbb{Z}_+$ s.t. G is k-edge-connected is denoted by $\lambda(G)$. ⌟

Def. (25.2.4.3) [Toughness]. For $t \in \mathbb{R}_+$, a graph $G \in \texttt{Graph}$ is called a t**-tough graph** if for any separator $S \subset V(G) \cup E(G)$, $G \setminus S$ has at most $\#S/t$ connected components. ⌟

Prop. (25.2.4.4). For any finite graph $G \neq \mathrm{pt} \in \texttt{Graph}^{\texttt{simple}}$, $\kappa(G) \leq \lambda(G) \leq \delta(G)$. ⌟

Proof: The second inequality is trivial. For the first, let F be a minimal edge separating set of G. If there is a vertex $v \in V(G)$ that is not incident to any edge in F, let C be the connected component of $G \setminus F$ containing v, then each edge in F connects C to another connected component, by minimality. But the vertices in C that is incident to any edge in F separates v from $G \setminus C$, thus $\kappa(G) \leq \lambda(G)$.

If every vertex $v \in V(G)$ is incident to an edge in F, then the neighborhoods w of v s.t. $vw \notin F$ are incident to different edges in F by minimality. Thus $\deg(v) \leq \lambda(G)$. As the neighborhoods of v separates G if $G \neq \{v\} \cup N(v)$, if G is not complete, then we get $\kappa(G) \leq \lambda(G)$. But when G is complete, $\kappa(G) = \lambda(G) = v(G) - 1$. □

Thm. (25.2.4.5) [Minimal Degree and Connectivity, Mader1972]. For $k \in \mathbb{Z}_+$, any $G \in \texttt{Graph}$ with $d(G) \geq 4k$ has a $(k+1)$-connected subgraph H s.t. $d(H) \geq d(G) - 2k$. ⌟

Proof: Cf.[Diestel]P13.? □

Def. (25.2.4.6) [(x,y)-Cuts]. For a finite graph G and $x, y \in V(G)$ with $d(x,y) \geq 2$, an (x,y)**-cut** in G is a set $S \in V(G) \setminus \{x,y\}$ s.t. $G \setminus S$ has no (x,y)-paths. ⌟

Thm. (25.2.4.7) [Menger]. Let G be a finite graph and $x, y \in V(G)$ s.t. $d(x,y) \geq 2$. Denote $\kappa_G(x,y)$ the minimum size of an (x,y)-cut in G and $\lambda_G(x,y)$ a maximum number of internally-disjoint (x,y)-paths in G, then $\kappa_G(x,y) = \lambda_G(x,y)$. ⌟

Proof: □

Def. (25.2.4.8) [(x,U)-Fans]. For a finite graph G and a subset $U \subset V(G)$ and $x \in V(G) \setminus U$, an **(x,U)-fan** of size k is a set of k-paths from x to U s.t. any two of them shear only x. ⌟

Prop. (25.2.4.9) [Fan Lemma, Dirac]. For $k \in \mathbb{Z}_+$ and $G \in \mathtt{Graph}$, $\kappa(G) \geq k$ iff $v(G) \geq k+1$, and for any subset $U \subset V(G)$ and each $x \in V(G) \setminus U$, G has an (x,U)-fan of size $\min(k, \#U)$. ⌟

Proof: If G has at least $k+1$ vertices and for any subset $U \subset V(G)$ with $|U| \geq k$ and each vertex $x \notin U$, G has an (x,U)-fan of size k, we show G is k-connected: If there is a $(k-1)$-vertex cut S, let A be a connected component of $G \setminus S$, and $U = V(G) \setminus A$. Then $\#U \geq k$, and for any $x \in A$, there are no (x,U)-cut of size k, because each path from x to U must intersect with S.

Conversely, if G is k-connected and $U \subset V(G), \#U \geq k$. Let $G' = G *_U \{y\}$, then G' is also k-connected. Then by Menger's theorem(25.2.4.7), $\lambda_G(x,y) = \kappa_G(x,y) \geq k$. Let $P_1, \ldots, P_k$ be internally-disjoint (x,y)-paths in G', then after deleting y, they form an (x,U)-fan of size k. □

Hamilton Cycles

Def. (25.2.4.10) [Eulerian Tours]. For a connected graph $G \in \mathtt{Graph}^{\text{fin}}$, an **Eulerian tour** is a circuit on G that traverses each edge of G exactly once. An **Eulerian graph** is a finite connected graph that admits an Euler tour. ⌟

Def. (25.2.4.11) [Hamilton Cycles]. For a graph $G \in \mathtt{Graph}^{\text{fin}}$, a **Hamilton-cycle** is a cycle in G that contains each vertex of G exactly once. Similarly, a **Hamilton-path** is a simple path in G that traverse each vertex of G exactly once. G is called a **Hamiltonian graph** if it has a Hamiltonian path.

G is called **Hamiltonian-connected** if each pair of vertices $x \neq y \in G$ is the endpoint of a Hamiltonian path in G. ⌟

Prop. (25.2.4.12) [Euler1736]. A connected graph $G \in \mathtt{Graph}^{\text{fin}}$ is an Eulerian graph iff $2|\deg(v)$ for any $v \in V(G)$. ⌟

Proof: One direction is clear. For the other, we use induction on $v(G)$. If $v(G) = 0$, this is true. For $v(G) > 0$, we can clearly find a walk with no repeated edges. Let W be such a walk with maximum length. Then we claim W is a Euler tour: Suppose not, then $G' = G \setminus E(W)$ also satisfies the hypothesis that $2|\deg(v)$ for any $v \in V(G)$. As G is connected there is an edge $e \in E(G')$ that is incident to a vertex in W. Then by induction hypothesis, the component of G' containing e has an Eulerian tour, which in concatenating with W makes a larger walk, contradiction. □

Thm. (25.2.4.13) [Asratian-Khachatrian1990]. A connected graph $G \in \mathtt{Graph}^{\text{fin}}$ has a Hamiltonian cycle if $v(G) \geq 3$, and

$$\deg(u) + \deg(w) \geq \#N(u) \cup N(v) \cup N(w)$$

for any induced path uvw(i.e. $uw \notin E(G)$). ⌟

Proof: The hypothesis is in fact equivalent to that

$$\#N(u) \cup N(w) \geq \#N(v) \setminus N(\{(u,w)\}).$$

As $\{u,w\} \subset N(v) \setminus N(\{(u,w)\})$, this implies that G has simple circuits. Let C be a longest simple circuit in G. Suppose G is not Hamiltonian, then there exists $u \in G \setminus C$ with $V = N(u) \cap C \neq \varnothing$. Let $V^+ = \{v^+ | v \in V\}$ be the set of successors of V in G, then by the maximality of C, $V \cap V^+ \neq \varnothing$, and $V^+ \cup \{u\}$ is an independent set, and no two of them have a common neighborhood outside C. Thus for any $v \in V$, we have

$$\#N(u) \cap N(v^+) \geq \#N(v) \setminus N(\{u, v^+\}) \geq \#N(v) \cap V^+ + 1.$$

Thus

$$e(V, V^+) = \sum_{v \in V} \#N(v) \cap V^+ \leq \sum_{v \in V} (\#N(u) \cap N(v^+) - 1) = e(V, V^+) - \#V,$$

contradiction. □

Cor. (25.2.4.14) [Dirac1952]. For any finite simple graph $G \in \mathtt{Graph}^{\mathtt{simple}}$ with $n = v(G) \geq 3$ and $\delta(G) \geq n/2$ has a Hamilton cycle. ⌟

Thm. (25.2.4.15) [Chvátal-Erdös]. If $k \in \mathbb{Z}_+$ and a simple graph $G \in \mathtt{Graph}^{\mathrm{fin}}$ satisfies $v(G) \geq 3, i(G) \leq \kappa(G)$, then G has a Hamiltonian-cycle. ⌟

Proof: The hypothesis implies that G is not a tree thus contains a simple path. Let $k = \kappa(G)$, and take a longest simple path C, if there exists $x \in V(G) \setminus C$, then by fan lemma(25.2.4.9), there exists an (x, U)-fan of size $\min(k, \#C)$, with vertices $x_1, \ldots, x_r$. Let y_i be the successor of x_i in C, then $xy_i \notin E(G)$ for each i, otherwise there is a longer simple path. This implies that $\#C > k$. Now for the set $\{x, y_1, \ldots, y_r\}$, the hypothesis $\kappa(G) = k$ implies that there is a path $y_i y_j$. Then we can find a cycle of larger size, contradiction. □

Cor. (25.2.4.16). If $k \in \mathbb{Z}_+$ and a simple graph $G \in \mathtt{Graph}^{\mathrm{fin}}$ satisfies $v(G) \geq 3, i(G) \leq \kappa(G) + 1$, then G has a Hamiltonian-cycle. ⌟

Proof: The graph $G * \mathrm{pt}$ satisfies the hypothesis of(25.2.4.15) and has a Hamiltonian cycle. Thus G has an Hamiltonian-path. □

Cor. (25.2.4.17). If $k \in \mathbb{Z}_+$ and a simple graph $G \in \mathtt{Graph}^{\mathrm{fin}}$ satisfies $v(G) \geq 3, i(G) \leq k$, and G is k-connected, then G is Hamiltonian-connected. ⌟

Proof: The proof is similar to that of(25.2.4.15): For any vertices $x \neq y \in G$, just choose the longest path from x to y. □

Prop. (25.2.4.18) [Tutte1956]. Any 4-connected Tutte planer graph has a Hamilton cycle. ⌟

Proof: □

Conj. (25.2.4.19) [Toughness Conjecture, Chvátal]. There exists $t \in \mathbb{R}_+$ s.t. every t-tough graph(25.2.4.3) has a Hamilton-cycle. ⌟

Proof: □

5 Complete Graphs

Cliques and Independent Sets

Def. (25.2.5.1) [Cliques]. For $G \in \texttt{Graph}$, a **clique** in G is a subgraph $H \subset G$ that is a complete graph. An **independent set** in a graph is a set of vertices that no two of them are adjacent.

For any graph G, let $\omega(G)$ be the size of the maximal clique in G, and let $\alpha(G) = \omega(G^c)$ be the size of the maximal independent set of G. ⌟

Def. (25.2.5.2) [Simplicial Cliques]. For $G \in \texttt{Graph}$, a **simplicial clique** in G is a clique K in G s.t. $N(k) \setminus K$ is a clique in $G \setminus K$ for any $k \in K$. ⌟

Prop. (25.2.5.3). If $G \in \texttt{Graph}$ is claw-free**??**nd K is a simplicial clique in G, then for any $k \in K$, $N(k) \setminus K$ is also a simplicial clique. ⌟

Proof: By definition $N(k) \setminus K$ is a clique. If for some $k \in K$ and $n \in N(k) \setminus K$, the set $H = N(n) \setminus (N(k) \cup K)$ is not a clique, then there exists two non-adjacent vertices $x, y \in H$. Then the graph induced by $\{x, y, n, k\}$ is a claw, contradiction. □

Prop. (25.2.5.4) [Erdös]. For any $k, l \in \mathbb{Z}_+$ and a graph G of size $(k-1)(l-1)+1$, either G contains a complete k-graph, or any no-circuits ordering of the complement graph G^c contains a directed path of l-vertices. ⌟

Proof: Consider any ordering on G^c. then we can put the vertices in a matrix by the following rule: The first row are vertices with no inward order, and for any $k \geq 1$, the row k are vertices not in the first k row and has an inward edge from some vertex in the row k.

Then there are no edges between vertices in the same row, and we are done if some row has k vertices. If each row has less than k vertices, then there are at least l row, which will give us a directed path of l-vertices, by our rule of construction. □

Prop. (25.2.5.5) [Turán/Ajtai-Komlós-Szeméredi]. If G is a multi-graph with $\omega(G) = 2$(25.2.5.1) and $v(G) \leq n, d(G) \leq t$, where $n, t \in \mathbb{R}_+$, then

$$\alpha(G) \geq \max\left(\frac{n}{100t}\log t, \frac{n}{t+1}\right).$$

⌟

Proof: Cf.[note on Ramsey Numbers]. □

Prop. (25.2.5.6). Let G be a graph with $n = \#V(G), e = \#E(G)$, and h be the number of triangles in G. Suppose $p \in (0,1)$ with $pn \geq 3$, then there exists an induced subgraph $G' \subset G$ s.t.

$$n' > np/2, \quad e' < 3ep^2, \quad h' < 3hp^3.$$

⌟

Proof: □

Prop. (25.2.5.7) [Ajtai-Komlós-Szeméredi]. Let $\varepsilon \in \mathbb{R}_+$ and G be a graph with $n = v(G), t = d(G)$, h the number of triangles in G. Suppose $h < nm^{2-\varepsilon}$ and $t \leq m-1$, where $m \in \mathbb{Z}_{>12^{2/\varepsilon}}$, then

$$\alpha(G) > \frac{\varepsilon}{4800}.\frac{n}{m}.\log m.$$

⌟

Proof: Cf.[note on Ramsey Numbers]. □

Independence Polynomials

Def. (25.2.5.8)[Independence Polynomials]. For $G \in \texttt{Graph}^{\text{fin}}$, the **independence polynomial** is defined to be

$$I(G) = \sum_{A \subset V(G), A \text{ independent}} X^{\#A} \in \mathbb{Z}[X].$$

⌟

Prop. (25.2.5.9). For any $G \in \texttt{Graph}^{\text{fin}}$ and $v \in V(G)$, $I(G) = I(G \setminus \{v\}) + XI(G \setminus N(v))$. ⌟

Prop. (25.2.5.10) [Independence Polynomials of Line Graphs are Real-Rooted]. If $G \in \texttt{Graph}^{\text{fin}}$ is claw-free, then $I(G)$ is real-rooted. In particular, the independence polynomial of a line graph is real-rooted. ⌟

Proof: Use induction on $v(G)$. The case $v(G) = 0$ is trivial, and if $v(G) > 0$, take $v \in V(G)$, then $I(G) = I(G\setminus\{v\}) + XI(G \setminus N(v))$. So to prove $I(G)$ is real-rooted, it suffices to prove that $I(G\setminus\{v\})$ and $XI(G \setminus N(v))$ has a common interlacing polynomial(3.3.3.14).

For this we use another induction on $v(G)$. The case $v(G) = 1$ is trivial, so suppose $v(G) \geq 2$. If $N(v) \setminus \{v\} = \varnothing$, then $I(G \setminus N(v)) = I(G \setminus \{v\})$, so the assertion is true. And if $N(v) \setminus \{v\} \neq 0$, let $n \in N(v) \setminus \{v\}$, then

$$I(G \setminus \{v\}) = I(G \setminus \{u, v\}) + XI(G \setminus (u \cup N(u))),$$

so by(3.3.3.14), it suffices to show that every pair of the polynomials

$$XI(G \setminus (u \cup N(u))), \quad XI(G \setminus (v \cup N(v))), \quad I(G \setminus \{u, v\})$$

has a common interlacing. The two pairs $(XI(G \setminus (u \cup N(u))), I(G \setminus \{u, v\}))$ and $(XI(G \setminus (v \cup N(v))), I(G\setminus\{u, v\}))$ are compatible by induction hypothesis. And for the pair $(I(G\setminus(u\cup N(u))), I(G\setminus (v \cup N(v))))$, let $H = G \setminus (\{u, v\} \cup N(u) \cup N(v))$, then it is easy to show that $N_H(u), N_H(v)$ are both simplicial cliques in H(25.2.5.2). So we can use lemma(25.2.5.11) to show that the pair $(I(G \setminus (u \cup N(u))), I(G \setminus (v \cup N(v))))$ has a common interlacing. □

Lemma (25.2.5.11). If $G \in \texttt{Graph}^{\text{fin}}$, and $I(H)$ is real-rooted for every induced subgroup H, then

- For any two simplicial cliques $K, L \subset V(G)$(25.2.5.2), the two polynomials $I(G \setminus K), I(G \setminus L)$ have a common interlacing polynomial.
- For any simplicial clique $K \subset V(G)$, the two polynomials $I(G), XI(G \setminus K)$ have a common interlacing polynomial.

⌟

Proof: The proof use induction on $v(G)$ for both assertions. The case $v(G) = 0$ is trivial. For $v(G) > 0$, we may assume $K \neq \varnothing$, and denote $H = G \setminus (K \cup L)$. Then

$$I(G \setminus L) = I(H) + \sum_{v \in K \setminus L} XI(H \setminus N_H(v)),$$

$$I(G \setminus K) = I(H) + \sum_{v \in L \setminus K} XI(H \setminus N_H(v)).$$

$$I(G) = I(G \setminus K) + \sum_{v \in K} XI(G \setminus N(v)).$$

So it suffices to show that every pair of the polynomials

$$\{XI(H \setminus N_H(v))\}_{v\in K\cup L}, \quad I(H)$$

has a common interlacing polynomial(3.3.3.14). These from from the induction hypothesis and(25.2.5.3). For assertion 2, it suffices to show that every pair of the polynomials

$$I(G \setminus K), XI(G \setminus K), \{XI(H \setminus N_H(v))\}_{v\in K}$$

has a common interlacing polynomial. The pair $(I(G \setminus K), XI(G \setminus K))$ follows from the hypothesis, The pairs $(I(G \setminus K), XI(H \setminus N_H(v)))$ have common interlacings by induction hypothesis and(25.2.5.3). The pairs $(XI(G \setminus K), XI(H \setminus N_H(v)))$ have common interlacings by induction hypothesis and(25.2.5.3). The family $\{XI(H \setminus N_H(v))\}_{v\in K}$ have common interlacings by induction hypothesis and(25.2.5.3). □

6 Planer Graphs

Def. (25.2.6.1) [Planer Graphs]. A **planer graph** is a graph $G \in \mathtt{Graph}$ that is embeddable in $\mathbb{R}^2$. ⌟

Prop. (25.2.6.2) [Plane Graphs]. When can a graph be embedded in $\mathbb{R}^2$.**?** ⌟

Proof: □

Prop. (25.2.6.3) [Euler]. Any finite planer graph $G \in \mathtt{Graph}^{\mathtt{simple}}$ satisfies $e(G) < 3v(G) - 6$. ⌟

Proof: □

Prop. (25.2.6.4) [Maximally Plane Graphs are Triangulations]. For any finite planer graph $G \in \mathtt{Graph}^{\mathtt{simple}}$ with $v(G) \geq 3$, G is maximally planer iff it is a planer triangulation. ⌟

Proof: Cf.[Diestel]P96. □

7 Flows

Def. (25.2.7.1) [Circulations]. A **circulation** on a finite multi-graph G is a function $f : \overrightarrow{E}(G) \to H$ where $H \in \mathcal{A}\mathrm{b}$, satisfying the following:

- For any $(e, x, y) \in \overrightarrow{E}(G)$, $f(e, x, y) = -f(e, y, x)$,
- (**Kirchhoff's law**)For any $x \in V(G)$,

$$\sum_{(e,x,y)\in \overrightarrow{E}(G)} f(e, x, y) = 0.$$

⌟

Def. (25.2.7.2). For a finite multi-graph G and and function $f : \overrightarrow{E}(G) \to H$ where $H \in \mathcal{A}\mathrm{b}$, for any two subsets $X, Y \subset V(G)$, denote

$$f(X, Y) = \sum_{(e,x,y)\in \overrightarrow{E}(G), x\in X, y\in \overline{Y}} f(e, x, y).$$

⌟

Def. (25.2.7.3) [Networks and Flows]. A **network** is a quadruple $N = (G, s, t, c)$ where G is a finite multi-graph, $s \neq t \in V(G)$, and $c : \overrightarrow{E}(G) \to \mathbb{N}$ a map called the **capacity function**. Then a **flow** on a network N is a function $f : \overrightarrow{E}(G) \to \mathbb{R}$ satisfying the following:

- For any $(e, x, y) \in \overrightarrow{E}(G)$, $f(e, x, y) = -f(e, y, x)$,
- For any $x \in V(G) \setminus \{s, t\}$,
$$\sum_{(e,x,y)\in\overrightarrow{E}(G)} f(e, x, y) = 0.$$
- $f(\overrightarrow{e}) \le c(\overrightarrow{e})$ for any $\overrightarrow{e} \in \overrightarrow{E}(G)$.

⌟

Def. (25.2.7.4) [Flow-Cuts]. For a flow f on a network $N = (G, s, t, c)$, a **flow-cut** is a pair $(S, \overline{S})$ where $S \subset V(G), \overline{S} = V(G) \setminus S, s \in S, t \in \overline{S}$, and $c(S, \overline{S}) = \sum_{(e,x,y)\in\overrightarrow{E}(G),x\in S,y\in\overline{S}} c(e, x, y)$ is called the **capacity of the cut**. ⌟

Prop. (25.2.7.5) [Total Values of Flows]. Given a flow f on a network $N = (G, s, t, c)$ for any flow-cut $(S, \overline{S})$, $f(S, \overline{S}) = f(s, V(G))$, called the **total value of the flow** f, denoted by $|f|$.

It is clear that $|f| \le c(S, \overline{S})$ for any flow-cut S. ⌟

Thm. (25.2.7.6) [Maximum Value and Minimum Capacity]. For any network $N = (G, s, t, c)$, the maximal total value of a flow on N equals the minimum value $c(S, \overline{S})$ for ay flow-cut S. Moreover, such a maximal flow can be integral-valued. ⌟

Proof: Let f be a flow with maximal total value. Let S be the set of all vertices $v \in V(G)$ s.t. there exists a path $x_0e_0x_1e_1 \ldots x_{k-1}e_kx_k$ from s to v with $f(e_i, x_i, x_{i+1}) < c(e_i, x_i, x_{i+1})$ for any $i \in [k-1]$.

If $t \in S$, suppose W is a shortest such path from s to t, and $\varepsilon = \min_{\overrightarrow{e}\in W}(c(\overrightarrow{e}) - f(\overrightarrow{e}))$, then we can modify f to add a value ε along the orientation of W. In this way, we get a flow with bigger $|f| = f(s, V)$, contradiction.

So $t \notin S$. Thus $(S, \overline{S} = V(G) \setminus S)$ is a flow-cut for N, and by the definition of S, $f(\overrightarrow{e}) = c(\overrightarrow{e})$ for any $\overrightarrow{e} \in \overrightarrow{E}(S, \overline{S})$. Thus $|f| = f(S, \overline{S}) = c(S, \overrightarrow{S})$. □

8 Extremal Graph Theory

Prop. (25.2.8.1) [Rademacher]. For any $n \in \mathbb{Z}_+$, any graph G with $\#V(G) = 2n, \#E(G) = n^2 + 1$ contains at least n triangles. ⌟

Proof:

□

Thm. (25.2.8.2) [Turán1941]. For any $r, n \in \mathbb{Z}_+, r > 1$, any $G \in \mathtt{Graph}^{\mathtt{simple}^n}$ not containing a subgraph K^r with $e(G) = \mathrm{Xtrm}(n, K_r)$ is isomorphic to $\mathrm{Tur}^{r-1}(n)$. ⌟

Proof: Cf.[Graph Theory, Diestel]P175. □

Thm. (25.2.8.3) [Erdös-Stone1946]. Given any $r, s \in \mathbb{Z}_+, r \ge 2$ and $\varepsilon \in \mathbb{R}_+$, then for $n \in \mathbb{Z}_+$ sufficiently large, any graph $G \in \mathtt{Graph}^{\mathtt{simple}}$ with $v(G) = n$ and $e(G) \ge t_{r-1}(n) + \varepsilon n^2$ contains K_s^r as a subgraph. ⌟

Proof: Cf.[Graph Theory, Diestel]P178.? □

Szemerédi's Regularity Lemma

Def. (25.2.8.4) [ε-Regular Pairs]. For $G \in \mathtt{Graph}^{\mathtt{simple}}$, two disjoint non-empty subsets $A, B \subset V(G)$ are called a **ε-regular pair** if for any $X \subset A, Y \subset B$ s.t. $\#X > \varepsilon\#A, \#Y > \varepsilon\#B$, we have

$$|d(X,Y) - d(A,B)| < \varepsilon.$$

⌟

Thm. (25.2.8.5) [Szeméredi's Regularity Lemma]. For any $\varepsilon \in \mathbb{R}_+$ and $m \in \mathbb{Z}_+$, there exists $M(\varepsilon, m), N(\varepsilon, m) \in \mathbb{Z}_+$ satisfying the following: For any graph $G \in \mathtt{Graph}^{\mathtt{simple}}$ with $v(G) \geq N(\varepsilon, m)$, there is a partition of $V(G)$ into $k+1$ classes

$$V(G) = V_0 \amalg V_1 \amalg \ldots \amalg V_k$$

where V_0 is called the **exceptional set**, s.t.

- $m \leq k \leq M(\varepsilon, m)$,
- $\#V_0 < \varepsilon v(G)$,
- $\#V_1 = \ldots = \#V_k$,
- All but at most εk^2 pairs of $(V_i, V_j), 1 \leq i < j \leq k$ are ε-regular pairs(25.2.8.4).

In other words, in some sense, every graph can be approximated by random graphs. ⌟

Proof: ? □

Cor. (25.2.8.6) [Szeméredi's Regularity Lemma, alternative forms]. For any $\varepsilon \in \mathbb{R}_+$, there exists $M(\varepsilon) \in \mathbb{Z}_+$ satisfying the following: For any graph $G \in \mathtt{Graph}^{\mathtt{simple}}$, $V(G)$ can be partitions into

$$V(G) = V_1 \amalg \ldots \amalg V_k$$

s.t.

- $\#V_i \leq \lceil \varepsilon v(G) \rceil$ for any i,
- $|\#V_i - \#V_j| \leq 1$ for any $1 \leq i < j \leq k$,
- All but at most εk^2 pairs of $(V_i, V_j), 1 \leq i < j \leq k$ are ε-regular pairs(25.2.8.4).

⌟

Proof: ? □

25.3 Graph Theory II

References are [Die17].

Notation (25.3.0.1).

- Use references as in Graph Theory I.

⌟

1 Random Graphs

Prop. (25.3.1.1) [Small Random Independent Sets]. Let $k \in \mathbb{Z}_+$ and let G_n be a random graph with each edge appearing with probability $p = 8k^2/n$, then

$$\lim_{n\to\infty} \mathbf{P}(\alpha(G_n) \geq \frac{k}{2n}) = 0.$$

⌟

Proof:

$$\mathbf{P}(\alpha(G_n) \geq n/(2k)) \leq \binom{n}{n/(2k)}(1 - 16k^2/n)^{\binom{r}{2}} \leq 2^n e^{-p(\frac{n}{2k})^2/2} \leq 2^n e^{-n},$$

which tends to 0 as n tends to ∞. □

<u>**Signed Adjacency Matrices**</u>

Prop. (25.3.1.2) [Signed Adjacency Matrices and Matching Polynomials, Godsil-Gutman]. For any $G \in \mathtt{Graph}$ and a choice of signing $s \in \{\pm 1\}^{E(G)}$ of the edges of G, then we can consider the signed adjacency matrices $A_{s,G}$ of G and the corresponding characteristic polynomials $f_s(G)$. Then

$$\mathbf{E}_{s\in\{\pm1\}^{E(G)}} f_s(G) = \mu_G(X).$$

⌟

Proof:

$$\begin{aligned}\mathbf{E}_{s\in\{\pm1\}^{E(G)}} f_s(G) &= \mathbf{E}[\sum_{\sigma\in \mathrm{Sym}([n]_+)} \mathrm{sgn}(\sigma)\prod_{i=1}^n (xI - A_{s,G})_{i,\sigma(i)}]\\ &= \sum_{k=0}^n x^{n-k}(-1)^k \sum_{S\subset[n]_+,\#S=k}\ \sum_{\pi\in\mathrm{Sym}(S)} \mathbf{E}[\mathrm{sgn}(\pi)\prod_{i\in S}(A_s)_{i,\pi(i)}]\\ &= \sum_{k\in 2\mathbb{N}, 0\leq k\leq n} x^{n-k} \sum_{S\subset[n]_+,\#S=k}\ \sum_{\pi\in\mathrm{Matching}(S)} (-1)^{k/2}\\ &= \mu_G(x)\end{aligned}$$

□

Prop. (25.3.1.3) [Random Adjacency matrices, Marcus-Spielman-Srivastava]. For any $G \in \mathtt{Graph}^{\mathtt{simple}}$ with an arbitrary ordering of $E(G)$, and any $p_1, \ldots, p_{e(G)} \in [0, 1]$, the expected value of the singed adjacency characteristic polynomial as in(25.3.1.2):

$$P(X) = \sum_{s\in\{\pm1\}^{E(G)}} \prod_{s_i=1} p_i \prod_{s_i=-1} (1 - p_i) f_s(X) \in \mathbb{R}[X]$$

is real-rooted. ⌟

Proof: Denote $d = \Delta(G)$. For any $s \in \{\pm 1\}^{E(G)}$ and $u \neq v \in V(G)$, denote by $s_{u,v}$ the value on the edge (u, v), and define $a^{\pm}_{u,v} = e_u \pm e_v$, $L^{\pm}_{u,v} = a^{\pm}_{u,v} a^t_{u,v}$. Then

$$d\mathbf{1} - A_s = \sum_{(u,v)\in E} a^{s_{u,v}}_{u,v} (a^{s_{u,v}}_{u,v})^t + D$$

where $D = \mathrm{diag}(d - d_1, \ldots, d - d_{e(G)})$.

Now

$$P(X + d) = \sum_{s\in\{\pm 1\}^{E(G)}} \prod_{s_i=1} p_i \prod_{s_i=-1} (1 - p_i) \det\Big(X\mathbf{1} + D + \sum_{(u,v)\in E(G)} a^{s_{u,v}}_{u,v} (a^{s_{u,v}}_{u,v})^t\Big),$$

which is real-rooted by(3.3.3.10). □

Cor. (25.3.1.4)[Signed Adjacency Characteristic polynomials are Interlacing, Marcus-Spielman-Srivastava]. For any $G \in \mathtt{Graph}^{\mathtt{simple}}$ with an arbitrary ordering of $E(G)$, the singed adjacency characteristic polynomials(25.3.1.2) form an interlacing family(3.3.3.16). ⌟

Proof: By(3.3.3.14), it suffices to show that for any $k \in [e(G)-1]_+$ and $s_1, \ldots, s_k \in \{\pm 1\}, \lambda \in \mathbb{R}_{\geq 0}$, the polynomial

$$\lambda f_{s_1,\ldots,s_k,1}(X) + (1 - \lambda) f_{s_1,\ldots,s_k,-1}(X)$$

is real-rooted. But this follows from(25.3.1.3). □

Thm. (25.3.1.5) [Minimal Eigenvalues of Signed Adjacency Characteristic Polynomials, Marcus-Spielman-Srivastava]. For any connected graph $G \in \mathtt{Graph}^{\mathtt{simple}}$ with universal covering T, there exists a signed adjacency characteristic polynomial $f_{s,G}$ of G(25.3.1.2) with all roots bounded above by $\rho(T)$. ⌟

Proof: This follows from(25.3.1.4)(3.3.3.18) and(25.3.1.2)(25.2.3.5). □

<u>Second Moment Method</u>

2 Coloring

Def. (25.3.2.1) [Colorings]. For $G \in \mathtt{Graph}$ and $k \in \mathbb{Z}_+$, a k-**vertex coloring** of G is a map $c : V(G) \to [k]_+$ s.t. $c(u) \neq c(v)$ for any any edge $e = (u, v) \in E(G)$.

A graph $G \in \mathtt{Graph}$ with a k-vertex coloring is called k-**colorable**. The infimum of $k \in \mathbb{Z}_+$ s.t. G is k-colorable is denoted by $\gamma(G)$, called the **chromatic number** of G.

Similarly, we can define **edge-colorings** of a graph as a vertex coloring of the line graph $L(G)$, and define the **edge-chromatic number** of G, denoted by $\gamma'(G)$. ⌟

Def. (25.3.2.2) [Chromatic Numbers]. For $G \in \mathtt{Graph}$, the **chromatic number** $\gamma(G) \in \mathbb{Z}_+ \cup \{\infty\}$ is the minimal number $n \in \mathbb{Z}_+$ s.t. $V(G)$ can be partitioned into n disjoint subsets $V = V_1 \amalg V_2 \amalg \ldots \amalg V_n$ s.t. if $x, y \in V_i(G)$ for some i, then $e(x, y) = 0$. ⌟

Def. (25.3.2.3) [Partite Graphs]. For $r \in \mathbb{Z}_{\geq 2}$, an r-**partite graph** is a graph G s.t. $V(G)$ has an r-partition $V = V_1 \amalg \ldots \amalg V_r$ s.t. vertices in a same partition class are not adjacent. 2-partite graphs are also called **bipartite graphs**.

A maximal r-bipartite graph $K_s * K_s * \ldots * K_s$ is denoted by K^r_s. ⌟

Prop. (25.3.2.4)[Bipartite Graphs and Odd Cycles]. A graph $G \in \mathtt{Graph}$ is bipartite iff it contains no odd cycles. ⌟

Proof: One direction is clear. For the other, let T be a spanning tree of G, with a root t. Then we can define a tree order on $V(G)$. Now $V(G)$ is partitions into two classes according to whether $v \in V(G)$ satisfies $d(t, v)$ is even.

This is truly a bipartite partition, because if an odd-distance vertex is adjacent to an even-distance vertex, then we get an odd cycle. □

Prop. (25.3.2.5) [Chromatic Numbers and Independent Sets]. For a finite graph $G \in \mathtt{Graph}^{\mathtt{simple}}$, $v(G) \leq i(G)\gamma(G)$. ⌟

Proof: Let $V(G) = V_1 \amalg \ldots \amalg V_{\gamma(G)}$ be a coloring of G, then each V_i is an independent set. Thus $\# V_i(G) \leq i(G)$. □

Prop. (25.3.2.6) [Chromatic Numbers and Minimal Degree]. For any $k \in \mathbb{Z}_+$, any k-chromatic graph $G \in \mathtt{Graph}^{\mathrm{fin}}$ has a k-chromatic subgraph H with $\delta(H) \geq k - 1$. ⌟

Proof: Cf.[Diestel]P123. □

Cor. (25.3.2.7). For any $G \in \mathtt{Graph}^{\mathrm{fin}}$, G contains a cycle of length at least $v(G)/\gamma(G)$. ⌟

Proof: This follows from(25.3.2.6) and(25.2.1.10). □

Prop. (25.3.2.8) [Coloring Numbers and Spectrums]. For $k \in \mathbb{Z}_{\geq 2}$ and a connected k-regular graph $G \in \mathtt{Graph}^{\mathtt{simple}}$ with $n = v(G) < \infty$, we have

$$i(G) \leq \frac{n}{k} \max\Big(|\lambda_1(G)|, |\lambda_{v(G)-1}(G)|\Big).$$

In particular, by(25.3.2.5),

$$\gamma(G) \geq \frac{k}{\max\Big(|\lambda_1(G)|, |\lambda_{v(G)-1}(G)|\Big)}.$$

⌟

Proof: Let $F \subset V(G)$ be a maximal independent set of G. Take $f \in \ell^2(V(G))$ s.t.

$$f(x) = \begin{cases} \# V(G) \setminus F & , x \in F \\ -\# F & , x \notin F \end{cases}.$$

Then $||f|| = \# F \cdot \# V(G) \setminus F \cdot \# V(G) \leq i(G)n^2$. And for any $x \in F$, $(Af)(x) = -ki(G)$. So $||Af||^2 \geq k^2 i(G)^3$.

Since $\sum_{v \in V(G)} f(v) = 0$, $||Af|| \leq \max(|\mu_1|, |\mu_{n-1}|)||f||$, so $ki(G)^{3/2} \leq \max(|\mu_1|, |\mu_{n-1}|) \cdot ni(G)^{1/2}$, which gives the desired result. □

Thm. (25.3.2.9)[Large Girth, Large Chromatic and Large minimal Degree Graphs, Erdös]. For any $k \in \mathbb{Z}_+$, there exists a finite graph $G \in \mathtt{Graph}^{\mathtt{simple}}$ with

$$g(H), \gamma(H), \delta(H) > k.$$

⌟

Proof: Assume $k \geq 3$. Fix $\varepsilon \in (0, 1/k)$ and n large, and consider the random graph G_n of size n with each edge appearing with probability $p = n^{\varepsilon-1}$. Then the expected value of number X of cycles with length$\leq k$ is

$$\mathbf{E}(X) = \sum_{i=3}^{k} \frac{n(n-1)\dots(n-i+1)}{2i} p^i \leq \frac{1}{2}\sum_{i=3}^{k} n^i p^i \leq \frac{k-2}{2} n^{k\varepsilon}.$$

Thus

$$\mathbf{P}(X \geq n/2) \leq \mathbf{E}(X)/(n/2) \leq (k-2)n^{k\varepsilon-1}.$$

So when n is large, $\mathbf{P}(X \geq n/2) \leq 1/2$. And notice $n^{\varepsilon-1} \geq 16k^2/n$ for n large, so by(25.3.1.1), when n is large, $\mathbf{P}(i(G_n) \geq n/(2k)) \leq 1/2$. Thus there is a graph G with $v(G) = n, i(G) < n/(2k)$, and has less than $n/2$ cycles of length$\leq k$.

Delete a vertex from each cycle of length$\leq k$ in G, and let H be the remaining graph, then $v(H) \geq n/2, g(H) > k$, and $\gamma(H) \geq v(H)/i(H) \geq \frac{1}{2}n/i(G) > k$(25.3.2.5).

Finally, we can make $\delta(G)$ large by restricting to a subgraph H, by(25.3.2.6). □

Thm. (25.3.2.10) [Vizing[Viz64]]. For any finite simple graph $G \in \mathtt{Graph}^{\mathtt{simple}}$, $\Delta(G) \leq \gamma'(G) \leq \Delta(G) + 1$. ⌟

Proof: $\Delta(G) \leq \gamma'(G)$ is clear. For the other inequality, use induction on $e(G)$: The case $e(G) = 0$ is trivial, and for $e(G) > 0$, for any $e = (x, y) \in E(G)$, there is a color of $G \setminus \{e\}$, and if there is a color α that is missing at x and a color β that is missing at y, then the maximal (β, α)-alternating path from y will end in x, otherwise we can switch α, β in the color of this maximal path, and color e with α.

Now let $xy_0 \in E(G)$, and let c_0 be the coloring of $G \setminus \{xy_0\}$, and let α be a color missing at x in the coloring c_0, and $c(1)$ be the color missing at y_0 in the coloring c_0. Then there may exists $xy_1 \in E(G)$ s.t. $c_0(xy_1) = c(1)$. Continuing this way, we find a maximal $k \in \mathbb{Z}_+$ s.t. there exists $xy_0, xy_1, \dots, xy_k \in E(G)$ s.t. $c(i) \overset{\triangle}{=} c_0(xy_i)$ is a color missing at y_{i-1} in the coloring c_0.

Then we can define colorings c_i of $G \setminus \{xy_i\}$ for each i: $c_i(e) = \begin{cases} c(i+1) & , e = xy_k, k \in [i] \\ c_0(e) & \text{otherwise} \end{cases}$.

Let β be a color missing at y_k in the coloring c_0, and consider the (β, α)-alternating path P from y_k ending at x. By maximality of k, this path ends with $y_k, \dots, y_i, x$ for some $i \in [k]$. Then $\beta = c(i+1)$, which is missing at y_i in the coloring c_0(thus also missing at y_i in the coloring c_k). Then in the coloring c_i, the (β, α)-path from y_i is just the reverse of P ending at y_k, and then cannot go further, contradiction. □

Prop. (25.3.2.11) [König1916]. For any bipartite graph $G \in \mathtt{Graph}^{\mathrm{fin}}$, $\gamma'(G) = \Delta(G)$. ⌟

Proof: Use induction on $e(G)$. The case $e(G) = 0$ is trivial. For $e(G) > 0$, take $e = (x, y) \in G$, and choose a $\Delta(G)$-coloring of $G' = G \setminus \{e\}$, which is possible by induction hypothesis. Then there exists $\alpha, \beta \in [\Delta(G)]_+$ s.t. x is not incident with an α-edge and y is no incident with an β-edge. If α can be chosen to be β, then a coloring of G is possible.

If $\alpha \neq \beta$, then x has an β-edge. Then we can extend this edge to a maximal (α, β)-alternating path W in G'. This path must be a simple path, and it cannot contain y, because in this way, it must end with an α-edge, making an odd cycle in G, contradicting the fact that G is bipartite. So we can now swap all the colors of edges in W, and then color e with β. This is a $\Delta(G)$-coloring of G. □

Prop. (25.3.2.12) [Csaba-Kühn-Lo-Osthus-Treglown2016]. There exists $n_0 \in \mathbb{Z}_+$ s.t. for any $n \in \mathbb{Z}_{n_0}$ and $d \in \mathbb{Z}_{\geq n/2}$, any d-regular graph $G \in \texttt{Graph}$ with $v(G) = n$ satisfies $\gamma'(G) = \Delta(G)$. ⌟

Proof: □

Tutte Polynomial

Def. (25.3.2.13) [Tutte Polynomials]. The **Tutte polynomial** of a multi-graph G is defined to be $T_G(q, v) =$**?**. ⌟

Prop. (25.3.2.14). For any $G \in \texttt{Graph}$ and $q \in \mathbb{Z}_+$, the number of ways of coloring vertices of G with no two vertices of the same color connected is just $T_G(q, -1)$. ⌟

Proof: Cf.[The Knot Book, Adams]P233.**?** □

List Colorings

Def. (25.3.2.15) [List Colorings]. For $k \in \mathbb{Z}_+$, a graph $G \in \texttt{Graph}$ is called k-**choosable** iff for any family of subsets $S_v \subset \mathbb{N}$ indexed by $V(G)$, there is a map $c : V(G) \to \mathbb{N}$ s.t. $c(v) \in S_v$ for any $v \in V(G)$, and $c(u) \neq c(v)$ for any any edge $e = (u, v) \in E(G)$. The infimum of $k \in \mathbb{Z}_+$ s.t. G is k-choosable is denoted by $\mathrm{ch}(G)$, called the **choice number** of G.

Similarly, we can define **edge-list-colorings** of a graph as a vertex coloring of the line graph $L(G)$, and define the **edge-choice number** of G, denoted by $\mathrm{ch}'(G)$.

Clearly, $\mathrm{ch}(G) \geq \gamma(G), \mathrm{ch}'(G) \geq \gamma'(G)$. ⌟

Prop. (25.3.2.16)[Bondy-Boppana-Siegel]. If $H \in \texttt{Graph}^{\mathrm{fin}}$ be an oriented graph s.t. every induced subgraph has a kernel(25.2.1.5), and $\{S_v\}_{v \in V(H)}$ is a family of lists(25.3.2.15) s.t. $\deg^+(v) < \#S_v$ for any $v \in V(H)$, then H can be colored from the list S_v. ⌟

Proof: Use induction on $v(H)$. $v(H) = 0$ is trivial, and for $v(H) > 0$, take $\alpha \in \cup_v S_v$, and let H' be the subgraph induced by vertices $v \in V(H)$ s.t. $\alpha \in S_v$. Then H' has a kernel $U \neq \varnothing$. Now color U with α. Then the graph $H \setminus U$ can be colored from the list $\{S'_v\}_{v \in V(H)}$, where $S'_v = S_v \setminus \{\alpha\}$, by induction hypothesis and the definition of a kernel. Thus H can also be colored from the list S_v. □

Conj. (25.3.2.17) [List Coloring Conjecture]. For any $G \in \texttt{Graph}$, $\mathrm{ch}'(G) = \gamma'(G)$. ⌟

Proof: □

Thm& Conj.Cor. (25.3.2.18) [Bipartite Graphs, Galvin[Gal95]]. For any bipartite graph $G \in \texttt{Graph}$, $\mathrm{ch}'(G) = \gamma'(G) = \Delta(G)$. ⌟

Proof: The second equality follows from(25.3.2.11). For the first, it suffices to show that $\mathrm{ch}'(G) \leq \gamma'(G)$. Let $G = X \amalg Y$ where X, Y are independent subset of G. Assume $k = \gamma'(G) < \infty$, and let c be a k-coloring.

We define an orientation on $L(G)$ as follows: For any two adjacent edges $e, e' \in E(G)$ s.t. $c(e) < c(e')$, assign $e < e'$ if e, e' meet in X, and $e > e'$ if e, e' meet in Y. In this way, $\deg^+(e) > k$ for any $e \in E(G)$.

Notice this orientation also defines a linear preference on $E(G)$(25.2.3.2), thus any induced subgraph of $L(G)$ has a kernel by the stable matching theorem(25.2.3.3). Now it follows from(25.3.2.16) that $L(G)$ is k-choosable. □

Planer Graphs

Thm. (25.3.2.19) [4-Coloring Problem, Appel-Haken1977]. Every planer graph is 4-colorable. ⌟

Proof: ?Cf.[N. Robertson, D. Sanders, P.D. Seymour and R. Thomas1977]. □

Thm. (25.3.2.20) [3-Coloring Theorem, Grötzsch1959]. Every Planer graph not containing a triangle is 3-colorable. ⌟

Proof: □

Thm. (25.3.2.21) [Alon1993]. For any $k \in \mathbb{N}$, there exists $f(k) \in \mathbb{N}$ s.t. any graph $G \in \texttt{Graph}$ with $d(G) \geq f(k)$ satisfies $\mathrm{ch}(G) \geq k$. ⌟

Proof: □

Thm. (25.3.2.22) [5-Choice Theorem, Thomassen[Tho94]]. Any planer graph is 5-choosable. ⌟

Proof: It suffices to prove for finite maximally planer graphs $G \in \texttt{Graph}^{\texttt{simple}}$. By(25.2.6.4), G is a graph triangulation, so this follows from the following excellently tailored lemma:

Lemma (25.3.2.23). Let G be a planer graph s.t. $v(G) \geq 3$, its interiors is triangularized, and its boundary is a cycle $C = v_1 v_2 \ldots v_k v_1$. Then given any family of subsets $S_v \subset \mathbb{N}$ indexed by $V(G)$ s.t. $\#S_v \leq 5$, and $\#S_v \leq 3$ if $v \in C$, and given $c_1 \in S_{v_1}, c_2 \in S_{v_2}$, there is a map $c: V(G) \to \mathbb{N}$ s.t. $c(1) = c_1, c(2) = c_2$, $c(v) \in S_v$ for any $v \in V(G)$, and $c(u) \neq c(v)$ for any any edge $e = (u, v) \in E(G)$. ⌟

Proof: Use induction on $v(G)$. The case $v(G) = 3$ is trivial. And for $v(G) \geq 4$, if there is an arc vw in G, then we can use induction hypothesis on the two parts divided by vw and get the desired result for G. If instead there are no arcs in G, let $v_1, u_1, u_2, \ldots, u_m, v_{k-1}$ be the neighborhoods of v_k with their clockwise orientation around v_k. Now choose two elements $a, b \in S_{v_k}$ distinct to c_1, and delete a, b from $S_{u_1}, \ldots, S_{u_m}$. Then the resulting family is a family for the graph $G' = G \setminus \{v_k\}$ that satisfies the induction hypothesis, thus there is a choice function $c: V(G) \setminus \{v\} \to \mathbb{N}$. Now either a or b are different from $c(v_{k-1})$, so we can define $c(v_k)$ to be this number. □

□

Remark (25.3.2.24). This is strict because Voigt(1993) constructed a plane graph of order 238 that is not 4-choosable. ⌟

3 Cayley Graphs

Def. (25.3.3.1) [Cayley Graphs]. For $G \in \mathcal{G}\mathrm{rp}$ and $S \subset G$ s.t. $k \overset{\triangle}{=} \#S < \infty$ and $S = S^{-1}$, the **Cayley graph** is a graph $\mathrm{Cay}(G, S) \in \texttt{Graph}$ s.t.

$$V(\mathrm{Cay}(G, S)) = G, \quad E(\mathrm{Cay}(G, S)) = \{(x, y) \in G^2 | y^{-1}x \in S\}.$$

Then

- $\mathrm{Cay}(G, S)$ is a k-regular.
- $\mathrm{Cay}(G, S)$ is connected iff S generates G.
- If there is a homomorphism $\chi: G \to \mathbb{Z}/(2)$ s.t. $\chi(S) = \{1\}$, then $\mathrm{Cay}(G, S)$ is bipartite. The converse is also true if S generates G.

⌟

Proof: 3: One direction is clear. For the other direction, if S generates G, by item2, G is connected, so we can use the bipartition to define χ using the parity of distances. □

4 Perfect Graphs

Def. (25.3.4.1) [Perfect Graphs]. A **Perfect graph** is a finite simple graph G s.t. for any induced subgraph $H \subset G$, the maximal cardinality of a clique of H equals the chromatic number of H. ⌟

Def. (25.3.4.2) [Berge Graphs]. A finite simple graph G is called a **Berge graph** if it doesn't contain holes or antiholes(25.2.1.21) of odd cardinality. ⌟

Thm. (25.3.4.3) [Perfect Graph Theorem, Chudnovsky-Robertson-Seymour-Thomas]. A simple finite graph G is perfect iff it is Berge. ⌟

Proof:

□

5 Triangulated Graphs

6 Interval Graphs

7 Graph Minors

Conj. (25.3.7.1) [Self-Minor Conjecture, Seymour]. Every countably-infinite graph is a proper minor of itself(i.e. the minor is not an identity). ⌟

Proof:

□

Thm& Conj.Cor. (25.3.7.2) [Graph Minor Theorme, Robertson-Seymour 1986–2004]. The minor relation on the set of finite graphs is a quasi-well-ordering. ⌟

Proof: Clearly there cannot be an infinite decreasing minor sequence of finite graphs, so by(2.2.3.19), it suffices to show that there cannot be an infinite set of non-comparable finite graphs. This follows from the self-minor conjecture, because by considering the disjoint union of the graphs.

Alternatively, ? □

Lemma (25.3.7.3) [Kruskal1960]. The root-preserving topological minor relation on the set of finite rooted trees is a quasi-well-ordering. ⌟

Proof: Clearly there cannot be an infinite decreasing topological minor sequence of finite rooted trees, so by(2.2.3.19), it suffices to show that there cannot be an infinite set of non-comparable finite rooted trees.

Suppose the contrary, and we can choose a bad sequence $(T_i)_{i\in\mathbb{N}}$ of finite rooted trees s.t. for any $n \in \mathbb{N}$, T_n is a tree of minimum order s.t. $(T_0, T_1, \ldots, T_n)$ extends to a bad sequence. Let r_n be root of T_n, and let A_n be the set of trees of the forest $T_n \setminus \{r_n\}$. Then we claim that $A = \cup_n A_n$ is quasi-well ordered by the root-preserving topological minor relation:

Let (T^k) be a sequence of trees in A, and find a smallest $n \in \mathbb{N}$ s.t. $T^k \in A_n$ for some k. Then $T^k \subsetneq T_n$, and

$$T_0, \ldots, T_{n-1}, T^k, T^{k+1}, \ldots$$

is not a bad sequence by the choice of T_n. Let (T, T') be an ascending pair, then T cannot be in $(T_0, \ldots, T_{n-1})$, as then we will have $T \le T' \le T_{n'}$, but $n' \ge n$, so $(T, T_{n'})$ is an ascending pair in $(T_i)_{i\in\mathbb{N}}$, contradiction. Thus (T, T') is an ascending pair in (T^k), which is what we want to prove.

Now by(2.2.3.20), the sequence $(A_n)_{n\in\mathbb{N}} \in [A]^{<\aleph_0}$ has an ascending pair $A_i \le A_j$ where $i < j$. Let $f : A_i \to A_j$ be injective with $T \le f(T)$ for any $T \in A_i$, then we get a root-preserving injection $T_i \to T_j$. Thus $T_i \le T_j$, contradiction. □

8 Lifts of Graphs

Def. (25.3.8.1) [Double Covers of Graphs]. For any simple graph $G \in \mathtt{Graph}^{\mathtt{simple}}$, the **double covering** of G is the graph $\widetilde{G} = (\widetilde{V}, \widetilde{E})$ where $\widetilde{V} = V(G) \times \{\pm 1\}$, and

$$\widetilde{E} = \{(v_1, \varepsilon_1, v_2, \varepsilon_2) \in \widetilde{V}(G)^2 | (v_1, v_2) \in E(G), \varepsilon_1 \neq \varepsilon_2\}.$$

It is a bi-partite graph, and $\widetilde{G} \to G$ is a covering map. ⌟

Def. (25.3.8.2) [Signing of a 2-Lifting]. For any simple graph $G \in \mathtt{Graph}^{\mathtt{simple}}$, the **signed 2-lift** of G with signing $s : E(G) \to \{\pm 1\}$ is the graph $\widetilde{G}_s = (\widetilde{V}_s, \widetilde{E}_s)$ s.t. $\widetilde{V}_s = E(G) \times \{\pm 1\}$, and

$$\widetilde{E}_s = \{(v_1, \varepsilon_1, v_2, \varepsilon_2) \in \widetilde{V}(G)^2 | (v_1, v_2) \in E(G), \varepsilon_1 \begin{cases} = \varepsilon_2 & , s(v_1, v_2) = 1 \\ \neq \varepsilon_2 & , s(e(v_1, v_2)) = -1 \end{cases}\}.$$

It is a bi-partite graph, and $\widetilde{G} \to G$ is a covering map. ⌟

Thm. (25.3.8.3) [Spectrums of Signed 2-Lifts, Bilu-Linial]. For any simple graph $G \in \mathtt{Graph}^{\mathtt{simple}}$ with signing $s : E(G) \to \{\pm 1\}$, the spectrum of the signed 2-lift of G w.r.t. s is the sum of the spectrum of G and the spectrum of the signed adjacency matrix $A_{s,G}$ of G(25.3.1.2). ⌟

Proof: It is not hard to see that the adjacency matrix of $\widetilde{G}_s$ is $\widetilde{A} = \begin{bmatrix} A_1 & A_2 \\ A_2 & A_1 \end{bmatrix}$, where $A_1 = (V(G), s^{-1}(1))$, and $A_2 = (V(G), s^{-1}(-1))$, $A = A_1 + A_2$, $A_s = A_1 - A_2$.

Then it is easy to see that if v is an eigenvector of A with eigenvalue λ, then (v, v) is an eigenvector of $\widetilde{A}$ with eigenvalue λ, and if u is an eigenvector of A_s with eigenvalue μ, then $(u, -u)$ is an eigenvector of $\widetilde{A}$ with eigenvector μ. As these vectors are linearly independent, the result follows. □

9 Expander Graphs

References are [DSV03].

Def. (25.3.9.1) [Expanding Constants]. For $G \in \mathtt{Graph}$, the **expanding constant** of G is defined to be

$$h(G) = \inf_{F \subset V(F), \# F < \infty} \Big(\frac{e(F, V(G) \setminus F)}{\min(\# F, \#(V(G) \setminus F))} \Big).$$

⌟

Prop. (25.3.9.2) [Cheeger – Buser Inequlity, Dodziuk/Alon-Milman]. Let $k \in \mathbb{Z}_{\geq 2}$ and $G \in \mathtt{Graph}^{\mathtt{simple}}$ be a finite connected k-regular graph with $n \overset{\triangle}{=} v(G)$, and the spectrum of M_G are $\mu_0 \geq \mu_1 \ldots \geq \mu_{n-1}$, then

$$\frac{k - \mu_1}{2} \leq h(X) \leq \sqrt{2k(k - \mu_1)}.$$

⌟

Proof: Take an arbitrary orientation of G, and consider the the coboundary functor $d : \ell^2(V(G)) \to \ell^2(E(G)) : df(e) = f(e^+) - f(e^-)$, and its adjoint $d^* : \ell^2(E(G)) \to \ell^2(V(G))$. Then $d^* d = L_G = k\mathbf{1} - A_G$. The spectrum of L_G is $0, k - \lambda_1, \ldots, k - \lambda_{n-1}$. So for any $f \in \ell^2(V(G))$ s.t. $\sum_{v \in V(G)} f(v) = 0$, we have $|df|_2^2 = \langle L_G f, f \rangle \geq (k - \lambda_1)|f|_2^2$.

Now for any $F \subset V(G)$, consider $f \in \ell^2(V) : f(x) = \begin{cases} \#(V \setminus F) & , x \in F \\ -\#F & , x \notin F \end{cases}$. Then $\sum_{v \in V(G)} f(v) = 0$, and $|f|_2^2 = n\#F\#(V \setminus F)$. And

$$df(e) = \begin{cases} \pm n & , e \in E(F, V \setminus F) \\ 0 & , \text{otherwise} \end{cases}.$$

So $|df|_2^2 = n^2 e(F, V \setminus F)$. The the inequality above applied to f implies that

$$e(F, V \setminus F) \geq (k - \lambda_1)\frac{\#F \cdot \#V \setminus F}{n} \geq \frac{k - \lambda_1}{2}\min(\#F, \#V \setminus F).$$

This proves the lower hound for $h(F)$.

For the upper bound: For any $f \in \ell^2(V(G))$, define $B_f = \sum_{e \in E(G)} |f(e^+)^2 - f(e^-)^2|$, then

Lemma (25.3.9.3).

- If $\beta_r > \beta_{r-1} > \ldots > \beta_0$ are the values of f, and let $L_i = f^{-1}([\beta_i, \infty))$, then $B_f = \sum_{i=1}^r e(L_i, V(G) \setminus L_i)(\beta_i^2 - \beta_{i-1}^2)$.
- $B_f \leq \sqrt{2k}|df|_2|f|_2$.
- If $\#\operatorname{Supp}(f) \leq n/2$, then $B_f \geq h(G)|f|_2^2$.

⌟

Proof: 1: This is clear.

2:

$$B_f = \sum_{e \in E(G)} |f(e^+) + f(e^-)|.|f(e^+) - f(e^-)| \leq \sqrt{\sum_{e \in E(G)} (f(e^+) + f(e^-))^2} \cdot \sqrt{\sum_{e \in E(G)} (f(e^+) - f(e^-))^2} \leq \sqrt{2k}|df|_2|f|_2.$$

3: The hypothesis implies that $\#L_i \leq n/2$ for any i, thus $e(L_i, V(G) \setminus L_i) \geq h(G)\#L_i$. Thus

$$B_f = \sum_{i=1}^r e(L_i, V(G) \setminus L_i)(\beta_i^2 - \beta_{i-1}^2) \geq h(G)\sum_{i=1}^r \#L_i(\beta_i^2 - \beta_{i-1}^2) = h(G)|f|_2^2.$$

□

Now consider an eigenvalue g for L_G with eigenvector $k - \lambda_1$, and let $V^+ = \{x \in V | g(x) > 0\}$, $f = \max(g, 0)$. We may assume $0 < \#V^+ \leq n/2$. Then for $x \in V^+$,

$$L_G f(x) = kg(x) - \sum_{y \in V^+} A_{xy} g(y) \leq kg(x) - \sum_{y \in V} A_{xy} g(y) = (k - \lambda_1)g(x).$$

So

$$|df|_2^2 = \langle L_G f, f \rangle = \sum_{x \in V^+} L_G f(x) g(x) \leq (k - \lambda_1) \sum_{x \in V^+} g(x)^2 \leq (k - \lambda_1)|f|_2^2.$$

Combining this and the lemma above, we get

$$h(x)|f|_2^2 \leq B_f \leq \sqrt{2k}|df|_2|f|_2 \leq \sqrt{2k(k - \lambda_1)}|f|_2^2,$$

which implies $h(x) \leq \sqrt{2k(k - \lambda_1)}$. □

Def. (25.3.9.4) [Expander Graphs]. For $k \in \mathbb{Z}_{\geq 2}$, a family of k-regular finite simple graphs $(X_n) \in \mathtt{Graph}^{\mathbb{Z}_+}$ is called a family of **expander graphs** if $\varinjlim v(X_n) = \infty$, and $\inf_n h(X_n) > 0$, or equivalently by (25.3.9.2), $\inf_n(k - \mu_1(X_n)) > 0$. ⌟

Ramanujan Graphs

References are [DSV03] and [L-S88].

Def. (25.3.9.5) [Ramanujan Graphs]. A **Ramanujan graph** is a finite connected graph $G \in \texttt{Graph}^{\text{fin}}$ with universal covering T s.t. for any eigenvalue λ_i of G, either $|\lambda_i| = \lambda_1$, or $|\lambda_i| \leq \rho(T)$.

In particular, by(25.2.2.9), for any $c, d \in \mathbb{Z}_{\geq 2}$, a finite connected (c,d)-bi-regular graph has trivial eigenvalues $\pm\sqrt{cd}$, so it is a **Ramanujan bi-regular graph** iff all its non-trivial eigenvalues λ_i satisfy $|\lambda_i| \leq \sqrt{c-1} + \sqrt{d-1}$. ⌟

Cor. (25.3.9.6). For a k-regular non-bi-partite Ramanujan graph G, $\gamma(G) \geq \frac{k}{2\sqrt{k-1}} \geq \frac{\sqrt{k}}{2}$, by(25.3.2.8). ⌟

Conj. (25.3.9.7) [Bilu-Linial]. For any $c, d \in \mathbb{Z}_{\geq 3}$ and any (c,d)-bi-regular graph G, there is a signing of a 2-lift(25.3.8.2) such that the new eigenvalues all have absolute value $\leq \sqrt{c-1} + \sqrt{d-1}$. ⌟

Proof: □

Thm& Conj.Cor. (25.3.9.8) [Marcus-Spielman-Srivastava]. For any $c, d \in \mathbb{Z}_{\geq 3}$ and any (c,d)-bi-regular graph G, there is a signing of a 2-lift such that the new eigenvalues are all bounded above by $\sqrt{c-1} + \sqrt{d-1}$. ⌟

Proof: Then the universal cover T of G is a (c,d)-bi-regular tree, which has spectrum radius $\rho(T) = \sqrt{c-1} + \sqrt{d-1}$ by(25.2.2.9). Thus the assertion follows from(25.3.1.5) and(25.3.8.3). □

Cor. (25.3.9.9) [Lubotzky-Phillips-Sarnak/Margulis/Chiu/Lubotzky/Marcus-Spielman-Srivastava]. For any $c, d \in \mathbb{Z}_{\geq 3}$, there exists an infinite family of (c,d)-bi-regular Ramanujan graphs. ⌟

Proof: This follows from consecutively using(25.3.9.8) on any (c,d)-bi-regular Ramanujan graph G, for example a complete (c,d)-bi-regular graph(because its spectrum is $\{\sqrt{cd}, -\sqrt{cd}, 0, 0, \ldots, 0\}$). □

Explicit Constructions

Def. (25.3.9.10) [$S_{p,q}$]. Let $p \neq q \in \texttt{Prime}_{\geq 3}$ s.t. $q \geq 2\sqrt{p}$, then $\mathbb{H}(\mathbb{F}_q) \cong \text{Mat}(2; \mathbb{F}_q)$. Fix such an isomorphism ψ_p.

Let $S_p \subset \mathbb{H}(\mathbb{Z})$ be a distinguished set of elements of norm p, $\#S_p = p+1$(**?** Cf.[Sarnak, Ramanujan Graph book]P68). Define

$$S_{p,q} = \psi_q(S_p) \subset \text{PGL}(2; \mathbb{F}_q),$$

then $\#S_{p,q} = p+1$, and $S_{p,q} \subset \text{PSL}(2; \mathbb{F}_q)$ iff $\left(\frac{p}{q}\right) = 1$. ⌟

Proof: Cf.[Sarnak, Ramanujan Graph book]P113.**?**

For the last assertion, notice $x \in \text{GL}(2; \mathbb{F}_q)$ mapsto $\text{PSL}(2; \mathbb{F}_q)$ iff $\det(x) \in \mathbb{F}_q^2$, so $S_{p,q} \subset \text{PSL}(2; \mathbb{F}_q)$ iff $\left(\frac{p}{q}\right) = 1$. □

Thm. (25.3.9.11) [$X^{p,q}$]. Let $p \neq q \in \texttt{Prime}_{\geq 3}$ s.t. $q \geq 2\sqrt{p}$, we can define

$$X^{p,q} = \begin{cases} \text{Cay}(\text{PSL}(2; \mathbb{F}_q), S_{p,q}) & , \left(\frac{p}{q}\right) = 1 \\ \text{Cay}(\text{PGL}(2; \mathbb{F}_q), S_{p,q}) & , \left(\frac{p}{q}\right) = -1 \end{cases}.$$

Then $X^{p,q}$ is a $(p+1)$-regular connected Ramanujan graph, and for fixed p, this forms a large girth family(25.2.1.17). In fact,

- If $\left(\frac{p}{q}\right) = -1$, then $X^{p,q}$ is bipartite, $v(X^{p,q}) = q(q^2-1)$, and $g(X^{p,q}) \geq 4\log_p q - \log_p 4$.
- If $\left(\frac{p}{q}\right) = 1$, then $X^{p,q}$ is not bipartite, $v(X^{p,q}) = q(q^2-1)/2$, and $g(X^{p,q}) \geq 2\log_p q$.

⌟

Proof:

□

10 Potential Theory on Graphs

Riemann-Roch on Graphs

References are [B-N07].

Conj. (25.3.10.1). Is there is a Serre duality for graphs?

Is there an analogy of Hirzebruch – Riemann – Roch theorem for higher-dimensional simplicial complexes?

Is there a relation between Riemann-Roch theorems for tropical varieties/toric varieties/graphs?

⌟

Proof:

□

11 Zeta Functions

Def. (25.3.11.1)[Ihara Zeta Functions]. For a finite unoriented graph $G \in \mathtt{Graph}^{\mathrm{fin}}$, the **Ihara zeta function** is defined to be

$$Z(u,G) = \prod_{\mathfrak{p}\in P}(1-u^{\mathrm{length}(\mathfrak{p})})^{-1},$$

where P is the set of primes circuits in G(25.2.1.19).

Similarly we can define zeta function $Z^o(u,G)$ of an oriented graph.

WARNING: the zeta function of a graph and its duplication oriented graph, because of the primality condition. ⌟

Prop. (25.3.11.2). For a finite oriented graph $G \in \mathtt{Graph}^{\mathrm{fin}}$ and $m \in \mathbb{Z}_+$, let N_m be the number of circuits in G of length m with an endpoint, then

$$Z^o(u,G) = \exp\Big(\sum_{m\in\mathbb{Z}_+}\frac{N_m}{m}u^m\Big) = \det(1-uM_G)^{-1}.$$

In particular, it is a rational function. ⌟

Proof: The first equation is easy by taking log. For the second equation, because $N_m = \mathrm{tr}(M_G^m)$, let the eigenvalues of M_G be $\lambda_1,\ldots,\lambda_n$, then using an triangulation of M_G,

$$\exp\Big(\sum_{m\in\mathbb{Z}_+}\frac{N_m}{m}u^m\Big) = \exp\Big(\sum_{m\in\mathbb{Z}_+}\frac{1}{m}\sum_{i=1}^n\lambda_i^m u^m\Big) = \prod_{i=1}^n\exp(-\log(1-\lambda_i u)) = \det(1-uM_G)^{-1}.$$

□

Cor. (25.3.11.3). For $G \in \texttt{Graph}^{\text{fin}}$, G is bipartite iff $Z(u, G)$ is an even function. ⌟

Proof: Since the vertices $v \in V(G)$ s.t. $\deg(v) = 1$ doesn't affect the result, we can discard them. Then the assertion follows easily from(25.3.2.4). □

Prop. (25.3.11.4) [Edge Zeta Functions]. For a finite unoriented graph $G \in \texttt{Graph}^{\text{fin}}$, consider its **line graph** G_L where

$$V(G_L) = \overrightarrow{E}(G), \quad E(G_L) = \{(e_1, e_2) \in \overrightarrow{E}(G) \times \overrightarrow{E}(G), e_1 \neq \overline{e}_2, t(e_1) = s(e_2)\}.$$

Then it is easy to see that

$$Z(u, G) = Z^o(u, G_L).$$

⌟

Thm. (25.3.11.5) [Bass]. For a finite connected unoriented graph $G \in \texttt{Graph}^{\text{fin}}$ s.t. $\deg(v) \geq 2$ for any $v \in G$, we have

$$Z(u, G) = (1 - u^2)^{\chi(G)} \det(\mathbf{1} - uA + u^2(D - \mathbf{1}))^{-1}.$$

⌟

Proof: Cf.[Zeta functions of finite graphs]. □

Cor. (25.3.11.6) [Regular Graphs]. Let $q \in \mathbb{Z}_+$ and $G \in \texttt{Graph}$ a finite connected k-regular graph, then

$$Z(u, G) = (1 - u^2)^{(1-q)v(G)/2} \det((1 + qu^2)\mathbf{1} - uA)^{-1}.$$

In particular, by(25.2.2.3),

- $$\text{Pole}(Z(u, G)) \subset [q^{-1}, 1] \cup [-1, -q^{-1}] \cup \{|z| = q^{-1/2}\}.$$
- $u = -q^{-1}$ is a pole iff G is bipartite.
- $\text{Pole}(Z(u, G)) \subset \{|z| = q^{-1/2}\} \cup \{\pm 1, \pm q^{-1}\}$ iff G is a Ramanjan graph(25.3.9.5).

⌟

Prop. (25.3.11.7) [Northshield]. For a finite connected oriented graph $G \in \texttt{Graph}^{\text{fin}}$ s.t. $\deg(v) \geq 2$ for any $v \in G$,

$$\lim_{u \to 1} \frac{Z(u, G)}{(1 - u)^{\chi(G) - 1}} = \frac{2^{\chi(G) - 1}}{\chi(G)\,\text{tree}(G)}.$$

⌟

Proof: Let $f(u) = \det(\mathbf{1} - uA + u^2(D - \mathbf{1})|\ell^2(V(G)))$, then by(25.3.11.5), it suffices to prove that

$$f`(1) = -2\chi(G)\,\text{tree}(G).$$

Let $M(u) = \mathbf{1} - uA + u^2(D - \mathbf{1})$, and let M_k be the result of M derivating the k-th row. Then $M_k(1) = M(1) + (\deg(v_k) - 2)e_{kk}$. So

$$\frac{\partial}{\partial u} \det(M(u))|_{u=1} = \sum_k [\det M(1) + (\deg(v_k) - 2) \det \widetilde{M}_{kk}],$$

where M_{kk} is the (k, k)-th cofactor of $M(1)$. But by (25.2.2.7), $\det \widetilde{M}_{kk} = \text{tree}(G)$, so the result follows. □

12 Applications

Thm. (25.3.12.1) [Monsky]. A square cannot be divided into m triangles of the same area, where m is odd. ⌟

Proof: Choose a 3-coloring on $\mathbb{R}^2$: By(14.2.1.28) there can be an extended 2-adic valuation $|\cdot|_2$ on $\mathbb{R}$ that extends the 2-adic valuation on $\mathbb{Q}$, then color a point (x, y)

- 0 if $|x|_2 < 1, |y|_2 < 1$,
- 1 if $|x|_2 \geq 1$ and $|x|_2 \geq |y|_2$.
- 2 if $|y|_2 \geq 1$ and $|y|_2 > |x|_2$.

Then there are two things:

1. The coloring is invariant under translation by vectors represented by a point of color 0.
2. The valuation of the area of a triangle with vertices of 3 different colors is bigger than 1, because we can assume one vertex is the origin, and then its area is $\frac{1}{2}|x_1y_2 - x_2y_1|$, which, because the coloring, must have 2-adic valuation bigger than 1.

Now back to the question, let the square be placed as a unit square, then its area is 1, and it has exactly one $(0, 1)$-edge, so by Spencer's lemma(25.2.1.28), it has a triangle with vertices of pairwise different colors, so its area A has valuation> 1, but the total area is $mA = 1$ that has valuation 1, so $|m| < 1$, which means that m is even. □

Prop. (25.3.12.2) [Hindman's Theorem]. Whenever $\mathbb{N}$ is colored with f.m. colors, one can find an infinite subset $A \subset \mathbb{N}$ and a color c that whenever $F \subset A$ is finite, the color of the sum of numbers in F is colored c. ⌟

Proof: Cf.[W. W. Comfort, Ultrafilters: some old and some new results, Bull. Amer. Math. Soc. 83 (1977) 417–455.] □

25.4 Combinatorial Set Theory

Def. (25.4.0.1) [Notations]. For a set S, let $[S]^r$ be the set of subsets of S of order r. Let κ, λ be cardinals, we write $\kappa \to (\lambda)^r_s$ as a shorthand for: for any set S with $|S| = \kappa$ and every partition of $[S]^r$ into s classes, there exists a subset $H \subset S$ that $[H]^r$ is in the same class, and $|H| \geq \lambda$. ⌟

Prop. (25.4.0.2) [Ramsey's Theorem for $\aleph_0$]. For any positive natural number r, s if we color the r-subsets of a set with cardinality $\aleph_0$ into s families, then there is a subset of cardinal $\aleph_0$ that all its r-subsets are colored the same. ⌟

Proof: Cf.[Graph Theory, Thm9.1.2]. □

Cor. (25.4.0.3). Every infinite linearly ordered set contains a subset isomorphic to $(\mathbb{N}, <)$ or $(\mathbb{N}, >)$. ⌟

Proof: Choose a well ordering of it. Then consider this new ordering and the original ordering. Then there is an infinite set that is compatible with the original ordering, or converse. Then its initial segment of order type ω_0 satisfies the requirement. □

Def. (25.4.0.4) [Weakly Compact Cardinals]. An **weakly compact cardinal** is an uncountable cardinal κ that $\kappa \to (\kappa)^r_s$(25.4.0.1) for any $r, s \in \mathbb{Z}_+$. ⌟

Prop. (25.4.0.5). Weakly compact cardinals are strongly inaccessible. ⌟

Proof: Cf.[Jec03]P224. □

Trees

Def. (25.4.0.6). A **tree** is a partial ordered set T that there is a minimal element r and for each x, $\{y \in T | y < x\}$ is finite and linearly ordered.

A tree is called **of finite branched** for each x, there is a finite set $\{y_1, \ldots, y_r\}$ is T that $y_i > x$ and if $z > x$, then $z \geq y_i$ for some i.

⌟

Def. (25.4.0.7) [Height]. For any node x, $\{y \in T | y < x\}$ is a well-ordered set, which is isomorphic to an ordinal by(2.2.4.7), it is called the **height** of x. T_α denotes the set of all nodes of T of order α. The least α that $T_\alpha \neq \varnothing$ is called the **height** of T.

A **branch** is a maximal chain in T, its **length** is its ordinal. The length is always smaller than the height of the tree. If it equals the height of the tree, it is called **cofinal**. ⌟

Def. (25.4.0.8). A **subtree** is a subset T' of T that if $x \in T', y < x$, then $x \in T'$.

An **antichain** of a tree T is a subset $A \subset T$ that any two elements in A are incomparable. ⌟

Def. (25.4.0.9). A **path** through T is a morphism of ordering from ω to T. ⌟

Lemma (25.4.0.10) [König's Lemma]. If T is an infinite finite branching tree, then there is a path through T. ⌟

Proof: Use recursion to choose for each n an element that has infinite successors. □

Def. (25.4.0.11). An **Aronszajn tree** is a tree of height κ and all its level sets are at most countable, but has no branches of length κ. ⌟

Prop. (25.4.0.12). An **Aronszajn tree** of height ω_1 exists. ⌟

Proof: Cf.[Set Theory Jech P228]. □

1 Finite Sets

Thm. (25.4.1.1) [Dirichlet's Box Principle]. ⌟

Proof: □

2 Finite Ramsey's Theory

Thm. (25.4.2.1) [Finite Ramsey's Theorem]. For any $\alpha, k, n_1, \ldots, n_k \in \mathbb{Z}_+, n_i \geq \alpha$, there exists a minimal $R(\alpha, k; n_i) \in \mathbb{Z}_+$ s.t. if we divide the α-subsets of a set with cardinality $R(\alpha, k; n_i)$ into k groups $C_1, \ldots, C_k$, then there is some $1 \leq i \leq k$ and a subset S of cardinality n_i s.t. all the α-subset of S is in C_i. Moreover,

$$R(\alpha, k; n_i) \leq R(\alpha - 1, k; m_j = R(\alpha, k; n_1, \ldots, n_{j-1}, n_j - 1, n_{j+1}, \ldots, n_k)) + 1.$$

⌟

Proof: We use double induction on (α, k) in lexicographical order. If $\alpha = 1$, clearly $R(1, k; n_i) = \sum_{i=1}^{k}(n_i - 1) + 1$. And if $k = 1$, then $R(\alpha, 1; n_1) = n_1$.

Suppose $\alpha > 1, k > 1$, if some $n_i = \alpha$, then $R(\alpha, k; n_i) = R(\alpha, k - 1; n_1, \ldots, \widehat{n_i}, \ldots, n_k)$, thus we are reduced to smaller k. So we can assume that $n_i > \alpha$ for each i. In this case, we prove that

$$R(\alpha, k; n_i) \leq R(\alpha - 1, k; m_j = R(\alpha, k; n_1, \ldots, n_{j-1}, n_j - 1, n_{j+1}, \ldots, n_k)) + 1.$$

And this will finish the induction process.

To prove this, notice that if we have a set X with cardinality equal to the RHS, and let $x \in X$, then we can divide the $(\alpha - 1)$ subsets of $X \setminus \{x\}$ into k groups $C'_1, \ldots, C'_k$ s.t. an $(\alpha - 1)$-set S has cardinality $\alpha - 1$ belongs to C'_i iff $S \cup \{x\}$ belongs to C_i. Then by definition, there exists some i and some subset Y of $X \setminus \{x\}$ of cardinality $R(\alpha, k; n_1, \ldots, n_{i-1}, n_i - 1, n_{i+1}, \ldots, n_k)$ s.t. all $(\alpha - 1)$-subset of Y belongs to C'_i. Then by definition, there either exists some $j \neq i$ and some subset Z_1 of Y of cardinality n_j s.t. all the α-subset of Z_1 is in C_j, in which case the assertion is satisfied; or exists some subset Z_2 of Y of cardinality $n_i - 1$ s.t. all the α-subset of Z_2 is in C_i. Then $Z_2 \cup \{x\}$ satisfies the assertion. □

Prop. (25.4.2.2) [Szekeres]. For any $a, b \in \mathbb{Z}_{\geq 2}$, $R(2; a, b) \leq \binom{a+b-2}{a-1}$. ⌟

Proof: Use induction on $a + b$: If $a = 2$ or $b = 2$, this is easy. And for $a, b \geq 3$, by(25.4.2.1),

$$R(2; a, b) \leq R(2; a - 1, b) + R(2; a, b - 1) \leq \binom{a+b-3}{a-2} + \binom{a+b-3}{a-1} = \binom{a+b-2}{a-1}$$

□

Prop. (25.4.2.3) [Erdös]. For $k \in \mathbb{Z}_{\geq 3}$,

$$2^{k/2} < R(2; k, k) \leq \binom{2k-2}{k-1} < 4^{k-1}.$$

⌟

Proof: If $N < 2^{k/2}$, then the number of different graphs of N vertices equals $2^{N(N-2)/2}$, and the number of different graphs containing a complete k-graph is less than

$$\binom{N}{k}2^{N(N-1)/2-k(k-1)/2} < \frac{N^k}{k!}2^{N(N-1)/2-k(k-1)/2} < \frac{2^{N(N-1)/2}}{2},$$

because $2^{\frac{k}{2}+1} < k!$ for $k \geq 3$. So there exists a graph G that neither G and its complement graph G' contains a complete k-graph. Thus $2^{k/2} < R(2; k, k)$.

The second inequality follows form(25.4.2.2). □

Prop. (25.4.2.4) [Erdös]. There exists $C \in \mathbb{R}_+$ s.t.

$$R(2; 3, x) \geq Cx^2/\log^2 x$$

for any $x \in \mathbb{Z}_+$. ⌟

Proof: [Graph theory and Probability 2, Erdös]. □

Prop. (25.4.2.5) [Ajtai-Komlós-Szeméredi]. For any $k \in \mathbb{Z}_{\geq 2}$, there exists $C_k \in \mathbb{R}_+$ s.t. for $x \in \mathbb{Z}_+$ sufficiently large,

$$R(2; k, x) \leq 5000\frac{x}{\log(R(2; k-1, x)^{\frac{1}{k-2}})}.R(2; k-1, x).$$

In particular, there exists $C'_k \in \mathbb{R}_+$ s.t.

$$R(2; k, x) \leq C'_k x^{k-1}/\log^{k-2} x.$$

⌟

Proof: Cf.[note on Ramsey numbers].**?**

$k = 2$ is trivial. For $k \in \mathbb{Z}_{\geq 3}$, let $\varepsilon \in (\frac{0.96}{k-2}, \frac{1}{k-2})$. Suppose G is a graph with

$$n = \#V(G) \geq 5000\frac{x}{\log(R(2; k-1, x)^{\frac{1}{k-2}})}.R(2; k-1, x)$$

and $\omega(G) < k$ and $\alpha(G) \geq x$. Let $h(G)$ be the number of triangles in G.

Suppose $\deg(P) \geq R(2; k-1, x)$ for some $P \in V(G)$, then $\omega(G) \geq k$ or $\alpha(G) \geq x$, contradiction. So $\deg(P) < R(2; k-1, x)$ for any $P \in V(G)$, which implies that $t = 2\#E(G)/n < R(2; k-1, x)$.

If $h(G) < nR(2; k-1, x)^{2-\varepsilon}$, when x is large, $R(2; k, x)$ is large, so by(25.2.5.7),

$$\alpha(G) > \frac{\varepsilon}{4800}.\frac{n}{R(2; k-1, x)}.\log R(2; k-1, x) \geq x,$$

contradiction.

Thus when x is large, we can assume that $h(G) \geq nR(2; k-1, x)^{2-\varepsilon}$, thus some point $P \in V(G)$ belongs to at least $R(2; k-1, x)^{2-\varepsilon}/3$ triangles. Because $\deg(P) < R(2; k-1, x)$, there exists a point Q adjacent to P and $\deg(Q) > 2R(2; k-1, x)^{1-\varepsilon}/3 > R(2; k-2, x)$ by hypothesis on ε. Then we can find a clique of size $k-2$ that is adjoint to P and Q, contradiction. □

Erdös-Hajnal Cnnjecture

Conj. (25.4.2.6) [Erdös-Hajnal]. For any finite graph $H \in \mathtt{Graph}^{\text{fin}}$, there exists $\delta_H \in \mathbb{R}_+$ s.t. for any graph $G \in \mathtt{Graph}^{\text{fin}}$, if H is not an induced subgroup of G, then $\max(\omega(G), i(G)) \geq v(G)^{\delta_G}$. ⌟

Proof: □

3 Intersection Theorems

References are [EKR61] and [G-M16].

Prop. (25.4.3.1) [Sperner]. For $n \in \mathbb{Z}_+$, any system $\{S_1, \ldots, S_v\}$ of subsets of $[n]_+$ s.t. no set S_i contains another S_j, then $v \le \binom{n}{\lfloor n/2 \rfloor}$. ⌟

Proof: □

Thm. (25.4.3.2) [Erdös-Ko-Rado/Wilson]. For $k, n, t \in \mathbb{Z}_+$ s.t. $n \ge (t+1)(k-t+1)$ and any system $\mathcal{S} = \{S_1, \ldots, S_v\} \subset \mathscr{P}([n]_+)$ s.t.

- $\#S_i = k$ for each i,
- $\#S_i \cap S_j \ge t$ for any $1 \le i, j \le v$,

we have $v \le \binom{n-t}{k-t}$.

Moreover, if $n \ge (t+1)(k-t+1)+1$, then $v \le \binom{n-t}{k-t}$ iff $\mathcal{S}$ consists of all k-subsets containing a fixed subset of cardinality t. ⌟

Proof: Use counting by twice method: For any permutation σ of $[n]_+$, let $A_s^\sigma = \{\sigma(s), \sigma(s+1), \ldots, \sigma(s+k-1)\}$(where addition is modulo n), then it can be seen easily that among the subsets $\{A_1^\sigma, \ldots, A_n^\sigma\}$, at most k of them are contained in $\mathcal{S}$. Thus by counting twice,

$$\frac{\#\mathcal{S}}{\binom{n}{k}} \le \frac{k}{n},$$

which implies $\#\mathcal{S} \le \frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}$.

For equality**?**, Cf.[Wilson, Exact Bound on Erdös-Ko-Rado theorem] or [Erdös-Ko-Rado theorem]Chap8. □

Conj. (25.4.3.3) [Erdös-Ko-Rado]. For $r \in \mathbb{Z}_+$ and any system $\mathcal{S} = \{S_1, \ldots, S_v\} \subset \mathscr{P}([4r]_+)$ s.t.

- $\#S_i = 2r$ for each i,
- $\#S_i \cap S_j \ge 2$ for any $1 \le i, j \le v$,

we have $v \le \frac{1}{2}\binom{4r}{2r} - \frac{1}{2}\binom{2r}{r}^2$. ⌟

Proof: □

Thm. (25.4.3.4)[Hilton-Milner[H-M67]]. For $k, n \in \mathbb{Z}_+, n \ge 2k$ and any system $\mathcal{S} = \{S_1, \ldots, S_v\} \subset \mathscr{P}([n]_+)$ s.t.

- $\#S_i = k$ for each i,
- $\#S_i \cap S_j \ne \varnothing$ for any $1 \le i, j \le v$.
- $\bigcap_i S_i = \varnothing$,

we have $v \le \binom{n-1}{k-1} - \binom{n-k-1}{k-1} + 1$. ⌟

Proof: Cf.[Erdös-Ko-Rado theorem]P15. □

Conj. (25.4.3.5) [Erdös-Ko-Rado]. For $k \le n \in \mathbb{Z}_+$ and any system $\mathcal{S} = \{S_1, \ldots, S_v\} \subset \mathscr{P}([n]_+)$ s.t. $\#S_i \cap S_j \ge k$ for any $1 \le i, j \le v$, find the largest value of v. ⌟

Proof: □

Prop. (25.4.3.6) [Erdös-Ko-Rado]. For $n \in \mathbb{Z}_{\geq 2}$ and any system $\mathcal{S} = \{S_1, \ldots, S_v\} \subset \mathscr{P}([n]_+)$ s.t. $S_i \cap S_j \cap S_k \neq \varnothing$ for any $1 \leq i, j, k \in v$, then we have $v \leq 2^{n-1}$, with equality iff $\mathcal{S}$ consists of all subsets containing a fixed element. ⌟

Proof: The inequality is clear. Consider the smallest $p \in [v]_+$ s.t.

$$S_1 \cap S_2 \ldots \cap S_p \in \{S_1, \ldots, S_v\}.$$

If $p = n$, then they have a common element. If $p < n$, then

$$\{S_1 \cap S_2 \ldots \cap S_{p+1}, S_1, \ldots, S_v\}$$

is another class s.t. any two of them has non-empty intersection. This implies that $v + 1 < 2^{n-1}$. □

25.5 Partition Theory

References are [The Theory of Partitions, Andrews].

Def. (25.5.0.1) [Partitions]. For $n \in \mathbb{Z}_+$, a **partition** of n is a tuple $(a_1, \ldots, a_k) \in \mathbb{Z}_+^{\mathbb{Z}_+}$ s.t.

$$a_1 \leq a_2 \ldots \leq a_k, \quad \sum_i a_i = n.$$

The number of partitions of n is denoted by $\mathrm{Par}(n)$. For convenience, denote $\mathrm{Par}(0) = 1$, and $P(\alpha) = 0$ for $\alpha \in \mathbb{R} \setminus \mathbb{N}$. Clearly,

$$\sum_{n \in \mathbb{N}} \mathrm{Par}(n) X^n = \prod_{k \in \mathbb{Z}_+} (1 - X^k)^{-1} \in \mathbb{Z}[[X]].$$

⌟

Thm. (25.5.0.2) [Ramanujan's most Beautiful Identity].

$$\sum_{n \in \mathbb{N}} \mathrm{Par}(5n+4) X^n = 5 \prod_{k \in \mathbb{Z}_+} \frac{(1 - X^{5k})^5}{(1 - X^k)^6} \in \mathbb{Z}[[X]].$$

⌟

Proof: □

1 Congruences between Partition Functions

Thm. (25.5.1.1) [Ramanujan Congruences]. For any $n \in \mathbb{Z}_+$,

$$5 | \mathrm{Par}(5n+4),$$

$$7 | \mathrm{Par}(7n+5),$$

$$11 | \mathrm{Par}(11n+6).$$

⌟

Proof: 1 follows from(25.5.0.2).
2:
3: □

Prop. (25.5.1.2) [Ahlgren-Boylan]. A **Ramanujan congruence** is a congruence property of the partition function of the form: For any $n \in \mathbb{Z}_+$,

$$p | \mathrm{Par}(pn + r)$$

where $p \in \texttt{Prime}, r \in \mathbb{Z}$. Then the only Ramanujan congruences are those three listed in(25.5.1.1). ⌟

Proof: □

Prop. (25.5.1.3) [Atkin-O'Brien]. For any $n \in \mathbb{Z}_+$,

$$13 | \operatorname{Par}(11^3 \cdot 13n + 237).$$

⌟

Thm. (25.5.1.4) [Schinzel/Ono]. For any $p \in \texttt{Prime} \setminus \{3\}$ and $k \in \mathbb{Z}_+$, a positive portion of primes $\ell \in \texttt{Prime}$ satisfy

$$p | \operatorname{Par}(\frac{p^k \ell^3 n + 1}{24}).$$

⌟

Proof: Cf.[Distribution of the partition function modulo m]. □

Prop. (25.5.1.5) [Ono]. For any $p \in \texttt{Prime}_{\geq 5}$, there exists $N(p), P(p) \in \mathbb{Z}_+, N(p), P(p) \leq 8(m^3 - 2m - 1)$ s.t. for any $i \in \mathbb{Z}_{\geq N(p)}$,

$$\operatorname{Par}(\frac{p^i n + 1}{24}) \equiv \operatorname{Par}(\frac{p^{P(p)+i} n + 1}{24}) (\bmod\ p).$$

⌟

Proof: Cf.[Distribution of the partition function modulo m, Ono]. □

Conj. (25.5.1.6) [Newmann]. For any $M \in \mathbb{Z}_+$ and $r \in \mathbb{Z}$, there are infinitely many $n \in \mathbb{Z}_+$ s.t.

$$\operatorname{Par}(n) \equiv r (\bmod\ m).$$

⌟

Proof: □

Thm& Conj.Cor. (25.5.1.7) [Schinzel/Ono/Ahlgren-Boylan]. For any $p \in \texttt{Prime}_{\geq 5}$ and $r \in \mathbb{Z}_+$, there exists $C(p, r) \in \mathbb{R}_+$ s.t.

$$\#\{n \in \mathbb{Z}_+ : n \leq X, \operatorname{Par}(n) \equiv r (\bmod\ p)\} \geq \begin{cases} C(p,r)\sqrt{X}/\log X & , 1 \leq r \leq p-1 \\ C(p)X & , r = 0, p \geq 5 \\ C(p)\sqrt{X} & , p = 2 \end{cases}.$$

⌟

Proof: Cf.[Distribution of the partition function modulo m, Ono], [Arithmetic properties of the partition function], [On the parity of additive representation functions, Nicolas-Ruzsa-Sárközy]. □

Remark (25.5.1.8). What about $p = 3$**?**. ⌟

25.6 Additive Combinatorics

1 Zero-Sum Sets

Def. (25.6.1.1) [Davenport Numbers]. For $G \in \mathcal{A}\mathrm{b}^{\mathrm{fin}}$, define the **Davenport number** $D(G)$ to be the smallest positive integer s s.t. any sequence of G of length s has a non-empty subsequence whose elements product to $1 \in G$. ⌟

Thm. (25.6.1.2) [Emde-Kruyswijk/Meshulam]. For $G \in \mathcal{A}\mathrm{b}^{\mathrm{fin}}$ and let m be the largest order of an element of G, then

$$D(G) \leq \lceil m(1 + \log \frac{\#G}{m})\rceil.$$

⌟

Proof: Let $n \geq m(1 + \log \frac{\#G}{m})$ and let $g_1, \ldots, g_n$ be a sequence of elements in G. □

Prop. (25.6.1.3). For $G \in \mathcal{A}\mathrm{b}^{\mathrm{fin}}$ and $r > t \geq D(G)$, any sequence of elements of G of cardinality r contains at least $\binom{r}{t}/\binom{r}{D(G)-1}$ many distinct sequences of length at most t and at least $t - D(G) + 1$ s.t. its elements product to $1 \in G$. ⌟

Proof: □

Zero-Sum Sets of Prescribed Sizes

Prop. (25.6.1.4) [Cauchy-Davenport]. If A, B are two nonempty subsets of $\mathbb{F}_p$, then $|A + B| \geq \min\{p, |A| + |B| - 1\}$. ⌟

Proof: If $|A| + |B| > p$, then this is trivial, because $A \cap (B - x) \neq \varnothing$ for all x.

Now if $|A| + |B| \leq p$, and if $A + B \subset C$ with $|C| = |A| + |B| - 2$, define $f = \prod_{c\in C}(x + y - c)$, then $f(a, b) = 0$ for all $a \in A, b \in B$, but the coefficient of the highest degree term $x^{|A|-1}y^{|B|-1}$ is $C^{|A|-1}_{|A|+|B|-2} \neq 0$, so this contradicts combinatorial Nullstellensatz(3.3.1.6). □

Cor. (25.6.1.5). Any element of $\mathbb{F}_p$ is a sum of two squares, as there are $\frac{p+1}{2}$ squares. ⌟

Cor. (25.6.1.6) [Erdös-Ginzburg-Ziv]. For any $2n - 1$ elements (a_i) in $\mathbb{Z}/(n)$, there exists $I \subset \{1, 2, \ldots, 2n - 1\}$ with $\#I = n$ and $\sum_{i\in I} a_i = 0$. ⌟

Proof: We use induction on n. If $n \in \mathbf{P}$, then this follows from Cauchy-Davenport(25.6.1.4). If this is true for m, then for $p \in \mathbf{P}$ and $n = mp$, given any $2n - 1$ numbers, we can find pairwise disjoint subsets $I_1, \ldots, I_{2m-1}$ of $\{1, \ldots, 2pm - 1\}$ where $\#I_i = p$ and $\sum_{j\in I_i} a_j \equiv 0 (\mathrm{mod}\ p)$ for any $1 \leq i \leq 2m - 1$. Define

$$A_i = (\sum_{j\in I_i} a_j)/p,$$

then we can use the induction hypothesis for m and A_i to get the desired assertion. □

2 Arithmetic Progressions

Arithmetic Progressions in $\mathbb{Z}_+$

Thm. (25.6.2.1) [Salem-Spencer/Behrend]. Given $\varepsilon \in \mathbb{R}_+$, for $N \in \mathbb{Z}_+$ sufficiently large, there exists a subset $S \subset \mathbb{Z}/N$ that avoids three-term arithmetic sequences, with

$$\#S > N^{1-\frac{2\sqrt{2\log 2}+\varepsilon}{\sqrt{\log N}}}.$$

⌟

Proof: For this N, let $n = \lfloor\sqrt{\frac{2\log N}{\log 2}}\rfloor$, and $d \in \mathbb{Z}_+$ s.t. $(2d-1)^n \leq N < (2d+1)^n$. Then $d \geq 2$. Then for any $k \leq n(d-1)^2$, consider the set $S_k(n,d)$ of all positive integers of the form

$$A = a_1 + a_2(2d-1) + \ldots + a_n(2d-1)^{n-1},$$

where $0 \leq a_i \leq d-1$, and $\sum_i a_i^2 = k$.

It follows from triangular inequlity that the image of any such $S_k(n,d)$ in $\mathbb{Z}/(N)$ avoids three-term arithmetic sequences, and by Dirichlet's box principle, there exists some $1 \leq k \leq n(d-1)^2$ s.t.

$$\#S_k(n,d) \geq (d^n-1)/n(d-1)^2 \geq d^{n-2}/n \geq \frac{(N^{\frac{1}{n}}-1)^{n-2}}{n(2+\varepsilon)^{n-2}} = \frac{N^{1-2/n}}{n(2+\varepsilon)^{n-2}}.$$

So for N large,

$$\#S_k(n,d) \geq N^{1-\frac{2}{n}-\frac{\log n}{\log N}-\frac{(n-2)\log(2+\varepsilon)}{\log N}} > N^{1-\frac{2\sqrt{2\log 2}+3\varepsilon}{\sqrt{\log N}}}.$$

□

Thm. (25.6.2.2) [Erdös-Turán Conjecture, Szeméredi/Gowers]. For any $k \in \mathbb{Z}_+$ and $\delta \in \mathbb{R}_+$, if $N \in \mathbb{Z}_+$ and $N \geq 2^{2^{(\delta^{-1})^{2^{2^{k+9}}}}}$, then any subset $A \subset [N]_+$ with $\#A \geq \delta N$ contains an arithmetic sequence of length k. ⌟

Proof: ? □

Cor. (25.6.2.3) [Roth]. For $X \in \mathbb{Z}_+$, let $A(X)$ be the maximal set of a subset of $[X]_+$ that avoids three-term arithmetic sequences, then

$$\frac{A(X)}{X} = O(\frac{1}{\log\log X}).$$

⌟

Proof: We give Roth's proof for this special case.

Let $b(X) = A(2^{4^X})/2^{4^X}$, then $b(X)$ is decreasing by(25.6.2.4), and(25.6.2.5) applied to $m = 2^{4^X}$ implies that if $\delta = \frac{1}{2^{4^{X+1}}\eta}$ where $0 < \eta < 1/2$, then

$$b(X)^2 < C[b(X)\delta + b(X)^2\delta^2 + (\delta^{-1}b(X)+1)(b(X)-b(X+1)+\frac{1}{2^{4^x}})].$$

Then notice for X large, we can choose $\delta = \delta(X) = \frac{b(X)}{2C_1} < \frac{1}{2}$ where $C_1 > \min(C,1)$ is a constant: it suffices to verify that $\frac{1}{2^{4^{X+1}}\cdot\frac{1}{2}} < \frac{b(X)}{2C}$, or equivalently $C < 2^{3\cdot 4^X-2}A(2^{4^X})$, which is clearly true for X large.

Thus by the fact $b(X) < 1$,

$$\begin{aligned} b(X)^2 &< C_1[b(X)\delta + b(X)^2\delta^2 + (\delta^{-1}b(X)+1)(b(X)-b(X+1)+\frac{1}{2^{4^x}})] \\ &\le b(X)^2(\frac{1}{2}+\frac{1}{4C_1}) + C_1(\delta^{-1}b(X)+1)(b(X)-b(X+1)+\frac{1}{2^{4^x}}) \\ &< \frac{3}{4}b(X)^2 + C_1(2C_1+1)(b(X)-b(X+1)+\frac{1}{2^{4^x}}) \end{aligned}$$

Thus there exists a constant C_2 s.t. for X large,

$$b(X)^2 < C_2(b(X)-b(X+1)+\frac{1}{2^{4^x}}).$$

which implies there exists a constant $C_3 > C_2$ that for X large,

$$Xb(2X)^2 \le \sum_{k=X}^{2X-1} b(X)^2 < C_3(b(X)-b(2X)+\frac{2C_3}{X}).$$

Hence whenever $2Xb(2X) > 4C_3$,

$$2Xb(2X) < \frac{1}{4C_3}4X^2b(2X)^2 < (Xb(X)-Xb(2X)+2C_3) < Xb(X).$$

From this that the fact $b(X)$ is decreasing(25.6.2.4) it is clear that $Xb(X)$ is bounded, i.e. $b(X) = O(\frac{1}{X})$. And clearly this together with(25.6.2.4) implies the desired assertion. □

Lemma (25.6.2.4). For any $X, Y \in \mathbb{Z}_+$, $A(X)$ equals the maximal number of elements without three-term arithmetic sequences that can be selected from any X-term arithmetic sequence. $\frac{A(XY)}{XY} \le \frac{A(X)}{X}$, and $\frac{A(X)}{X} \le \frac{X+Y}{X}\frac{A(Y)}{Y}$. ┘

Proof: The first assertion is easy. Thus $A(X+Y) \le A(X) + A(Y)$, and

$$A(X) \le A(\Big[1+\lfloor\frac{X}{Y}\rfloor\Big]Y) \le \frac{X+Y}{X}A(Y).$$

□

Lemma (25.6.2.5) [Hardy-Littlewood Method]. For $X \in \mathbb{Z}_+$, let $a(X) = \frac{A(X)}{X}$, then for any $m \in 2\mathbb{Z}_+$, if $\delta = \frac{1}{m^4\eta}$ where $0 < \eta < 1/2$, there exists constant $C > 0$

$$a(m)^2 < C[a(m)\delta + a(m)^2\delta^2 + (\delta^{-1}a(m)+1)(a(m)-a(m^4)+m^{-1})].$$

┘

Proof: Let $\{u_1, \dots, u_{A(m^4)}\}$ be a maximal subset of $\{m^4\}$ without three-term arithmetic sequences, and let $\{2v_1, \dots, 2v_V\}$ be the set of even integers among u_k. Then by(25.6.2.4),

$$A(m^4) \le m^4a(m), \quad V \le A(\frac{m^4}{2}) \le \frac{m^4}{2}a(m), \quad V \ge A(m^4) - A(\frac{m^4}{2}) \ge m^4a(m^4) - \frac{m^4}{2}a(m).(\star)$$

Define

$$f_1(\alpha) = \sum_{k=1}^{A(m^4)} e^{2\pi\,\mathrm{i}\,\alpha u_k}, \quad f_2(\alpha) = \sum_{k=1}^{V} e^{2\pi\,\mathrm{i}\,\alpha v_k},$$

$$F_1(\alpha)=a(m)\sum_{n=1}^{m^4}e^{2\pi\,\mathrm{i}\,\alpha n},\quad F_2(\alpha)=a(m)\sum_{n=1}^{m^4/2}e^{2\pi\,\mathrm{i}\,\alpha n},$$

then by the above, $|f_i(\alpha)|\le m^4a(m),\quad |F_i(\alpha)|\le m^4a(m)$. And

$$f_i(\alpha)-F_i(\alpha)=O\Big(m^4[a(m)-a(m^4)]+m^3\Big)(\star\star):$$

Using(25.6.2.6), if $q=1$, this is true for $i=1$, and for $i=2$, use the lower bound for V above. On the other hand, if q cannot be chosen to be 1, then $S'=0$, and it suffices to show that $F_r(\alpha)=O(m^3)$, which is true by(14.1.1.1) and the fact $\{\{\alpha\}\}\ge 1/\sqrt{2N}$(because q cannot be chosen to be 1).

Thus

$$\begin{aligned}f_1(\alpha)f_2(-\alpha)^2-F_1(\alpha)F_2(-\alpha)^2&=f_1(\alpha)(f_2(-\alpha)+F_2(-\alpha))(f_2(-\alpha)-F_2(-\alpha))+F_2(-\alpha)^2(f_1(\alpha)-F_1(\alpha))\\&=O\Big([m^4a(m)]^2(m^4[a(m)-a(m^4)]+m^3)\Big).\end{aligned}$$

and by(14.1.1.1), if $0<\eta<\{\{\alpha\}\}<1/2$, then

$$f_1(\alpha)=O\Big(a(m)\eta^{-1}+m^4[a(m)-a(m^4)]+m^3\Big).(\star\star\star)$$

Then for any $0<\eta<1/2$,

- The hypothesis implies that $u_h=v_k+v_l$ iff $k=l$ and $u_h=2v_k$, so by $(\star)$

$$\int_{-\eta}^{1-\eta}f_1(\alpha)f_2^2(-\alpha)\mathrm{d}\alpha=V=O(m^4a(m)).$$

- By $(\star\star\star)$,

$$\int_{\eta}^{1-\eta}f_1(\alpha)f_2(-\alpha)^2\mathrm{d}\alpha<[\max_{\eta<\alpha<1-\eta}f_1(\alpha)]\int_0^1f_2(-\alpha)^2\mathrm{d}\alpha=O\Big(\Big[a(m)\eta^{-1}+m^4[a(m)-a(m^4)]+m^3\Big]m^4a(m)\Big).$$

- By $(\star\star)$ and(14.1.1.1),

$$\begin{aligned}\int_{-\eta}^{\eta}f_1(\alpha)f_2^2(-\alpha)\mathrm{d}\alpha&=\int_{-\eta}^{\eta}F_1(\alpha)F_2^2(-\alpha)\mathrm{d}\alpha+O\Big(\eta[m^4a(m)]^2(m^4[a(m)-a(m^4)]+m^3)\Big)\\&=\int_{-1/2}^{1/2}F_1(\alpha)F_2^2(-\alpha)\mathrm{d}\alpha+O(a(m)^3\eta^{-2})+O\Big(\eta[m^4a(m)]^2(m^4[a(m)-a(m^4)]+m^3)\Big)\\&=a(m)^3m^8/4+O(a(m)^3\eta^{-2})+O\Big(\eta[m^4a(m)]^2(m^4[a(m)-a(m^4)]+m^3)\Big)\end{aligned}$$

And these three estimates give the desired assertion. □

Lemma (25.6.2.6). Let $M\in\mathbb{Z}_+$ and $A=\{u_1,\dots,u_U\}$ be a subset of $[M]_+$ without three-term arithmetic sequences. For any $\alpha\in\mathbb{R}$, by Dirichlet's box principle, there exists $h,q\in\mathbb{Z}$ s.t.

$$\alpha=\frac{h}{q}+\beta,\quad (h,q)=1,1\le q\le\sqrt{M},\quad q|\beta|<1/\sqrt{M}.$$

Thus for any $m\in\mathbb{Z}_+,m<M$, we can define

$$S=S(\alpha)=\sum_{k=1}^{U}e^{2\pi\,\mathrm{i}\,\alpha u_k},\quad S'=S'(\alpha,q,h,m)=\frac{A(m)}{m}\frac{1}{q}(\sum_{r=1}^{q}e^{2\pi\,\mathrm{i}\,\frac{rh}{q}})(\sum_{n=1}^{M}e^{2\pi\,\mathrm{i}\,\beta n}).$$

Then
$$|S-S'| = M\frac{A(m)}{m} - U + O(m\sqrt{M}),$$
and $S'=0$ unless $q=1$. ⌟

Proof: Firstly, notice
$$S = \frac{1}{mq}\sum_{r=1}^{q}\sum_{n=1}^{M}\sum_{n\le u_k\le n+mq, u_k\equiv r(\mathrm{mod}\ q)} e^{2\pi\,\mathrm{i}\,\alpha u_k} + O(mq),$$
because the coefficient for $e^{2\pi\,\mathrm{i}\,\alpha u_k}$ is 1 unless $u_k\le mq$, which is compensated by the error term.

Then notice
$$e^{2\pi\,\mathrm{i}\,\alpha u_k} = e^{2\pi\,\mathrm{i}\,\frac{rh}{q}} e^{2\pi\,\mathrm{i}\,\beta u_k} = e^{2\pi\,\mathrm{i}\,\frac{rh}{q}} e^{2\pi\,\mathrm{i}\,\beta n} + O(mq|\beta|),$$
and the number of k s.t. $u_k\equiv r(\mathrm{mod}\ q)$ and $n\le u_k\le n+mq$ is at most $A(m)$ for each n,r, by(25.6.2.4), which we denote by $A(m)-D(n,m,q,r)\le A(m)$, then
$$S = S' - \frac{1}{mq}\sum_{r=1}^{q} e^{2\pi\,\mathrm{i}\,\frac{rh}{q}}\sum_{n=1}^{M} e^{2\pi\,\mathrm{i}\,\beta n} D(n,m,q,r) + O(Mmq|\beta|) + O(mq).$$
But this estimate is also true for $\alpha\in\mathbb{Z}$, so
$$U = M\frac{A(m)}{m} - \frac{1}{mq}\sum_{r=1}^{q}\sum_{n=1}^{M} D(n,m,q,r) + O(mq),$$
then combining these two estimates and the facts $q\le\sqrt{M}, q|\beta|\le 1/\sqrt{M}$, the assertion follows. □

Conj. (25.6.2.7) [Erdös-Turán]. Let $S\subset\mathbb{Z}_+$ s.t.
$$\sum_{n\in S}\frac{1}{n} = \infty,$$
then S contains arithmetic progressions of any length. ⌟

Proof: □

Arithmetic Progressions in Finite Fields

Lemma (25.6.2.8). For $n\in\mathbb{Z}_+, d\in\mathbb{R}_+$, let $S_{n,d}$ be the subspace of all polynomials in $\mathbb{F}_q[X_1,\dots,X_n]$ with total degree at most d and each variable has degree at most $q-1$. Let $\alpha,\beta\in\mathbb{F}_q$.

Suppose $P\in S_{n,d}$ satisfies $P(\alpha a+\beta b)=0$ for every pair $(a,b)\in A^2$ unless $a=b$, then
$$\#\{a\in A|P((\alpha+\beta)a)\ne 0\}\le 2\dim S_{n,d/2}.$$
⌟

Proof: Let
$$P(\alpha x+\beta y) = \sum c_{m,m'} m(x)m'(y)$$
where the sum is over pairs of monomials (m,m') s.t. $\deg(mm')\le d$. Then
$$P(\alpha x+\beta y) = \sum_{\deg m\le d/2} m(x)F_m(y) + \sum_{\deg m\le d/2} m(y)G_m(x).$$
Then the $\#A\times\#A$ matrix $\Big[P(\alpha a+\beta b)\Big]_{a,b\in A}$ has rank at most $2\dim S_{n,d/2}$. And the hypothesis means that this matrix is diagonal, so at most $2\dim S_{n,d/2}$ many diagonal entries are non-zero. □

Thm. (25.6.2.9). For $p \in \mathbf{P}, q \in p^{\mathbb{Z}_+}$, and $\alpha, \beta, \gamma \in \mathbb{F}_q$ that are not all zero s.t. $\alpha + \beta + \gamma = 0$. Let A be a subset of $\mathbb{F}_q^n$ s.t. the equation

$$\alpha a_1 + \beta a_2 + \gamma a_3 = 0$$

has no solutions $(a_1, a_2, a_3) \in A^3$ except when $a_1 = a_2 = a_3$. Then

$$\#A \leq 3 \dim S_{n,(q-1)n/3} (25.6.2.8).$$

⌟

Proof: WLOG, assume that $\gamma \neq 0$. Let $d \in [0, (p-1)n]$, then the space V of polynomials in $S_{n,d}$ that vanishes on the complement of $-\gamma A$ has dimension at least $\dim S_{n,d} - q^n + \#A$.

Let $P \in V$ be a function with maximal support $\Sigma \subset \mathbb{F}_q^n$, then $\#\Sigma \geq \dim V$, otherwise there is a non-zero polynomial $Q \in V$ vanishing on Σ, thus $\Sigma \subsetneq \mathrm{Supp}(P+Q)$.

Let $S(A) = \{\alpha a_1 + \beta a_2 | a_1 \neq a_2 \in A\} \subset \mathbb{F}_q$, then by hypothesis, $S(A) \cap \{-\gamma A\} = 0$. Thus P vanishes on $S(A)$. Then by(25.6.2.8), $P(-\gamma a) \neq 0$ for at most $2 \dim S_{n,d/2}$ many points of $a \in A$. Thus

$$\dim S_{n,d} - q^n + \#A \leq \dim V \leq \#\Sigma \leq 2 \dim S_{n,d/2}.$$

So

$$\#A \leq 2 \dim S_{n,d/2} + (q^n - \dim S_{n,d}) = 2 \dim S_{n,d/2} + \dim S_{n,(q-1)n-d}.$$

So if we take $d = \frac{2}{3}(q-1)n$, then we get the desired assertion. □

Cor. (25.6.2.10) [Ellenberg-Gijswijt]. For $p \in \mathbf{P}, q \in p^{\mathbb{Z}_+}$, and let A be a subset of $(\mathbb{F}_q)^n$ containing no three-term arithmetic progressions, then there exists some calculable constant $C_q < q$ s.t. $\#A = O(C_q^n)$.

In particular, $C_3 < 2.756$. ⌟

Proof: Take $\alpha = \beta = 1, \gamma = -2$, and use the fact(Cf.[E-G17]P342.**?**)

$$\lim_{n \to \infty} \frac{1}{n} \log(\frac{1}{q^n} \dim S_{n,(q-1)n/3}) = -I(\frac{2}{3}(q-1)) = -\sup_{\theta \in \mathbb{R}} \left\{ \frac{2}{3}(q-1)\theta - \log\left(\frac{1}{q}(1+e^\theta+\ldots+e^{(q-1)\theta})\right) \right\} < 0.$$

□

3 Littlewood-Offord Problem

Prop. (25.6.3.1) [Littlewood-Offord Problem, Erdös].

- If $\{x_i\}_{1 \leq i \leq n}$ is a set of real numbers with $|x_i| \geq 1$, then for any $r \in \mathbb{Z}_+$, the number of sums $\sum \pm x_k$ which lies in the interior of any interval of length $2r$ doens't exceed $r\binom{n}{\lfloor n/2 \rfloor}$.
- If $\{x_i\}_{1 \leq i \leq n}$ is a set of complex numbers with $|x_i| \geq 1$, then for any $r \in \mathbb{Z}_+$, the number of sums $\sum \pm x_k$ which lies in the interior of an arbitrary circle of radius r is $O(r\binom{n}{\lfloor n/2 \rfloor}) \leq O(r 2^n / \sqrt{n})$.

⌟

Proof: Cf.[Erdös, On a lemma of Littlewood and Offord. Bull. Amer. Math. Soc. 51 (1945), 898–902.] □

4 Sidon's Problem

Prop. (25.6.4.1) [Erdös-Turán]. For $n \in \mathbb{Z}_+$, let $\Phi(n)$ be the maximal number of subset $\{a_1, \ldots, a_X\}$ of $[n]_+$ s.t. $\{a_i + a_j\}_{i \leq j}$ are pairwise different. Then

$$\frac{1}{\sqrt{2}} \leq \varliminf_{n\to\infty} \frac{\Phi(n)}{\sqrt{n}} \leq \varlimsup_{n\to\infty} \frac{\Phi(n)}{\sqrt{n}} \leq 1.$$

⌟

Proof: Let $p \in \mathbf{P} \setminus \{2\}$ and $a_k = 2pk + u(k), k = 1, 2, \ldots, p-1$, where $1 \leq u(k) \leq p-1, u(k) \equiv k^2 (\mathrm{mod}\ p)$. Then $a_k < 2p^2$ for each k, and

$$a_i + a_j = a_k + a_l \iff (i,j) = (k,l),$$

because in this case

$$i + j = k + l, \quad i^2 + j^2 \equiv k^2 + l^2 \equiv q.$$

Thus $\Phi(2p^2) \geq p - 1$, and because there are infinitely primes, $\varliminf_{n\to\infty} \frac{\Phi(n)}{\sqrt{n}} \geq \frac{1}{\sqrt{2}}$.

For the other direction, for any such set $S = \{a_1, \ldots, a_X\}$ of $[n]_+$ s.t. $\{a_i + a_j\}_{i \leq j}$ are pairwise different. Choose $1 \leq m < n$, then for each $u \in \mathbb{Z}$, let $A_u = \#[u - m, u) \cap S$, then

$$\sum_{u=1}^{m+n} A_u = mx,$$

and the number of triples (i, j, n) s.t. $a_i, a_j \in A_u, a_j > a_i$ is

$$\sum_{u=1}^{m+n} \frac{1}{2} A_u (A_u - 1) \geq \frac{1}{2}(m+n) \frac{mx}{m+n} (\frac{mx}{m+n} - 1).$$

But by the hypothesis, there are at most

$$\sum_{r=1}^{m-1} (m - r) = \frac{1}{2} m(m-1)$$

such triples. Thus

$$\frac{1}{2} mx(mx - m - n) \leq \frac{1}{2} m(m-1)(m+n),$$

and whence

$$x < \frac{n}{m} + \sqrt{n + m + \frac{n^2}{m^2}}.$$

Taking $m = \lfloor \sqrt{n} \rfloor$, we get $x = \sqrt{n} + O(n^{\frac{1}{4}})$, thus $\varlimsup_{n\to\infty} \frac{\Phi(n)}{\sqrt{n}} \leq 1$. □

5 Sums and Products

Conj. (25.6.5.1) [Erdös-Szeméredi]. For $n \in \mathbb{Z}_+$, denote

$$g(n) = \min\Big(\max(\#(A + A), \#(A \cdot A)) : A \subset \mathbb{C}, \#A = n\Big).$$

Then it is conjectured that for any $\varepsilon \in \mathbb{R}_+$, when n is large, $g(n) \geq n^{2-\varepsilon}$. ⌟

Thm& Conj.Cor. (25.6.5.2) [Erdös-Szeméredi/Elekes/Solymosi]. Let $g(n)$ be as in(25.6.5.1), then there exists $C \in \mathbb{R}_+$ s.t. if $n \geq 2$,

$$g(n) \geq C \frac{n^{14/11}}{(\log n)^{3/11}}.$$

⌟

Proof: We only prove that $g(n) \geq 0.23n^{5/4}$, for the stronger result, Cf.[On the number of sums and products, Solymosi]?.

Let $A = \{a_1, \ldots, a_n\}$. and define n^2 linear functions on $\mathbb{R}$:

$$f_{j,k}(x) = a_j(x - a_k).$$

Then each $f_{j,k}$ maps at least n points in $A + A$ into $A \cdot A$: In fact, $f_{j,k}(a_k + a_i) = a_i a_j$. Thus $\Gamma(f_{j,k}) \subset \mathbb{R}^2$ contain at least n points from $(A + A) \times (A \cdot A)$. As $n \leq 10\sqrt{\#(A + A) \cdot \#(A \cdot A)}$, it follows from(25.1.3.8) that

$$n^2 \leq 100(\#(A + A) \cdot \#(A \cdot A))^2/(n - 1)^3$$

from which the assertion follows. □

Prop. (25.6.5.3) [Erdös -Szeméredi]. Let $g(n)$ be as in(25.6.5.1), then there exists $c \in \mathbb{R}_+$ s.t.

$$g(n) < \frac{n^2}{e^{c \log n/ \log\log n}}.$$

⌟

Proof: Cf.[Sums and Products of Integers]. □

Finite Fields

Thm. (25.6.5.4) [Bourgain-Katz-Tao/Bourgain-Konyagin]. Let $p \in \mathbf{P}$, then for $\delta \in \mathbb{R}_+$ and any $A \subset \mathbb{F}_p$ s.t. $\#A < q^{1-\varepsilon}$, there exists $\delta = \delta(\varepsilon) \in \mathbb{R}_+$ and $C \in \mathbb{R}_+$ s.t.

$$\max(\#(A + A), \#(A \cdot A)) \geq C(\delta)(\#A)^{1+\delta}.$$

⌟

Proof: Cf.[BGK06] □

Lemma (25.6.5.5). For $p \in \mathbf{P}$, and $A \subset \mathbb{F}_p$, denote

$$I(A) = \{a_1(a - 2 - a_3) + a_4(a_5 - a_6) : a_1, \ldots, a_6 \in A\}.$$

Then

$$\#I(A) \geq \begin{cases} p/2 & , \#A \geq \sqrt{p} \\ 0.1(\#A)^{3/2} & , \#A \leq \sqrt{p} \end{cases}.$$

⌟

Proof: Cf.[BGK06]P381. □

Thm. (25.6.5.6). For any $C_1, C_2 \in \mathbb{R}_+$, there exists $C \in \mathbb{R}_+$ s.t. for any $p \in \mathbf{P}_{\geq 3}, q \in p^{\mathbb{Z}_+}$, if $A \subset \mathbb{F}_q$ with $C_1 q^{1/2} \leq \#A \leq C_2 q^{7/10}$, then

$$\max(\#(A + A), \#(A \cdot A)) \geq C \frac{(\#A)^{3/2}}{q^{1/4}}.$$

⌟

Proof: Cf.[Sum-product Estimates in Finite Fields via Kloosterman Sums]. □

6 Others

Thm. (25.6.6.1). Given $n \in \mathbb{Z}_+$ and a set $M \subset (\mathbb{Z}_+)^n$, there exists a finite subset $S \subset M$ s.t. for any $m \in M$, there exists $s \in M$ s.t. $s_i \leq m_i$ for each $1 \leq i \leq n$. ⌟

Proof: Use induction on n. The case $n = 1$ is trivial, and for the induction process, choose randomly an $m \in M$. Then an element n is not "divisible" by m iff some $n_i < m_i$. Notice there are only f.m. such n_i. For each of this case, consider the subset $M'_{i,n_i} \subset (\mathbb{Z}_+)^{n-1}$ with the i-th coordinate discarded, then by induction there exists a finite subset S'_{i,n_i} s.t. each element in M'_{i,n_i} is divisible by some element in S'_{i,n_i}. Then S being $\{m\}$ with the collection of S'_{i,n_i} just satisfies the requirement. □

Prop. (25.6.6.2) [Erdös]. For any $k, l \in \mathbb{Z}_+$ and $a_1 < a_2 < \ldots < a_{(k-1)(l-1)+1} \in \mathbb{Z}_+$, there either exists k of them no one dividing the other, or there exists l of them each of a multiple of the previous one. ⌟

Proof: This follows immediately from(25.2.5.4). □

25.7 Word Theory

1 Sturmain Words

Def. (25.7.1.1). Given any word w on an alphabet $\mathcal{A}$, for any $k \in \mathbb{Z}_+$, let $W_k(w)$ be the set of k-words appearing in A. ⌟

Prop. (25.7.1.2) [Morse-Hedlund]. For any infinite word w over an alphabet $\mathcal{A}$,

- If w is eventually periodic, then there exists $C \in \mathbb{R}_+$ s.t. $\#W_k(w) \leq C$ for any $k \in \mathbb{Z}_+$.
- If w is not eventually periodic, then $\#W_{k+1}(w) \geq W_k(w) + 1$ for any $k \in \mathbb{Z}_+$. In particular, $\#W_k(w) \geq k + 1$.

⌟

Proof: □

Cor. (25.7.1.3). Given any infinite word w over a finite alphabet $\mathcal{A}$ that is not eventually periodic, then for any $n \in \mathbb{Z}_+$, there exists finite words V, W of length n, and $a, a', b, b' \in \mathcal{A}$ s.t. each of $a \amalg W, a' \amalg W, V \amalg b, V \amalg b'$ appears in w infinitely often. ⌟

Proof: This follows from the fact $\#W_{k+1}(w) \geq W_k(w) + 1$ and the fact $\#\mathcal{A} < \infty$. □

Def. (25.7.1.4) [Sturmian Words]. For $\theta, \rho \in \mathbb{R}$ s.t. $\theta \in (0, 1)$ and θ is irrational, we can define

$$s_n = \lfloor (n + 1)\theta + \rho \rfloor - \lfloor n\theta + \rho \rfloor, \quad s'_n = \lceil (n + 1)\theta + \rho \rceil - \lceil n\theta + \rho \rceil, \quad n \in \mathbb{Z}_+.$$

And define the infinite words

$$s_{\theta,\rho} = s_1 s_2 s_3 \ldots, \quad s'_{\theta,\rho} = s'_1 s'_2 s'_3 \ldots.$$

These are called **Sturmian words** with slope θ and intercept ρ. ⌟

Prop. (25.7.1.5). An infinite word w on alphabet $\{0, 1\}$ is a Sturmian word iff $\#W_k(w) = k + 1$ for any $k \in \mathbb{Z}_+$. ⌟

Proof: Cf.[Distributions modulo one]P225.? □

2 Thue-Morse Words

Cf.[Distributions modulo one].

25.8 Game Theory

1 Nash Equilibrium

References are [Non-corporative Games, Nash].

Def. (25.8.1.1) [Games]. A finite normal-form (mathematical)**game** is a tuple (N, A, O, μ, u), where

- N is a finite set of players, $n = \#N$.
- $A = (A_1, \ldots, A_n)$, where each A_i is a finite set of actions(or **pure strategies**).
- O is a set of outcomes.
- $\mu : A \to O$ determines the outcome as a function of the action profile.
- $u = (u_1, \ldots, u_n)$ where $u_i : O \to \mathbb{R}$ is the real-valued utility function for player i.

⌟

Def. (25.8.1.2) [Mixed Strategies]. In a mathematical game(25.8.1.1) (N, A, u), each player may randomize his actions, this is called a **mixed strategy**. The **support** of a mixed strategy s_i for player i is the set of pure strategies that s_i has positive probability.

Give a mixed strategy profile $s = (s_1, \ldots, s_n)$, the **expected utility** for player i is

$$u_i(s) = \sum_{a\in A} u_i(a) \prod_j s_j(a_j).$$

⌟

Def. (25.8.1.3) [Best Response]. In a mathematical game(25.8.1.1) (N, A, u), given any mixed strategy profile $s^i = (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$, a **best response** of player i to this strategy profile is a mixed strategy s_i s.t. $u_i(s_i, s^i) \geq u_i(s_i', s^i)$ for any mixed strategy s_i'. ⌟

Def. (25.8.1.4) [Nash-Equilibrium]. A strategy profile $s = (s_1, \ldots, s_n)$ is a **Nash equilibrium** if for each player i, s_i is a best response(25.8.1.3) to $s^i = (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$. ⌟

Thm. (25.8.1.5) [Nash1951]. Each finite normal-form mathematical game(25.8.1.1) has a Nash-equilibrium. ⌟

Proof: Let S be the set of mixed strategy profiles. Given a mixed strategy profile s, for all i and $a_i \in A_i$, define

$$\varphi_{i,a}(s) = \max(0, u_i(a, s^i) - u_i(s)),$$

and define the function $f : S \to S$ by

$$f(s)_i(a) = \frac{s_i(a) + \varphi_{i,a}(s)}{1 + \sum_{b\in A_i} \varphi_{i,b}(s)}.$$

Then with the natural topology, S is homeomorphic to $\mathbb{D}^1$ and f is continuous. So by Brouwer Fixed Point Theorem, f has a fixed point s.

Now we show this s is a Nash-equilibrium: By linearity of expected utility(25.8.1.2), for each i, there exists at least one $a \in A_i$ s.t. $u_{i,a}(s) \leq u_i(s)$. Then $\varphi_{i,a}(s) = 0$, and because $f(s) = s$, $\varphi_{i,b}(s) = 0$ for each $b \in A_i$. This implies that $u_i(s_i', s^i) \leq u_i(s)$ for any mixed strategy s_i'. As this is true for any i, we know s is a Nash-equilibrium. □

Prop. (25.8.1.6) [Symmetries in Games]. ⌟

Proof: □

Def. (25.8.1.7) [Solutions of Games]. ⌟

Finite Deterministic Competitive Games

Thm. (25.8.1.8). For any finite deterministic competitive game with complete information, one of the players has a winning strategy. ⌟

Proof: □

2 Greedoids

Def. (25.8.2.1) [Greedoids and Antimatroids with Repetitions]. For a set of symbols Σ, a language L on Σ(2.7.2.5) is called

- **left-hereditary** if $\alpha,\beta\in\mathrm{String}(\Sigma)$ and $\alpha\beta\in L$, then $\alpha\in L$.
- **permutable** if $\alpha,\beta\in L$ and $\mathrm{length}_x(\alpha)=\mathrm{length}_x(\beta)$ for any $x\in A$, then $\beta x\in L\iff\alpha x\in L$.
- **locally-free** if $\alpha\in L$ and $x\neq y\in\Sigma$ with $\alpha x\in L,\alpha y\in L$, then $\alpha xy\in L$.
- **strongly exchangeable** if for any $\alpha,\beta\in L$, there is a subword α' of α s.t. $\beta\alpha'\in L$, and $\mathrm{length}_x(\beta\alpha')=\max(\mathrm{length}_x(\beta),\mathrm{length}_x(\alpha))$ for any $x\in\Sigma$.
- **augmentary** if $\alpha,\beta\in L$ and $\mathrm{length}(\alpha)>\mathrm{length}(\beta)$, then there exists $x\in\alpha$ s.t. $\beta x\in L$.

A **greedoid** is a left-hereditary and augmentary language on a set of symbols. An **antimatroids with repetition** is a left-hereditary locally-free permutable language on a set of symbols. ⌟

Prop. (25.8.2.2)[Ranks of Greedoids]. In a greedoids, any two maximal words have the same length, called the **rank of this language**(which is defined to be ∞ if no maximal words exist). ⌟

Def. (25.8.2.3) [Flats]. In a left-hereditary language L on a set of symbols Σ, a **flat of words** is an equivalent class of words where two words $\alpha,\beta\in L$ are called equivalent if for any $\gamma\in\mathrm{String}(\Sigma),\alpha\gamma\in L\iff\beta\gamma\in L$.

A flat f is called a **subflat** of a flat g if any word in f can be extended to a word in g. ⌟

Prop. (25.8.2.4) [Strongly Exchangeable Languages]. Any strongly exchangeable language L on a set of symbols Σ is locally-free and permutable. Conversely, any left-hereditary locally-free and permutable language is strongly exchangeable. ⌟

Proof: It is easy to show that a strongly exchangeable language is locally-free and permutable. Conversely, for $\alpha,\beta\in L$, let α' be the subword of α consisting of those $x\in\Sigma$ that are preceded by at least $\mathrm{length}_x(\beta)$ many occurrence of x, then we show that $\beta\alpha'\in L$: We use induction on $\sum_x\max(\mathrm{length}_x(\alpha,\mathrm{length}_x(\beta))$. Let α'' be the longest prefix of α' s.t. $\beta\alpha''\in L$. Suppose for the contrary that $\alpha''\neq\alpha'$, and let x be the letter in α' following α''. Then $\mathrm{length}_x(\beta\alpha'')<\mathrm{length}_x(\alpha)$. Then we can write $\alpha=\alpha_1x\alpha_2$, where $\mathrm{length}_x(\alpha_1)=\mathrm{length}_x(\beta\alpha'')$.

By the definition of α', $\mathrm{length}_y(\alpha_1)\leq\mathrm{length}_y(\beta\alpha'')$ for any $y\in\Sigma$, so $\sum_y\max(\mathrm{length}_y(\alpha_1,\mathrm{length}_y(\beta\alpha''))<\sum_y\max(\mathrm{length}_y(\alpha,\mathrm{length}_y(\beta))$. Then by induction hypothesis, there exists $\gamma\in\mathrm{String}(\Sigma)$ s.t. $\alpha_1\gamma\in L$, and $\mathrm{length}_y(\alpha_1\gamma)=\mathrm{length}_y(\beta\alpha'')$ for any $y\in\Sigma$. Clearly $x\notin\gamma$, so we can use locally-freeness repeatedly to show that $\alpha_1\gamma x\in L$. Now permutability implies that $\beta\alpha''x\in L$, contradicting the maximality of α''. □

Cor. (25.8.2.5) [Antimatroids with Repetitions are Greedoids, Björner-Lovász-Shor]. Any antimatroids L with repetitions on a set of symbols Σ is a greedoids. And if L has finite rank(25.8.2.2), for any two words $\alpha,\beta\in L$, $\overline{\alpha}$ is a subflat of $\overline{\beta}$(25.8.2.3) iff $\mathrm{length}_x(\alpha)\leq\mathrm{length}_x(\beta)$ for any $x\in\Sigma$. In particular, α,β belongs to the same flat iff $\mathrm{length}_x(\alpha)=\mathrm{length}_x(\beta)$ for any $x\in\Sigma$. ⌟

Proof: By(25.8.2.4), any antimatroids with repetitions is strongly-exchangeable, thus is clearly augmentary.

If $\text{length}_x(\alpha) \leq \text{length}_x(\beta)$ for any $x \in \Sigma$, then by strongly exchangeable property, there exists $\gamma \in \text{String}(\Sigma)$ s.t. $\text{length}_x(\alpha\gamma) = \text{length}_x(\beta)$ for any $x \in \Sigma$. Thus by permutability, α is a subflat of β. Conversely, let $\alpha\gamma$ be equivalent to β, and extend $\alpha\gamma$ to a maximal word $\alpha\gamma\delta$, then $\beta\delta$ is also in L, and by strong exchangeability, $\text{length}_x(\alpha\gamma) = \text{length}_x(\beta)$ for any $x \in \Sigma$. In particular, $\text{length}_x(\alpha) \leq \text{length}_x(\beta)$ for any $x \in \Sigma$. □

3 Firing Games

References are [ALS91].

Def. (25.8.3.1) [Firing Games]. Given a finite set A, a **firing game** is a legal sequence of elements of A. where for any finite legal sequence $(a_1, \ldots, a_k)$ of A, there is a rule to determine which element $a_{k+1} \in A$ can be chosen s.t. $(a_1, \ldots, a_{k+1})$ is also legal. A firing game terminates for a legal sequence $(a_1, \ldots, a_k)$ if no such $a_{k+1} \in A$ can be found. ⌟

Def. (25.8.3.2) [Monotone Firing Games]. A **monotone firing game** is a firing game on a set A satisfying the following: For any $k, l \in \mathbb{N}$ and $c \in A$, if $X = (a_1, \ldots, a_k), Y = (b_1, \ldots, b_l)$ be two legal sequences s.t.

$$\#\{i|a_i = x\} \leq \#\{j|b_j = x\}$$

for any $x \in A$, and

$$\#\{i|a_i = c\} = \#\{j|b_j = c\},$$

then $(b_1, \ldots, b_l, c)$ is legal if $(a_1, \ldots, a_k, c)$ is legal. ⌟

Thm. (25.8.3.3) [Thorup]. For a monotone firing game on a set A, any element of A appears the same number of times in any terminating sequence legal sequence. ⌟

Proof: It is easy to check that the set of legal sequences form a antimatroids with repetitions on A(25.8.2.1), so the assertion follows from(25.8.2.5).

Alternatively, let $X = (a_1, \ldots, a_m), Y = (b_1, \ldots, b_n)$ be two legal terminating firing sequences. It suffices to prove that for any element $c \in A$, c appears in Y no more than it does in X. If this is not true, consider the smallest $k \in \mathbb{N}$ s.t.

$$\#\{i|a_i = a_{k+1}, i \leq k\} = \#\{j|b_j = a_{k+1}\}.$$

Then we can compare the two sequences $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_n)$, and use the minimality of k to conclude that $(b_1, \ldots, b_n, c)$ is also a legal sequence, contradicting the fact that Y is terminating. □

Lemma (25.8.3.4). The possible records of games form a locally-free permutable left-hereditary language on the set $V(G)$. ⌟

Chip-Firing Games

Def. (25.8.3.5) [Chip-Firing Games]. Given a simple finite graph G and a number a_i to each of its vertex v_i called the **initial distribution of chips**, a **chip-firing game** on this graph is sequence of **chip-firings** which means if $a_i \geq \deg(v_i)$ for some i, then we can decrease a_i by $\deg(v_i)$, and increase a_j by 1 for each v_j that is connected to j. ⌟

Thm. (25.8.3.6) [Björner-Lovász-Shor]. Given a simple finite graph G and initial distribution of chips(25.8.3.5), either every game can be continued infinitely, or every game terminates under after the same number of moves, and the number of times a given vertex is fired is the same in each vertex. ⌟

Proof: This is clearly a monotone firing game, so the assertion follows from(25.8.3.3). □

Lemma (25.8.3.7)[Tardos/Björner-Lovász-Shor]. Let G be a connected simple finite graph. Then:

- If a chip-firing game is infinite, then every node is fired infinitely often.
- If a chip-firing game terminates, then there is a node that is not fired at all.

⌟

Proof: 1: There is a vertex that is fired infinitely often, so the vertices connected to it receives infinitely many chips, so they must fire infinitely often too. In this way, because G is connected, every vertex is fired infinitely often.

2: Suppose each vertex is fired. Consider the vertex v s.t. at the end of the game, v has been idle for the longest time. Then after it fired the last time, all of its neighbors fired at least once. Thus v has $\deg(v)$ chips, so it can be fired again, contradiction. □

Prop. (25.8.3.8). Let G be a connected simple finite graph with $n = \#V(G)$ and $e = \#E(G)$, and $\sum_i a_i = N$.

- If $N > 2e - n$, then the game is infinite.
- If $e \le N \le 2e - n$, then there is an initial configuration of chips with infinite games and also an initial configuration of chips with finite games.
- If $N < e$, then the game is finite.

⌟

Proof: 1: If $N > 2e - n$, then there is always a vertex v with at least $\deg(v)$ chips.

2: We can always place $\deg(v_i) - 1$ chips at vertex v_i, so in this way we can place $2e - n$ chips with a finite game. On the other hand, if we have e chips, then we can choose an arbitrary acyclic orientation of vertices of G, and place $\deg^+(v_i)$ chips at vertex v_i. Then for this configuration the game is infinite: There is a source v, so we can fire v, and then after reverting the orientation of all edges from v, we get another acyclic orientation of G, and the chips are also places by $\deg^+(v_i)$ at vertex v_i. Then this process can go on forever.

3: Choose any acyclic orientation of G, and let $T = \sum_i \max(0, a_i - \deg^+(v_i))$. Call a vertex deficient if $a_i - \deg^+(v_i)$. Then along with any game, we can modify the orientation of G so that the quantity T never increases. And moreover, when the set of deficient vertices v_i changes, T decreases. In this way, we can show that the game is finite: A deficient vertex can never be fired, so an infinite game must change the set of deficient vertices infinitely often, contradiction.

To show the monotone property of T, when a vertex v is fired, reverse the orientation of all the edges leaving v, then this is also an acyclic orientation, but for T, the term at v decreases by $\deg^-(v)$, and all the terms at the vertices with an edge going to v increases by at most 1. Moreover, if such an vertex with an edge going to v is deficient, then in fact T decreases. If none of these are deficient, then the set of deficient sets doesn't change. □

Prop. (25.8.3.9). Let G be a connected simple finite graph with $n = \#V(G)$, and let λ_1 be the lest non-zero eigenvalue of the Laplacian matrix L_G(25.2.2.1), then any terminating chip-firing game with N chips has at most $\sqrt{2}nN/\lambda_1$ steps. ⌟

Proof: Suppose we start with a_i chips on vertex v_i and after s steps, we end up with b_i chips on vertex v_i. Let x_i be the number of times that v_i was fired. By(25.8.3.7), we may assume $x_n = 0$. Then clearly $Lx = \mathbf{a} - \mathbf{b}$.

Let

$$L_G = \sum_{i=1}^{n-1} \lambda_i v_i v_i^t$$

where $v_1 \leq v_1 \leq \ldots \leq v_{n-1}$ are the eigenvalues of L_G, and $v_1, \ldots, v_{n-1}$ are the corresponding orthogonal eigenvectors of unit length. Denote

$$L' = \sum_{i=1}^{n-1} \frac{1}{\lambda_i} v_i v_i^t, \quad v_n = \frac{1}{\sqrt{n}}(1, \ldots, 1)^t,$$

then

$$L' L_G = \sum_{i=1}^{n-1} v_i v_i^t = \mathbf{1} - v_n v_n^t = \mathbf{1} - \frac{1}{n}\mathbf{J}.$$

Hence $e_n^t L' L_G = e_n^t - \frac{1}{n}(1, \ldots, 1)^t$, and

$$s = (1, \ldots, 1).\mathbf{x} = n(e_n^t - e_n^t L' L)\mathbf{x} = -n e_n^t L' L \mathbf{x} = \sum_{i=1}^{n-1} -\frac{n}{\lambda_i}(e_n^t \lambda_i)(v_i^t(\mathbf{a} - \mathbf{b})).$$

Thus

$$s \leq \frac{n}{\lambda_i} \sum_{i=1}^{n-1} |e_n^t v_i|.|v_i^t(\mathbf{a} - \mathbf{b})| \leq \frac{n}{\lambda_i} \sqrt{\sum_{i=1}^{n-1} (e_n^t v_i)^2}.\sqrt{\sum_{i=1}^{n-1} (v_i^t(\mathbf{a} - \mathbf{b}))} \leq \frac{n}{\lambda_i}|\mathbf{a} - \mathbf{b}| \leq \sqrt{2}\frac{nN}{\lambda_1}.$$

□

26 Experimental Physics

26.1 Hamiltonian Mechanics

References are [Arn89] and [Notes on Quantum Field Theory, Etingof].

Notation (26.1.0.1).
- Use notations as in **??**.

⌟

1 Hamiltonian Mechanics

<u>**Newtonian Mechanics**</u>

Physical Law (26.1.1.1)[Space and Time in Newtonian Mechanics]. The **Galilean space-time structure** is a 4-dimensional real vector space. Its points are called world points or events.

The **time** is a projection from the space to $\mathbb{R}$: $t : \mathbb{R}^N \to \mathbb{R}$. Two events a, b are called **simultaneous** if $t(a) = t(b)$.

The set of events simultaneous to a given event forms a 3-dimensional affine subspace of $\mathbb{R}^3$, called a **space of simultaneous events**. ⌟

Def. (26.1.1.2) [Galilean Transformations]. By(26.1.1.1), we can assume that the Galilean space-time is isomorphic to $\mathbb{R} \times \mathbb{R}^3$, where the first coordinate is time. Any such isomorphism determines a **Galilean coordinate system** on the space-time structure. Thus on the Galilean space-time, we can define the Eisenstein metric $\mathrm{d}s^2 = \mathrm{d}x_1^2 + \mathrm{d}x_2^2 + \mathrm{d}x_3^2 - \mathrm{d}t^2$.

The **Galilean group** is the group of automorphisms of the Galilean space preserving the Eisenstein metric. The transformations of a Galilean coordinate system is also the class of **inertia coordinate systems** w.r.t. this coordinate system. ⌟

Prop. (26.1.1.3). Any Galilean transformation g can be written as a product $g_1 \circ g_2 \circ g_3$ where
- g_1 is a **uniform motion** with velocity v: $g_1(t, x) = (t, x + tv)$.
- g_2 is a **translation of the origin**: $g_2(t, x) = (t + s, x + x')$.
- g_3 is a **rotation of coordinate axis**: $g_3(t, x) = g_3(t, Gx)$, where $G \in O(3, \mathbb{R})$.

⌟

Proof: □

Def. (26.1.1.4)[Motion, Velocity and Acceleration]. A **motion** in $\mathbb{R}^N$ is a smooth curve $x : I \to \mathbb{R}^N$, where I is an interval in $\mathbb{R}$.

For $t_0 \in I$, the **velocity of a motion** $x : I \to \mathbb{R}^N$ is defined to be the derivative $\dot{x} = \frac{\partial}{\partial t} x|_{t=t_0}$. And the **acceleration vector** of t_0 is defined to be the the second derivative $\ddot{x} = \frac{\partial^2}{\partial t^2} x|_{t=t_0}$. ⌟

Physical Law (26.1.1.5) [Newtonian Mechanics and Newton's Principle of Determinacy]. Any motion of a newtonian mechanical system uniquely determined by its initial positions(i.e. $x(t_0) \in \mathbb{R}^N$) and its initial states(i.e. $\dot{x}(t_0) \in \mathbb{R}^N$).

The study of motions in a newtonian system is called a **Newtonian mechanics**(of particles). ⌟

Def. (26.1.1.6) [Newton's Equation]. In a given Galilean coordinate system, it follows from the newton's principle of determinacy(26.1.1.5) that there is a function $F : \mathbb{R}^N \times \mathbb{R}^N \times \mathbb{R} \to \mathbb{R}$ s.t. for any motion x in $\mathbb{R}^N$,

$$\ddot{x}(t) = F(x, \dot{x}, t).$$

This is called the **Newton's equation**. ⌟

Axiom (26.1.1.7) [Galileo's Principle of Relativity]. The Newton's equations(26.1.1.6) are invariant under the action of Galilean group(26.1.1.2). Equivalently,

$$F(x, \dot{x}, t) = F(x, \dot{x}, t + s),$$

$$F(x + tv, \dot{x} + v, t) = F(x + tv, \dot{x} + v, t),$$

$$GF(x, \dot{x}, t) = F(Gx, G\dot{x}, t), \quad G \in O(3, \mathbb{R}).$$

⌟

Def. (26.1.1.8) [Forces]. A **force** is a vector field on the configuration space.

A **conservative force** is a force F s.t. there exists a potential energy U s.t. $\operatorname{grad} U = F$. ⌟

Def. (26.1.1.9) [Work of a Force]. The **work** of a force**?** F on a path γ is defined to be

$$A = (F, \gamma) = \int_\gamma (F, \mathrm{d}\gamma).$$

⌟

Prop. (26.1.1.10). If the configuration space is simply-connected(e.g. $\mathbb{R}^N$), then a force is conservative iff its work along any path only depends on the endpoints. ⌟

Hamiltonian Mechanics

Def. (26.1.1.11) [Lagrangian Dynamical System]. A **Lagrangian (dynamical) system** of particles consists of the following:

- A differentiable manifold M.
- A differentiable function $\mathcal{L} \in C^\infty(TM \times \mathbb{R})$ called the **Lagrangian of the system**.

If $\mathcal{L}$ factors through the projection to TM, then it is called an **autonomous Lagrangian system**, otherwise it is called a **non-autonomous Lagrangian system**.

In particular, a Lagrangian system is a classical field theory(13.1.0.1). ⌟

Def. (26.1.1.12) [Generalized Coordinates and Velocities]. Given a Lagrangian system M, any smooth chart $\varphi_\alpha : U_\alpha \subset M \cong V_\alpha \subset \mathbb{R}^n$ defines a **generalized coordinate** $q_i = (\varphi_\alpha)_i$ on U_α. And $\frac{\partial}{\partial \dot{q}_i}\mathcal{L} = p_i$ are called the **generalized velocities**. ⌟

Def. (26.1.1.13) [Hamiltonian Mechanics and the Principle of Least Action]. For any Lagrangian dynamical system(26.1.1.11) and any generalized coordinate q_i, then a **motion** in this system is a path $\gamma : [t_0, t_1] \to M$ s.t. γ is the extremal curve(11.13.1.3) of the functional

$$\Phi(\gamma) = \int_{t_0}^{t_1} \mathcal{L}(\gamma, \dot{\gamma}, t)\mathrm{d}t.$$

Equivalently, it satisfies the Euler-Lagrangian equation(11.13.1.5)

$$\frac{\partial}{\partial t}\frac{\partial}{\partial \dot{q}}\mathcal{L} = \frac{\partial}{\partial q}\mathcal{L}.$$

The study of motions in a Lagrangian system is called a **Hamiltonian mechanics**. ⌟

Def. (26.1.1.14) [Natural Lagrangians]. For a Lagrangian system with phase space M, A Riemannian structure on M will give a **kinetic energy**

$$T = \frac{1}{2}\langle v, v\rangle_x, \quad v \in T_x M,$$

and a **potential energy** is a function $U \in C^\infty(M)$ that is viewed as a function on TM via projection.

Then the Lagrangian $\mathcal{L}$ is called a **natural Lagrangian** if it is of the form $\mathcal{L} = T - U$ for some kinetic energy T and some potential energy U. ⌟

Thm. (26.1.1.15) [Hamilton's Form of the Principle of Least Action]. if q_i are the generalized coordinates for the system of n mass points in a Euclidean space, define the natural Lagrangian $\mathcal{L}(q, \dot{q}, t) = T - U$, where $T = \frac{1}{2}\sum m_i \dot{q}_i^2$ is the kinetic energy and U is a potential energy. Then its Euler-Lagrangian equation is

$$-\frac{\partial}{\partial q_i}U = m\ddot{q}_i, \quad 1 \le i \le n.$$

which is just the **Newton's equation** of kinetic mechanics. By(26.1.1.13), this equation is satisfied when the system evolves with time. ⌟

Cor. (26.1.1.16). Newtonian mechanics(26.1.1.5) are Hamiltonian mechanics, thus are classical field theories. ⌟

Example (26.1.1.17) [Free Particles]. In the system of a free mass point of weight m in $\mathbb{R}^3$, if $q = r$ is the usual coordinate, then

$$L = T = \frac{m\dot{r}^2}{2} = \frac{m}{2}(\dot{q}_1^2 + \dot{q}_2^2 + \dot{q}_3^2).$$

Then the generalized momenta are $p_i = m\dot{q}_i$. And the Lagrangian equation is $\frac{\partial}{\partial t}p = 0$. ⌟

Example (26.1.1.18) [Central Potential Fields]. In the system of a free mass point in $\mathbb{R}^2$ with a central potential field $U = U(r)$ in the polar coordinate (r, φ). Then in this coordinate $q_1 = r, q_2 = \varphi$,

$$\mathcal{L}(q, \dot{q}) = T(q, \dot{q}) - U(q) = \frac{m}{2}(\dot{q}_1^2 + q_1^2\dot{\varphi}^2) - U(q_1).$$

Then the generalized momentum is

$$p_1 = m\dot{r}, \quad p_2 = mr^2\dot{\varphi},$$

and the Lagrangian equations are

$$m\ddot{r} = mr\dot{\varphi}^2 - \frac{\partial}{\partial r}U, \quad \dot{p}_2 = 0.$$

Notice the second equation is called the **law of conservation of angular momentum**. This is a special case of(26.1.1.19). ⌟

Prop. (26.1.1.19) [Generalized Law of Conservation of Angular Momentum]. A coordinate q_i not appearing in the Lagrangian(i.e. $\frac{\partial}{\partial q_i}\mathcal{L} = 0$) is called a **cyclic coordinate**. Then it follows from(26.1.1.15) that the generalized momentum corresponding to a cyclic coordinate remains constant. ⌟

Symmetries

Thm. (26.1.1.20) [Noether's Theorem]. ⌟

Thm. (26.1.1.21) [Continuity Equation]. ⌟

Prop. (26.1.1.22) [Dimensional Analysis]. In an equation raising from a physical problem, we can normalize all the indeterminants to get a non-dimensional one, giving the equation some kind of characteristic length. ⌟

2 Symplectic Structure

26.2 Quantum Mechanics

Basic References are [Nap].

1 Basics

Physical Law (26.2.1.1) [Law of Quantum Mechanics]. The Schrodinger equation can be derived from the Dirac-von Neumann axioms:

The **states of particles** is a countable dimensional Hilbert space, and

- The **observables** of a quantum system are defined to be the (possibly unbounded)Hermitian operators A on $\mathbb{H}$. Then any continuous observable is unitarily diagonalizable, with real eigenvalues by Hilbert-Schmidt(11.9.4.16). The eigenvalues of the matrix corresponding to an observable is called the **observations**.
- The **state** φ of the quantum system is a unit vector of $\mathbb{H}$, up to scalar multiples.
- The expectation value of an observable A for a system in a state φ is given by the inner product $(\varphi, A\varphi)$.
- (Unitarity)The time evolution of a quantum state according to the Schrodinger equation is mathematically represented by a unitary operator $U(t)$ (depends only on the state an relative time)(one-parameter subgroup).

Now that $\varphi(t) = \widehat{U}(t)\varphi(t_0)$, so $\widehat{U}(t)\varphi(t_0) = e^{-i\widehat{\mathcal{H}}t}, where \widehat{\mathcal{H}}$ is Hermitian, called the **quantum Hamiltonian**.

So now take derivative w.r.t t, we get $i\frac{d\varphi}{dt} = \widehat{\mathcal{H}}\varphi$. By **quantum correspondence principle**, it is possible to derive the expression of $\widehat{\mathcal{H}}$ by classical methods. ⌟

Def. (26.2.1.2) [Qubits]. A **qubit** is a state that is complex combination of $|0\rangle$ and $|1\rangle$, i.e. $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$. ⌟

Def. (26.2.1.3) [Quantum Entanglement and Singlets]. Any tensor in a tensor space of two Hilbert space that is not a pure tensor will correspond to a **quantum entanglement**. The simplest quantum entanglement is the **singlet state**

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle \in (\mathbb{C}\{|0\rangle, |1\rangle\})^{\otimes 2} \cong \mathbb{C}^4.$$

⌟

Def. (26.2.1.4) [Pauli Observables]. The observables on a two dimensional Hilbert space, i.e. a qubit state space, are all combinations of **Pauli Observables** plus **1**:

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Their corresponding eigenvalues are denoted by

$$\uparrow = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \downarrow = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \rightarrow = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad \leftarrow = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}, \quad \otimes = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ i \end{bmatrix} \quad \odot = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -i \end{bmatrix}$$

⌟

Remark (26.2.1.5). The solution of a Schrodinger equation for a non Relativistic particle is assumed to be a Schwartz function (Vanish fast enough at infinity). The coefficients is assumed smooth enough to guarantee at least uniqueness and existence locally. ⌟

Prop. (26.2.1.6). The wave function on the (p,t) coordinates is the Fourier Transform of the wave function on the (x,t) coordinates, because the eigenstate of the p-operator $i\hbar\frac{\partial}{\partial x}$ is e^{ikx}, the coefficients of which is the value (probability) of the wave function of the (p,t) coordinates. ⌟

Prop. (26.2.1.7) [Schrödinger Uncertainty Principle]. Set $\sigma_A=\sqrt{\langle\widehat{A}^2\rangle-\langle\widehat{A}\rangle^2}$, then:

$$\sigma_A^2 2\sigma_B^2\geq\left|\frac{1}{2}\langle\widehat{A}\widehat{B}+\widehat{B}\widehat{A}\rangle-\langle\widehat{A}\rangle\langle\widehat{B}\rangle\right|^2+\left|\frac{1}{2i}\langle[\widehat{A},\widehat{B}]\rangle\right|^2.$$

⌟

Proof: Derived from definition and Schwarz inequality, Cf.[Wiki]. □

Cor. (26.2.1.8) [Heisenberg Uncertainty Principle]. $\sigma_x\sigma_p\geq\frac{\hbar}{2}$. ⌟

Proof:

$$[x,i\hbar\frac{\partial}{\partial x}]=i\hbar.$$

□

Prop. (26.2.1.9) [Spectral Decomposition]. In Quantum physics, one need to use spectral decomposition of the Hamiltonian operator. But at most cases, there are only countably many eigenstate and the eigenvalue has a lower bound and tends to infinity. In this case, $(\widehat{H}+A)^{-1}$ is a compact operator thus by spectral theorem(11.9.4.15) the eigenstate of $\widehat{H}$ forms a set of complete basis. ⌟

Prop. (26.2.1.10) [No-Cloning Theorem]. ? ⌟

Calculations

Prop. (26.2.1.11) [Virial Theorem]. For a system that $V(r)\sim r^n$, the average kinetic energy and the average potential energy has the relation :

$$2\langle T\rangle=n\langle V\rangle.$$

⌟

Spin

2 Quantum Computations

Classical Logic Gates

Def. (26.2.2.1) [Boolean Functions]. A **Boolean function** is a function $f:\mathbb{F}_2^n\to\mathbb{F}_2$. ⌟

Def. (26.2.2.2) [Classical Logic Gates]. There are four classical logic gates, if we let $0,1\in\mathbb{F}_2$, then:

- **AND gate**: $(a,b)\mapsto ab$.
- **OR gate**: $(a,b)\mapsto ab+a+b$.
- **NOT gate**: $a\mapsto a+1$.

- **COPY gate**: $a \mapsto (a, a)$.

┘

Def. (26.2.2.3) [Reversible Gates]. A gate is called **reversible** iff it is a bijection from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. ┘

Def. (26.2.2.4) [Simulations]. A set of gates is said to be able to **simulate** a boolean function f iff there is a composition of these gates that maps

$$(x_1, \ldots, x_{m+n}) \to (g_1(x_1, \ldots, x_{m+n}), \ldots, g_k(x_1, \ldots, x_{m+n}))$$

such that if we let $x_{i_1} = a_1, x_{i_2} = a_2, \ldots, x_{i_m} = a_m$ be fixed, where $\{0, 1 \ldots, m+n\} - \{i_1, \ldots, i_m\} = \{j_1, \ldots, j_n\}$(in some order), then $g_1(x_1, \ldots, x_{m+n}) = f(x_{j_1}, \ldots, x_{j_n})$.

A set of gates is called **universal** iff they can simulates all Boolean function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$. ┘

Prop. (26.2.2.5) [Classical Gates are Universal]. The four classical gates are universal. In fact, $\text{And}(x, y) = \text{OR}(\text{NOT}(x), \text{NOT}(y))$, so even AND is disposable, and COPY is not used as well. ┘

Proof: Just use OR gate to juxtapose all possible combinations that are mapped to 1. □

Example (26.2.2.6) [Reversible Gates].

- The **CNOT gate** is defined to be $\text{CNOT} : (a, b) \mapsto (a, b + a)$.
- The **Toffoli gate** is defined to be $\text{CCNOT} : (a, b, c) \mapsto (a, b, c + ab)$.
- The **Fredkin gate** or CSWAP gate is a three-bit gate defined as the quantization of the gate given by:$(a, b, c) \mapsto (a, (1 - a)c + ab, (1 - a)b + ac)$.

┘

Prop. (26.2.2.7). CNOT gate cannot simulate AND. In particular, CNOT is not universal. ┘

Proof: It can be shown that any Boolean function that can be simulated by CNOT gate is of the form $(x_1, \ldots, x_n) \mapsto \sum a_i x_i + b$. But AND is of the form $(a, b) \mapsto ab$, which is not of the form, so it is not simulated by CNOT. □

Prop. (26.2.2.8). The Toffoli gate(26.2.2.6) is universal(26.2.2.4). ┘

Proof: By(26.2.2.5), it suffices to show that it can simulate AND and NOT, then it can simulate OR because $\text{OR}(x, y) = \text{NOT}(\text{NOT}(x), \text{NOT}(y))$.

AND is outputted in the third bit with $c = 0, a = x, b = y$, NOT is outputted in the third bit with $a = 1 = c, b = x$. □

Prop. (26.2.2.9). The Fredkin gate(26.2.2.6) is universal(26.2.2.4). ┘

Proof: If we set the third input to be 0, then the second output of $\text{CSWAP}(x, y, 0)$ is $\text{And}(x, y)$, and if we set the second input to be 0 and the third input to be 1, then the second output of $\text{CSWAP}(x, 0, 1)$ is $\text{NOT}(x)$. Thus the Fredkin gate can simulate both AND and NOT gates, thus universal, by(26.2.2.5). □

Quantum Logic Gates

Our model of quantum computation is quantum logic gates.

Def. (26.2.2.10) [Quantum Logic Gates]. A **quantum logic gate** is a unitary matrix. In particular a quantum logic gate is always reversible. ⌟

Prop. (26.2.2.11) [Examples of Quantum Gates].

- The **Hadamard gate** H is a rotation on one single qubit given by the matrix $\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$.
- If a classical gate is reversible and its matrix is unitary, then the same matrix will give out a quantum gate with all entries 0 and 1, called the **quantization of classical gates**.

⌟

3 Quantum Algorithms

Algo. (26.2.3.1) [Deutsch-Jozsa Algorithm]. The **Deutsch-Jozsa problem** is that: given a function $f:\mathbb{F}_2^n\to\mathbb{F}_2$, which is either a constant function or a function that takes half value 0 and half value 1,

Consider the gate $U_f:(x_1,\ldots,x_n,x)\mapsto(x_1,\ldots,x_n,x+f(x_1,\ldots,x_n))$, then there is a **Deutsch-Jozsa algorithm** that can determine if f is a constant function just using the gate U_f once. ⌟

Proof: Make the state

$$H^{\otimes n+1}\circ U_f\circ H^{\otimes(n+1)}(0,0,\ldots,0,1)=\Big(\frac{1}{2^n}\sum_{(a_1,\ldots,a_n)\in\mathbb{F}_2^n}\Big(\sum_{(x_1,\ldots,x_n)\in\mathbb{F}_2^n}(-1)^{f(a_1\ldots a_n)+\sum_i a_ix_i}\Big)|a_1\ldots a_n\rangle\Big)\otimes|0\rangle,$$

and then measure all the first n bits in the $|0\rangle/|1\rangle$-basis. Then the result is $(0,0,\ldots,0)$ iff f is constant. □

Making Classical Algorithms Reversible

Because quantum computers can only deal with reversible algorithms, we need to spend either time or space to make classical algorithms revertible. This is because by von-Neumann-Landauer limit, it takes energy to erase a bit of information.

For example, The modular exponentiation algorithm(2.10.2.1) can be made revertible as in [Sho97].

Quantum Fourier Transform

Def. (26.2.3.2) [Quantum Fourier Transform]. The (inverse)**quantum Fourier transform** is an algorithm represented by the matrix

$$U_{\mathrm{QFT}}=\frac{1}{\sqrt{N}}\operatorname{Van}(1,\zeta_N,\zeta_N^2,\ldots,\zeta_N^{N-1}).$$

⌟

Proof: It suffices to prove this matrix is unitary, which is easy. □

Lemma (26.2.3.3) [Tensor Representation]. The trick of the quantum Fourier transform lies in its connection with the 2-adic decimal representation:

$$\begin{aligned} U_{\mathrm{QFT}}(|x_n x_{n-1}\dots x_1\rangle) = \frac{1}{\sqrt{N}}&(|0\rangle + \exp(2\pi\,\mathrm{i}\cdot 0.x_1)|1\rangle \\ &\otimes(|0\rangle + \exp(2\pi\,\mathrm{i}\cdot 0.x_2x_1)|1\rangle \\ &\otimes\dots \\ &\otimes(|0\rangle + \exp(2\pi\,\mathrm{i}\cdot 0.x_n x_{n-1}\dots x_1)|1\rangle \end{aligned}$$

⌟

Proof: Direct calculation.**?** □

Algo. (26.2.3.4) [Quantum Fourier Transform Algorithm, Shor]. Because of the tensor representation of quantum Fourier transform, it is anticipated that the transformation can be represented using Hadamard gate and phase change gates. The circuit given in `https://en.wikipedia.org/wiki/Quantum_Fourier_transform` shows that for $n\in\mathbb{Z}_+$, U_{QFT} on $N=2^n$ can be represented by a circuit with $n(n+1)/2$ gates up to a swap. And there are $O(n^2)$ qbit swaps to be performed, which shows that the quantum Fourier transform has complexity $O(n^2)$. ⌟

Shor's Algorithms

References are [Sho94], [Sho97]

Def. (26.2.3.5). For a number $M=pq$, where p,q are different odd prime numbers, $x\in(\mathbb{Z}/(M))^*$ is called **good** iff $r=\mathrm{ord}(x)$ is even, and neither of $x^{r/2}\pm 1$ is divisible by M.

Then at least half of $(\mathbb{Z}/(M))^*$ is good. ⌟

Proof: It suffices to consider a fixed order $2a$, and this is additive in $\mathbb{Z}/(2a,p-1)\mathbb{Z}\times\mathbb{Z}/(2a,q-1)\mathbb{Z}$.**?**. □

Algo. (26.2.3.6) [Shor's Algorithm for Computing Orders]. If we find a good x for M, then $x^{r/2}\pm 1$ contains separately a prime p or q, so we can use Euclidean algorithm to extract a prime of M. This is just the idea of Shor's algorithm(26.2.3.7). ⌟

Algo. (26.2.3.7) [Shor's Prime Factorization Algorithm]. For $M=pq$, we can factor p,q out with high probability in $O((\log M)^2)$ time. ⌟

Proof: Cf.[Napkin P274]. □

Algo. (26.2.3.8) [Shor's Discrete Logarithm Algorithm]. ⌟

Grover's Algorithm

Prop. (26.2.3.9). ⌟

Prop. (26.2.3.10) [Grover's Selection Algorithm]. If there are n items labeled $\{0,\dots,n-1\}$, and there is a marked item w. then there is a quantum algorithm that find w in $O(\sqrt{n})$ times. ⌟

Proof: Cf.[Quantum Algorithm MIT P33,35]. □

4 Quantum Informations

Quantum Cryptography

x1dddd

26.3 General Relativity Theory

1 Basics

Prop. (26.3.1.1) [Maxwell's Equation]. Normal Maxwell's equation reads:

$$\begin{cases} \mathrm{div}E = q & \text{(Coulomb's law)} \\ \mathrm{div}H = 0 & \text{(Gaussian law)} \\ \mathrm{curl}E = -\frac{1}{c}\frac{\partial H}{\partial t} & \text{(Faraday's law)} \\ \mathrm{curl}H = j + \frac{1}{c}\frac{\partial E}{\partial t} & \text{(Ampère-Maxwell law)} \end{cases}$$

where E is the magnetic field, H is the electric field, q the charge density, j the electric current.

In Minkowski space, we define the electromagnetic 2-form

$$F = \frac{1}{2}F_{\alpha\beta}dx^\alpha \wedge dx^\beta,$$

where $F_{i0} = E_i, \quad Fij = H_k$, and electric current J, $J^i = -j^i, J^0 = q$.

Maxwell's equation can be re-written as:

$$d^*F = J \qquad dF = 0.$$

Where $d^* = *d*$. ⌟

Proof: The Minkowski space is flat, the equivalence can be seen by direct calculation. □

27 Non-Commutative Geometry(Connes)

27.1 Supersymmetry

Def. (27.1.0.1) [Supermanifolds]. A **supermanifold** of dimension (n,m) is a smooth manifold $|M|$ together with a sheaf $\mathcal{O}_M$ of $\mathbb{Z}/(2)$-graded algebras that is locally isomorphic to $\mathcal{O}_{|M|}\otimes\Lambda[\xi_1,\ldots,\xi_m]$. The odd functions on M generate a nilpotent ideal $\mathcal{J}\subset\mathcal{O}_M$, with $(|M|,\mathcal{O}_M/\mathcal{J})$ a manifold, called the underlying manifold of M, denoted by M_{red}.

A map of supermanifolds $\varphi: M\to N$ is a map of manifolds $\varphi_0: M_0\to N_0$ together with a map of supervectors spaces $\varphi_0^*\mathcal{O}_N\to\mathcal{O}_M$. ⌟

Remark (27.1.0.2). In a similar fashion, we can define complex supermanifold, analytic supermanifolds or superschemes. ⌟

Prop. (27.1.0.3) [Morphisms between Supermanifolds]. Let M be a supermanifold and $U\subset\mathbb{R}^{p|q}$ an open submanifold, then a map of supermanifolds $f: M\to U$ is equivalent to a tuple $(f_1,\ldots,f_p,\varphi_1,\ldots,\varphi_q)$ s.t. for any $x\in|M|$, $(f_1(x),\ldots,f_p(x))\in|U|$.

In fact, giving such a tuple, suppose $f_i=f_i^0+r_i$ where $f_i^0\in\mathcal{O}_{|M|}$ and $r_i\in\mathcal{J}$, then in local coordinates, the pullback of $F=\sum F_I\theta^I$ is

$$F(f_1,\ldots,f_p,\varphi_1,\ldots,\varphi_q)=\sum_I\Big(\sum\partial^\alpha F(f_1^0,\ldots,f_p^0,\varphi_1,\ldots,\varphi_q)\frac{r^\alpha}{\alpha!}\Big)\varphi^I.$$

⌟

Def. (27.1.0.4) [Super Vector Bundles]. A **super-vector bundle** over a supermanifold M is an $\mathcal{O}_M$-sheaf $\mathcal{E}$, locally free of dimension $p|q$. ⌟

1 Real Structures

2 Super Lie Groups

Def. (27.1.2.1) [Super Classical Groups].

- $\mathrm{GL}(p|q)$.
- There is a Berezinian map $\mathrm{Ber}:\mathrm{GL}(p|q)\to\mathrm{GL}(1|0)$, and the kernel is denoted by $\mathrm{SL}(p|q)$.
- $\mathrm{OSp}(n|2m)$ is the group fixing an even supersymmetric non-degenerate bilinear form Φ.
- $\pi\,\mathrm{Sp}(n|n)$ is the group fixing an odd super-anti-symmetric non-degenerate bilinear form Φ.
- The kernel of $\mathrm{Ber}:\pi\,\mathrm{Sp}(n|n)\to\mathrm{GL}(1|0)$ is called the group of P-series.

- Let $D = \mathbb{R}[\eta]$ be the super division algebra with η odd and $\eta^2 = -1$, then there is a odd determinant map
$$\text{odet} : \text{GL}(n; D) \to \mathbb{R}^{0|1},$$
the kernel of odet is called the group of Q-series.

⌟

Proof: Cf.[Deligne, Supersymmetry]P70. □

28 Others

28.1 Probability Theory

References are [Dudley, Real Analysis and Probability], and [Real Analysis, Folland].

Notation (28.1.0.1).

- Use notations as in Real Analysis(Functions on $\mathbb{R}^n$).

⌟

1 Basics

Def. (28.1.1.1) [Events]. Given a probability space $(\Omega, \mathcal{M}, P)$, any measurable space $A \in \mathcal{M}$ is called an **event** in $\mathcal{M}$, and its **probability of the event** is defined to be $\mathbf{P}(A)$. ⌟

Def. (28.1.1.2) [Independent Events]. Given a probability space $(\Omega, \mathcal{M}, P)$, two events(28.1.1.1) A and B are called **independent events** if $\mathbf{P}(A \cap B) = \mathbf{P}(A) \cdot \mathbf{P}(B)$. Similarly, we can define jointly-independent events. ⌟

Def. (28.1.1.3) [Random Variables]. A measurable function(11.3.1.17) X from a probability space $(\Omega, \mathcal{M}, P)$(11.3.1.3) to a measurable space $(S, \mathcal{A})$ is called a **random variable** on Ω. ⌟

Def. (28.1.1.4) [Independent Variables]. Suppose $(\Omega, \mathcal{M}, P)$ is a probability space and $X : (\Omega, \mathcal{M}, P) \to (S, \mathcal{A})$ and $Y : (\Omega, \mathcal{M}, P) \to (T, \mathcal{B})$ are two random variables, then X, Y is called a pair of **independent variables** if for any event $U \in \mathcal{A}$ and $V \in \mathcal{B}$, $X^{-1}(U)$ and $Y^{-1}(V)$ are independent events(28.1.1.2), i.e.

$$\mathbf{P}(X \in U, Y \in V) = \mathbf{P}(X \in U) \cdot \mathbf{P}(Y \in V).$$

Similarly, we can define jointly-independent variables.

If $\mathscr{S}$ is a set of random variable, then variables in S are called **independent variables** if any subset of variables in $\mathscr{S}$ are jointly-independent. ⌟

Def. (28.1.1.5) [Expected Values, Variances and Standard Deviations]. Suppose $(\Omega, \mathcal{M}, P)$ is a probability space and X is a random variable on Ω(28.1.1.3) valued in $(\mathbb{R}, \mathrm{dm})$. Then

- If $\int_\Omega X \mathrm{d}P$ exists, it is called the **expected value** of X, denoted by $\mathbf{E}(X)$.
- The **variance** of X is defined to be

$$\mathrm{var}(X) \triangleq \sigma^2(X) \triangleq \begin{cases} \mathbf{E}(X - \mathbf{E}(X))^2 = \mathbf{E}(X^2) - (\mathbf{E}\, X)^2 & , \mathbf{E}(X^2) < \infty \\ +\infty & , \mathbf{E}(X^2) = \infty \end{cases}.$$

- The **standard deviation** of X is defined to be $\sigma(X) = \sqrt{\mathrm{var}(X)} \in [0, \infty]$.

Notice by Cauchy's inequality, if $\mathbf{E}(X^2) < \infty$, then $\mathbf{E}(X) < \infty$, so the definition makes sense. ⌟

Def. (28.1.1.6) [Covariances and Correlation Coefficients]. Suppose $(\Omega, \mathcal{M}, P)$ is a probability space and X, Y are real-valued random variables on Ω, then

- If $\mathbf{E}(X) < \infty, \mathbf{E}(Y) < \infty$, the **covariance** of X and Y is defined to be
$$\mathrm{cov}(X,Y) \stackrel{\triangle}{=} \mathbf{E}((X - \mathbf{E}(X))(Y - \mathbf{E}(Y))) = \mathbf{E}(XY) - \mathbf{E}(X) \cdot \mathbf{E}(Y).$$
- If $\mathbf{E}(X^2) < \infty$ and $\mathbf{E}(Y^2) < 0$, and $\mathrm{cov}(X) \neq 0, \mathrm{cov}(Y) \neq 0$, then the **correaltion coefficient** between X and Y is defined to be
$$r(X,Y) = \frac{\mathrm{cov}(X,Y)}{\sigma(X)\sigma(Y)}.$$

Notice $r(X,Y) \in [-1,1]$ if it is defined. ⌟

Proof: $r(X,Y) \in [-1,1]$ by Cauchy inequality because $L^2(\Omega)$ is a Hilbert space. □

Prop. (28.1.1.7) [Independence and Covariances]. Suppose $(\Omega, \mathcal{M}, P)$ is a probability space and X, Y are real-valued random variables on Ω that are independent, then $\mathrm{cov}(X,Y) = 0$. ⌟

Proof: Cf.[Dudley, P252]. □

Prop. (28.1.1.8). Suppose $(\Omega, \mathcal{M}, P)$ is a probability space and X, Y are real-valued random variables on Ω, then
$$\mathrm{var}(\sum_i X_i) = \sum_i \mathrm{var}(X_i) + 2 \sum_{1 \leq i < j \leq n} \mathrm{cov}(X_i, X_j).$$
In particular, if X_i are independent or pairwise-independent, by(28.1.1.7),
$$\mathrm{var}(X_1 + \ldots + X_n) = \sum_i \mathrm{var}(X_i).$$
⌟

Proof: We may first assume that $\mathbf{E}(X_i) = 0$ for each i, then
$$\mathrm{var}(\sum_i X_i) = \mathbf{E}((X_1 + \ldots + X_n)^2), \quad \mathrm{cov}(X_i, X_j) = \mathbf{E}(X_i X_j).$$
So the assertion is easy. □

2 Convergence of Laws and Central Limit Theorems

3 Conditional Expectations and Martingales

4 Stochastic Processes

Brownian Motion

Remark (28.1.4.1). The motion of a Brownian particle in $\mathbb{R}^N$ with a potential field U is described by a stochastic process $q = (q_1(t), \ldots, q_N(t)) \in \mathbb{R}^N$. (Which means that for each time t, there is a random variable $q(t) \in \mathbb{R}^N$ s.t. the dependence in t is regular in some sense.

All in all, the density of the probability that the motion with restrict $q(a) = \underline{a}, q(b) = \underline{b}$ is a smooth curve $\gamma : [a,b] \to \mathbb{R}^N$ is propositional to
$$e^{-S(\gamma)/\kappa}, \quad S(\gamma) = \int_a^b (\frac{1}{2}\dot{\gamma}^2 + U(\gamma)\mathrm{d}t$$
where κ is called the **diffusion coefficient**. ⌟

Remark (28.1.4.2). It follows from Kolmogorov's theorem that the stochastic process is determined by the **correlations functions**:

$$\operatorname{cor}(j_1, \ldots, j_n; t_1, \ldots, t_n) = \mathbf{E}\left(q_{j_1}(t_1) \cdot \ldots \cdot q_{j_n}(t_n)\right).$$

⌟

Proof: ? □

28.2 Information Theory

1 Cryptography

References are [Algebraic aspects of cryptography] and [Computational Complexity].

Def. (28.2.1.1) [Protocols]. A **protocol** is a multi−party algorithm, defined by a sequence of steps, specifying the actions required of two or more parties in order to achieve a specified objective ⌟

Public Key Cryptosystems

References are [AAG99].

Def. (28.2.1.2) [Keys]. public key cryptosystems use cyphers whose algorithm can be revealed to everyone without compromising the security of the cryptosystem.

In such cryptosystems, a set of specific parameters, called the **keys**, is supplemented together with the plaintext as an input to the cypher. The security of this cryptosystem depends entirely on the ecrecy of the keys. ⌟

Def. (28.2.1.3) [Key Establishment Protocols]. A **key establishment protocol** is a protocol whereby a key becomes available to two or more parties, for subsequent cryptographic applications.

The key establishment protocol is usually done over a reliable and secure channel. Once the key is established, subsequence communications involve sending cryptograms over a public channel which is vulnerable to total passive interception. ⌟

Algo. (28.2.1.4) [Public Key Cryptosystem]. A **public key cryptosystem** with signature works as follows:

- Each user A finds a encryption method E_A and a decryption method D_A of data, such that
$$E_A \circ D_A = D_A \circ E_A = \mathrm{id},$$
and both E_A and D_A are easy to compute, but it is hard or ineffective to know D_A from E_A.
- Each user A reveals E_A, and keeps D_A as secret.
- If user A wants to send message M to user B, he sends the message $E_B(D_A(M))$ to user B.
- If user B receives a message S from user A, he gets the plaintext $E_A(D_B(S))$.

⌟

Proof: The security of this system depends on the fact that it is ineffective to compute M from $E_B(D_A(M))$.

User B can prove the message is sent from user A because he has the texts M and $D_A(M)$, which is possible only because user A sent him the text $D_A(M)$, as it is hard to compute D_A.

User B cannot forge the message because he cannot find $D_A(M)$ from the message M. □

Algo. (28.2.1.5) [RSA Public Key cryptosystem, Rives-Shami- Adleman[RSA78]]. The (Rives-Shami- Adleman)**RSA public key cryptosystem** with signature works as follows:

- Use A chooses two large primes p, q using primality testing, and calculate $N = pq$.
- Then user A choose randomly an integer $2 \le e \le \varphi(N) - 2$ s.t. $(e, p) = (e, q) = 1$, and use the extended Euclid algorithm to find the inverse
$$d = \mathrm{rem}(e^{-1} (\mathrm{mod}\ \ \varphi(N))).$$

- User A reveals (N, e), which is called the **Public RSA key** of user A.
- The encryption method to user A is breaking a message to a series of positive integers (a_i) less than N, and then $E_A(a_i) = \text{rem}(a_i^e (\text{mod } N))$.
- The decryption method of user A is changing a text in the form of a series of positive integers (s_i) less than N to $D_A(s_i) = \text{rem}(s_i^d (\text{mod } N))$.
- Then use cryptosystem schemes as described in(28.2.1.4).

⌟

Proof: It is easy to show that $D_A \circ E_A = E_A \circ D_A = \text{id}$. By(28.2.1.4), the security of this cryptosystem depends on the difficulty of calculating d. It is shown that if d is know, then we can factor n effectively**?**, which is assumed to be difficult. □

Algo. (28.2.1.6) [Discrete Logarithm Key Establish Protocol, Diffie-Hellman1976]. Choose a $p \in \mathbf{P}$ and a primitive root g for p, then there is a key establish protocol as follows:

1. User A choose a random chosen $n \in \mathbb{Z}_+, n < p$, user B choose a random chosen $m \in \mathbb{Z}_+, n < p$.
2. Use A sends $g^n (\text{mod } p)$ to user B, and user B sends $g^m (\text{mod } p)$ to user A.
3. User A calculates $(g^n)^m (\text{mod } p)$, and user B calculates $(g^m)^n (\text{mod } p)$. Then user A and user B get a same element $s = g^{mn} (\text{mod } p)$.
4. Now User A can use this element s to send user B messages 1 bit a time.

⌟

Proof: The security of this cryptosystem is based on the difficulty of computing discrete logarithm over finite fields**?**. Because it is not feasible to determine any of $g^{mn} (\text{mod } p), g, m, n$ from $p, g^n (\text{mod } p)$ and $g^m (\text{mod } p)$. □

Algo. (28.2.1.7) [An Algebraic Key Establish Protocol, Anshel-Andhel-Goldfeld]. Let U, V be monoids and

$$\beta : U \times U \to V, \gamma_0, \gamma_1 : U \times V \to V$$

be feasibly computable functions satisfying the following properties:

- $\beta(x, y_1 y_2) = \beta(x, y_1)\beta(x, y_2)$.
- $\gamma_1(x, \beta(y, x)) = \gamma_2(y, \beta(x, y))$.
- Given $y_1, y_2, \ldots, y_k \in U$ and $\beta(x, y_1), \ldots, \beta(x, y_k)$, it is in general infeasible to determine the element x.

Then there is a key establish protocol as follows:

1. Publicly assign users A, B elements $S = \{s_1, \ldots, s_m\}$ and $T = \{t_1, \ldots, t_n\}$.
2. User A choose some $a \in S$ and transmit the elements $\beta(a, t_i)$ to user B.
3. User B chose some $b \in T$ and transmit the elements $\beta(b, t_i)$ to user A.
4. Then item1 guarantees that user A can calculate $\beta(b, a)$ and thus $\gamma_1(a, \beta(b, a))$. Similarly user B can calculate $\beta(a, b)$ and thus $\gamma_2(b, \beta(a, b))$. Then notice

$$\kappa = \gamma_1(a, \beta(b, a)) = \gamma_2(b, \beta(a, b))$$

is an established key.

But to extract an identical element, there are two cases: If there is a feasible algorithm to put every word in U in canonical form, then they get an identical element. Otherwise there are no canonical form algorithm but has a fast word identifying algorithm, then user A can choose a random word τ other than κ and then choose either send τ or κ to user B. Then user B can determine if this is κ or not, and receives a bit in this way.

⌟

Proof: The security of this cryptosystem is ? □

Remark (28.2.1.8). An example is given by $U = V = G \in \mathcal{G}\mathrm{rp}$ and

$$\beta(x,y) = x^{-1}yx, \quad \gamma_1(u,v) = u^{-1}v, \quad \gamma_2(u,v) = v^{-1}u.$$

Then

$$\kappa(a,b) = [a,b].$$

⌟

Algo. (28.2.1.9) [ECDHE Key Establishment Protocol]. ⌟

Algo. (28.2.1.10)[SIDH Key Establishment Protocol]. Using a supersingular elliptic curve $E/\mathbb{F}_{p^2}$. ⌟

Distributed Data Structures

Def. (28.2.1.11) [Secrete Sharings]. The goal of **secrete sharing** is to share a common secret in such a way that all of a group of people together can reconstruct the secret but any proper subset of them cannot do so. ⌟

Prop. (28.2.1.12)[Secrete Sharing via Lagrange Interpolation]. For $n \in \mathbb{Z}_{\geq 2}$, if we want to share a secrete among n peoples, we can choose a (large)field $k \in \mathtt{Field}$, and encode the information in a polynomial $f \in k[X]$ of degree $n-1$. Then we can choose distinct numbers $a_1, \ldots, a_n \in k$, and give each user i the number $f(a_i)$. In this way, it is easy to see that only all of them together can reconstruct the original information, through Lagrange interpolation.

The same method can be modified to store data among users that are robust to failure of some of them. ⌟

Elliptic Curves

2 Quantum Cryptography

Algo. (28.2.2.1) [Ekert's Key Establish Protocol]. The **Ekert's key establish protocol** is the following:

- A source emits a sequence of pair of entangled singlet half-spin particles to users A and B resp..
- For each particle, user A randomly choose from the three axis: $0, \pi/4, \pi/2$ to measure the spin of the particle.
- For each particle, user B randomly choose from the three axis: $\pi/4, \pi/2, 3\pi/4$ to measure the spin of the particle.
- User A and user B publish their data of axis of measurements, and determine the group particles that their axis of measurements are the same.

- Then they can use Bell's inequality on the group of particles with different axis of measurements as in [Eke91] to determine if there are eavesdroppers**?**.
- Finally, for the group of particles that they measured with the same axis of measurements, their result are opposite. Thus they get a sequence of same keys.

⌟

Proof: The security of this protocol follows from the no-cloning theorem(26.2.1.10) and also cannot measure a particle without disturbing the purity of the entanglement. Cf.[Neilson, Quantum Informations]. □

3 Error Correction

Def. (28.2.3.1)[Error Corrections]. Error correction are data structure designations that are used to eliminate the perturbations in the process of transmitting the data. ⌟

Prop. (28.2.3.2) [Error Correction via Lagrange Interpolation]. We can divide the data into n part and encode them in a polynomial f of degree $n-1$ over a (large)field $k\in\mathtt{Field}$. In this way, we can transmit the data $(u_i, f(u_i))$ for any $u_i\in k$. Then sending $n+l$ such pairs will be robust to the failure of losing l of them, by recovering the information via Lagrange's interpolation. ⌟

28.3 French to English Dictionary

1 A

- aide: help
- apres: after
- ans: years
- avoir: have
- aux: to the

2 B

-

3 C

- cas: case
- cet: this
- chaleureusement: warmly
- classifiant: classifying
- considere: consider
- corp: field
- courbe: curve

4 D

- dans: in
- d'apres: according to
- de: of, than
- des: of
- du: of
- d'une: of a

5 E

- en: in
- enonce: state
- est: is
- et: and
- etabli: established
- être: be

6 F

-

7 G

- générale: general
- grandes: large

8 H

-

9 I

- il y a: there is
- introduite: introduced
- indépendamment: independence

10 J

- Je: I

11 K

-

12 L

-
- la: the
- le: the
- les: the
- lignes: lines
- lues: read

13 M

-

14 N

-
- nous: we

15 O

-

16 P

-
- par: by, through
- peuvent: can
- plus: more
- pour: for, to
- preuve: proof
- principales: main
- presenterons: introduce
- prolonge: extended

17 Q

- qui: who

18 R

-
- recement: recently
- remercie: thank
- renvoyant: returning
- reste: rest

19 S

-
- sa: his
- ses: its, his, her
- schema: scheme
- strategie: strategy
- son: his
- sont: are
- suit: follows
- sur: on, about

20 T

- texte: text
- theoreme: theorem
- toroidale: toroidal
- traiter: treat

21 U

-
- un: a
- une: a

22 V

- variante: variant
- vectoriel: vector

23 W

-

24 X

-

25 Y

-

26 Z

-

Notations

This chapter consists of definitions and notations that are used often. These notations will be used throughout this book without referring, so if you are confused about some notation, you might find it here.

Chapter/Section/Subsection/... are called classes. Sometimes in the beginning of a class, there are notation assignments. They influence only the propositions contained in the same smallest class.

In any proposition, for any symbol appeared, there will only be two cases:

1. This symbol appear without assigned meanings. Then its meaning is defined in this chapter.
2. This symbol has been assigned meanings. Then its meaning may be different from the notations here(which I will try to avoid it from happening).

When they contradict(which I will try to avoid from happening), they have ascending priorities(e.g. notations assigned in the beginning of a chapter can be overrode by the notation assigned in the beginning of a section in this chapter), and have higher priorities than notation assignments in this chapter.

27 General

Notation (28.3.27.1).

- $\in$ is an abbreviation for "in" or "be/is/are in", depending on the syntax. So I will use this symbol more casually than usual.
- i is a chosen square root of -1 in $\mathbb{C}$.
- a.e. is an abbreviation for "all but finitely many".
- e.g. is an abbreviation for "for example".
- f.m. is an abbreviation for "finitely many".
- i.e. is an abbreviation for "which means".
- resp. is an abbreviation for "respectively".
- s.t. is an abbreviation for "such that".
- "Sufficiently large" means "is an integer greater than a given integer N_0 that only depends on the parameters defined before".

⌟

28 Set Theory

Notation (28.3.28.1) [Sets]. For $X \in \mathcal{S}\mathrm{et}$,

- Use $\#X$ instead of $|X|$(obsolete) to denote the cardinality of a set X.

- $\mathscr{P}(X)$ is the power set of X.
- To avoid confusion with other structures on sets, use bijection of sets instead of isomorphism of sets to indicate an isomorphism in $\mathcal{S}\mathrm{et}$.
- Use $U \subset X$ to indicate U is a subset of X. Use $U \subsetneq X$ ot indicate U is a proper subset of X.
- Use `\dutchcal` capital to represent a property on a set.
- If $\mathcal{P}$ is a property on X, then use $\{x \in X : \mathcal{P}(x)\}$ or $\{x \in X | \mathcal{P}(x)\}$ to indicate the subset of X defined by the property $\mathcal{P}$, depending on which avoids confusion better.
- If $S \subset \mathscr{P}(X)$, we say a property $\mathcal{P}$ holds for elements of Y sufficiently large if it holds for all elements of Y containing a fixed subset $S_0 \subset X$. Notice this definition is compatible with the definition of numbers being sufficiently large, by taking $X = \aleph_0$ and $Y = \mathbb{N} \subset \mathcal{P}(\aleph_0)$.
- Use `\mathtt` capital to represent a set that is doesn't form a category with good properties. For example, `GField` represents the set of global fields.
- If $f : X \to X$ is a self-map and $S \subset X$, then f is said to fix S or stablizes S if $f(S) \subset S$.
- For $n \in \mathbb{Z}_+$, use $\underline{a}^n$ to denote an n-tuple of elements $(a_1, \ldots, a_n)$. And the superscript n can be omitted sometimes.

⌟

Notation (28.3.28.2) [Common Sets].

- For $n \in \mathbb{N}$, $[n]$ is the set $\{0, 1, \ldots, n\}$.
- For $n \in \mathbb{Z}_+$, $[n]_+$ is the set $\{1, \ldots, n\}$.
- $\mathbb{Z}$ is the ring of integers.
- $\mathbb{Z}_+ \subset \mathbb{Z}$ is the commutative multiplicative monoid of positive integers.
- $\mathbb{Z}_- \subset \mathbb{Z}$ is the commutative multiplicative monoid of negative integers.
- $\mathbb{N} \subset \mathbb{Z}$ is the commutative multiplicative monoid of non-negative integers.
- $\mathbb{Q}$ is the field of rational numbers.
- $\mathbb{R}$ is the ordered valued field of real numbers.
- $\mathbb{R}_+$ is the ordered commutative multiplicative monoid of positive real numbers.
- $\mathbb{C}$ is the complete valued field of complex numbers.

⌟

29 Categories

Notation (28.3.29.1) [Categories].

- Use `\mathscr` capital for symbols representing a category.
- Use pr for morphisms that look like projections.

⌟

Notation (28.3.29.2) [Common Categories]. To avoid the set-theoretical issue that the class of all sets is not a set, we fix a cardinal κ, which will be given in prior in each situation, and define

- $\mathcal{S}\mathrm{et}$ to be the category of sets with cardinality$< \kappa$.
- $\mathcal{G}\mathrm{rp}$ to be the category of groups with cardinality$< \kappa$.

- $\mathcal{A}$b to be the category of Abelian groups with cardinality$< \kappa$.
- $\mathcal{G}$rp$^{\text{fin}}$ to be the category of finite groups. $\mathcal{A}$b$^{\text{fin}}$ to be the category of finite Abelian groups.
- $\mathcal{CA}$lg to be the category of commutative unital rings with cardinality$< \kappa$.
- For $p \in \mathbf{P}$, $\mathcal{CA}\text{lg}^p$ to be the category of commutative unital rings of characteristic p with cardinality$< \kappa$.
- `Field` to be the category of fields(3.2.1.3) with cardinality$< \kappa$.
- `Field`^{p} to be the category of fields of characteristic p(3.2.1.4) with cardinality$< \kappa$, where $p \in \mathbf{P} \cup \{0\}$.
- $\mathcal{T}$op to be the category of topological spaces with cardinality$< \kappa$.
- $\mathcal{T}$op $\mathcal{G}$rp to be the category of topological groups with cardinality$< \kappa$.
- $\mathcal{C}$at to be the category of categories with cardinality$< \kappa$.
- In generally, whenever we define the category of some objects, we mean the category of objects with cardinality$< \kappa$. This applies to the whole book.

⌟

Remark (28.3.29.3). If the cardinal κ in(28.3.29.2) is chosen to be too small, some construction in the categories won't be possible. For example, if you take $\kappa = 2$, then $\{\varnothing\} \coprod \{\varnothing\}$ is not definable in $\mathcal{S}$et. If you take $\kappa = \aleph$, then $\coprod_{\aleph} \{\varnothing\}$ is not definable in $\mathcal{S}$et.

So usually κ is taken to be a large enough strongly inaccessible cardinal (whose existence depends on the large cardinal axiom). But in specific cases we can take κ to be smaller to show some proposition is invariant of the axiom of large cardinals, for example the Weil conjecture(Deligne's theorem). ⌟

Notation (28.3.29.4) [Categories]. For $\mathcal{C}, \mathcal{D} \in \mathcal{C}$at, $A \in \mathcal{C}$,

- $\mathcal{C}/A$ or $\mathcal{C}_{/A}$ is the slice category of objects over A, $\mathcal{C}_{A/}$ is the slice category of objects under A.
- Func$(\mathcal{C}, \mathcal{D})$ is the category of functors from $\mathcal{C}$ to $\mathcal{D}$.
- $\mathcal{C}^{\text{op}}$ is the category with the arrows reversed.

⌟

Notation (28.3.29.5) [Monoidal Categories]. For a monoidal category $(\mathcal{C}, \otimes)$

- $\mathcal{C}^{opp}$ is the monoidal category with the same underlying category and the tensor product $\otimes$ reversed.

⌟

Homological Algebra

Notation (28.3.29.6) [Homological Algebras].

- Use `^\bullet` capital for symbols representing a complex over an Abelian category.
- Use K-groups instead of K-groups.

⌟

30 Topology

Notation (28.3.30.1) [Topological Spaces].

- cntd is an abbreviation for "connected".
- For a metric space X and $x \in X, \delta \in \mathbb{R}_+$, denote $U(x,\delta) = \{y \in X : d(x,y) < \delta\}, \mathbb{D}(x,\delta) = \{y \in X : d(x,y) \leq \delta\}$.
- For $X \in \mathcal{T}\mathrm{op}$, let X_0 to denote the closed points of X.

⌟

Notation (28.3.30.2) [Common Spaces].

- For $n \in \mathbb{Z}_+$, $\mathbb{S}^n$ is the unit sphere $\{x \in \mathbb{R}^n | ||x|| = 1\}$.
- For $n \in \mathbb{Z}_+$, $\mathbb{D}^n$ is the unit disk $\{x \in \mathbb{R}^n | ||x|| \leq 1\}$. $\mathbb{D}^2$ is also denoted by $\mathbb{D}$.
- For $n \in \mathbb{Z}_+$, $\mathbb{I}^n$ is the unit cube $\{x = (x_i) \in \mathbb{R}^n | |x_i| \leq 1\}$. $\mathbb{I}^1$ is also denoted by $\mathbb{I}$.
- For $n \in \mathbb{Z}_+, a < b \in \mathbb{R}_{\geq 0}$, $\mathbb{D}^n(a,b)$ is the annulus $\{x \in \mathbb{R}^n | a < ||x|| < b\}$. Similarly, we can define $\mathbb{D}^n[a,b), \mathbb{D}^n(a,b], \mathbb{D}^n[a,b]$.
- For $K \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$, $\mathbb{S}^\infty_{\mathbb{K}}$ is the unit sphere in $\mathbb{K}^\infty$.

⌟

31 Algebras

Notation (28.3.31.1) [Groups]. For $G \in \mathcal{G}\mathrm{rp}$,

- G_{ab} is the abelianization of G.
- Use $H \leq G$ to indicate that H is a subgroup of G.
- Use $H \trianglelefteq G$ to indicate that H is a normal subgroup of G.

⌟

Notation (28.3.31.2) [Free Groups].

- For $n \in \mathbb{Z}_+$, F_n is the free group generated by $[n-1]$.

⌟

Notation (28.3.31.3) [Abelian Groups]. For $G \in \mathcal{A}\mathrm{b}$,

- $G^\vee = \mathrm{Hom}(G, \mathbb{C}^\times)$ is the dual group of G. This applies to topological groups. Try not to use $\widehat{G}$, because this may be confused with the Langlands dual group or the completion.
-

⌟

Notation (28.3.31.4) [Linear Algebras]. For $R \in \mathcal{CA}\mathrm{lg}, m, n \in \mathbb{Z}_+$,

- For $V \in \mathcal{V}\mathrm{ect}/R$, V^* is the dual space of R.
- $\mathrm{Mat}(m \times n; R)$ is the group of $m \times n$-matrices with coefficients in R. $\mathrm{Mat}(m \times n; R)$ is also denoted by $\mathrm{Mat}(n, R)$.
- $GL(n,R)$ is the group of invertible elements in $\mathrm{Mat}(n;R)$.
- For $A \in \mathrm{Mat}(m,n;R)$, $A^t \in \mathrm{Mat}(n \times m; R)$ is the transpose of A.
- For $A \in GL(n,R)$, $A^{-1} \in GL(n,R)$ is the inverse of A. A^{-t} denotes $(A^{-1})^t = (A^t)^{-1}$.

⌟

Prop. (28.3.31.5) [Algebras]. For $R \in \mathcal{R}\text{ing}$,

- $\mathcal{M}\text{od}_R$ is the category of left R-modules.
- $\mathcal{A}\text{lg}_R$ is the the category of R-algebras.
- $\mathcal{R}\text{ing}_R$ is the category of associative unital R-algebras.
- $\mathcal{CR}\text{ing}_R$ is the category of commutative unital R-algebras.

┘

Notation (28.3.31.6) [Lie Algebras].

- Use `\mathfrak` lowercase for symbols representing a Lie algebra.

┘

32 Commutative Algebras

Notation (28.3.32.1) [Fields]. For $k \in \texttt{Field}$,

- $\operatorname{char} k$ is the characteristic of k.
- $\overline{k}$ is a fixed algebraic closure of k.
- k^{sep} is the separable closure of k in $\overline{k}$.
- k^{perf} is the perfect closure of k in $\overline{k}$.
- For a Galois extension k'/k, use $\text{Gal}(k'/k)$ instead of $\text{Gal}_{k'/k}$ or $G(k'/k)$ or $G_{k'/k}$ to denote the Galois group of k'/k.
- $\text{Gal}_k = \text{Gal}(k^s/k)$.
- $\mathtt{c} \in \text{Gal}(\mathbb{C}/\mathbb{R})$ is the complex conjugation. For $a \in \mathbb{C}$, $\mathtt{c}(a)$ is also denoted by $\overline{a}$.
- For $p \in \mathbf{P}$, $\mathbb{F}_p$ is the a fixed finite field of order p.
- For $p \in \mathbf{P}$, $\mathbb{F}_{p^r}$ is the fixed finite field of order p^r contained in $\overline{\mathbb{F}}_p$.
- $\mu(k)$ is the group of roots of unity in k.

┘

Notation (28.3.32.2) [Commutative Algebras].

- Use `\mathfrak` lowercase for a first prime ideals. Use `\mathfrak` uppercase for a prime ideal that is over a given prime ideal.
- Let $R \in \mathcal{CR}\text{ing}$ and f a non-zero-divisor in R, then use $R[\frac{1}{f}]$ instead of R_f to denote the localization ring at f.

┘

Notation (28.3.32.3) [Integral Rings]. For $R \in \mathcal{CR}\text{ing}$,

- Use "let (R, K) be an integral ring to indicate that R is an integral ring with fraction field K.
- $R^\times$ is the commutative monoid of non-zero elements in R.
- R^* is the commutative group of units of R.

┘

Notation (28.3.32.4) [Local Rings].

- Use "let $(R, K, \mathfrak{m}, k)$ be an integral local ring" to indicate that R is a local ring with maximal ideal $\mathfrak{m}$, $\kappa(\mathfrak{m}) = k$, and $\text{Frac}(R) = K$.

- DVR is the synonym for "discrete valuation ring".
- CDVR is the synonym for "complete discrete valuation ring".

⌟

Notation (28.3.32.5) [Dedekind Domains].

- Use `\mathcal` uppercase for symbols representing a Dedekind domain.?
- Use $\mathfrak{D}$ to denote differents of extensions of Dedekind domains.
- Use $\mathfrak{d}$ instead of δ to denote discriminants of extensions of Dedekind domains.

⌟

33 Algebraic Geometry

Notation (28.3.33.1) [Sheaves].

- Use `\mathcal` capital for symbols representing a sheaf of sets or a complex of sheaves of sets.
- Use `\mathscr` capital for symbols representing a sheaf of ∞-categories.

⌟

Notation (28.3.33.2) [Schemes]. Let $(X, \mathcal{O}_X) \in \mathcal{S}\mathrm{ch}$,

- For brevity, we can use X to denote the the scheme $(X, \mathcal{O}_X)$.
- Use $|X|$ to denote the underlying topological space, and $|X|_0$ to denote the closed points of $|X|$.
- Use `\mathbf` capital for a relative scheme.
- Use `\mathcal` capital for symbols representing an integral model.
- Use $\kappa(x)$ to denote the residue field of a point $x \in X$ instead of $k(x)$.
- Use $R(x)$ instead of $K(X)$ to denote the function field of an integral scheme X.
- Use $\mathcal{O}_X(D)$ instead of $\mathcal{L}(D)$ to denote the line bundle associated to a Cartier divisor D.

⌟

Notation (28.3.33.3) [Categories of Schemes]. Let $X \in \mathcal{S}\mathrm{ch}$,

- $\mathcal{S}\mathrm{ch}$ is the category of schemes.
- $\mathrm{N}\,\mathcal{S}\mathrm{ch}$ is the category of locally Noetherian schemes.
- For $R \in \mathcal{CA}\mathrm{lg}$, use $\mathcal{S}\mathrm{ch}\,/R$ to denote $\mathcal{S}\mathrm{ch}\,/\operatorname{Spec} R$.
- $\mathcal{S}\mathrm{ch}_{\mathrm{int}}$ is the category of integral schetmes.
- $\mathcal{S}\mathrm{ch}^{\mathrm{ft}}\,/X$ is the category of schemes of f.t. over X.
- $\mathcal{S}\mathrm{ch}^{\mathrm{loc.ft}}\,/X$ is the category of schemes locally of f.t. over X.
- $\mathcal{S}\mathrm{ch}^{\mathrm{f\acute{e}t}}\,/X$ is the category of schemes finite étale over X. In general, use superscript to denote relative properties w.r.t. X, and superscript to denote absolute properties.
- Use `\underline` for a functor on the category $\mathcal{S}\mathrm{ch}\,/X$.

⌟

Notation (28.3.33.4) [Morphisms of Schemes].

- Use i for a closed immersion and j for an open immersion.

- For $R \in \mathcal{CA}\mathrm{lg}, S \in \mathcal{CA}\mathrm{lg}_R, X \in \mathcal{S}\mathrm{ch}\,/R$, $X \times_{\operatorname{Spec} R} \operatorname{Spec} S$ is denoted by $X \otimes_R S$ or X_S.

⌟

Notation (28.3.33.5) [Modules on Schemes]. Let $(X, \mathcal{O}_X) \in \mathcal{S}\mathrm{ch}$,

- $\mathcal{M}\mathrm{od}(\mathcal{O}_X)$ is the category of $\mathcal{O}_X$-modules.
- $\mathcal{QC}\mathrm{oh}(X)$ is the category of Qco $\mathcal{O}_X$-modules.
- $\mathcal{C}\mathrm{oh}(X)$ is the category of coherent $\mathcal{O}_X$-modules.
- $\mathcal{C}\mathrm{oh}^{\mathrm{free}}(X)$ is the category of locally free sheaves on X.
- For $k \in \mathbb{N}$, $\mathcal{C}\mathrm{oh}^{\leq k}(X)$ is the category of coherent $\mathcal{O}_X$-modules with $\dim \operatorname{Supp}(\mathcal{F}) \leq k$.
- $D(X) = D(\mathcal{O}_X) = D(\mathcal{M}\mathrm{od}(\mathcal{O}_X))$.
- $D_{\mathcal{QC}\mathrm{oh}}(X) = D_{\mathcal{QC}\mathrm{oh}(X)}(\mathcal{M}\mathrm{od}(\mathcal{O}_X))$.
- $D_{\mathcal{C}\mathrm{oh}}(X) = D_{\mathcal{C}\mathrm{oh}(X)}(\mathcal{M}\mathrm{od}(\mathcal{O}_X))$.
- $\mathcal{D}(X) = \mathcal{D}(\mathcal{O}_X) = \mathcal{M}\mathrm{od}_{\mathcal{O}_X}(\mathcal{S}\mathrm{h}(X; \mathcal{D}(\mathbb{Z}))$.
- $\mathcal{D}_{\mathcal{QC}\mathrm{oh}}(X) = \mathcal{D}_{\mathcal{QC}\mathrm{oh}(X)}(\mathcal{M}\mathrm{od}(\mathcal{O}_X))$.
- $\mathcal{D}_{\mathcal{C}\mathrm{oh}}(X) = \mathcal{D}_{\mathcal{C}\mathrm{oh}(X)}(\mathcal{M}\mathrm{od}(\mathcal{O}_X))$.

⌟

Notation (28.3.33.6) [Group Schemes].

- μ is the group scheme $X \mapsto \mu(\Gamma(X, \mathcal{O}_X))$.

⌟

Notation (28.3.33.7) [Formal Schemes].

- Use mathfrak uppercase(aka. `\mfk`) for symbols representing a formal scheme that is usually not representable.

⌟

34 Analysis

Notation (28.3.34.1) [Numbers].

- π represents the smallest $x \in \mathbb{R}_+$ s.t. $e^{\mathrm{i}\,x} + 1 = 0$.
- γ_0 is the Euler's constant.

⌟

Notation (28.3.34.2) [Functions].

- for any positive-valued function $f : S \to \mathbb{R}_+$, I use $O(f)$ in an equation to denote that the difference of the other part of the equation is bounded by Cf, where $C \in \mathbb{R}_+$ is a constant that doesn't depend on any variables appearing in this equation.
- for any positive-valued function $f : S \to \mathbb{R}_+$, I use $\widetilde{O}(f)$ in an equation to denote that the difference of the other part of the equation is bounded by $Cf \cdot (\log f)^k$, where $C, k \in \mathbb{R}_+$ is a constant that doesn't depend on any variables appearing in this equation.
- For any functions $f, g : S \to \mathbb{C}$, we use $f \sim g$ or $f = \Theta(g)$ to denote $\{f = O(|g|)$ and $g = O(|f|)\}$.

⌟

Notation (28.3.34.3) [Real Analysis].

- $\sqrt{} : \mathbb{R}_+ \to \mathbb{R}_+$ is inverse of the function $\mathbb{R}_+ \to \mathbb{R}_+ : x \mapsto x^2$.
- For a differentiable function f, write $f^\backprime$ instead of f' to denote the derivative of f. For $p \in \mathbb{Z}_+$ and a p-th differentiable function f, write $f^{(p)}$ to denote the p-th derivative of f.
- Use $\mathscr{S}$ to denote the space of Schwartz-Bruhat functions.

⌟

Notation (28.3.34.4) [Complex Analysis].

- For $\alpha \in \mathbb{D}$, denote $\psi_\alpha(z) = \psi_\alpha(z) = \frac{\alpha - z}{1 - \overline{\alpha} z} \in \mathcal{M}(\mathbb{C})$.
- For $z \in \mathbb{C} \setminus (-\mathbb{R}_+)$, $\log z$ stands for the the principle branch of $\log z$, and for any $n \in \mathbb{Z}_+$, $\sqrt[n]{z}$ stands for $\exp(\frac{1}{n} \log z)$.
- For $n \in \mathbb{Z}_+$ and $\xi \in \mathbb{C}^n$, $e_\xi \in (\mathbb{C}^n)^\vee$ is the multiplicative character

  $$e_\xi : \mathbb{C}^n \to \mathbb{C}^* : x \mapsto \exp(2\pi\,\mathrm{i}(x, \xi)).$$

  Similarly, if $V \in \mathcal{V}\mathrm{ect}^n/\mathbb{C}$ and $\xi \in V^*$, then $e_\xi \in V^\vee$ is the multiplicative character

  $$e_\xi : \mathbb{C}^n \to \mathbb{C}^* : x \mapsto \exp(2\pi\,\mathrm{i}\langle x, \xi \rangle).$$

-

⌟

Notation (28.3.34.5) [Special Functions].

- $\Gamma(s) \in \mathcal{M}(\mathbb{C})$ is the Gamma function.
- $\zeta(s) \in \mathcal{M}(\mathbb{C})$ is the Riemann zeta function.
- $\wp(\tau) \in \mathcal{M}(\mathbb{C})$ is the Weierstrass $\wp$ function.

⌟

Notation (28.3.34.6) [Fourier Transforms].

- Use $f^\vee$ or $\mathscr{F}(f)$ to denote the Fourier transform of a function f on a locally compact Abelian group.
- Sometimes, use $f^\wedge$ to denote the inverse Fourier transform, which is just $(x \mapsto -x) \circ f^\vee$.

⌟

Notation (28.3.34.7) [Functional Analysis].

- Use `dutchcal` capital to denote a subset of the space of continuous functions on a topological space.

⌟

35 Geometry

Notation (28.3.35.1).

- Use Γ instead of Λ for a lattice.

⌟

36 Differential Geometry

Notation (28.3.36.1) [Manifolds].

-

⌟

Notation (28.3.36.2) [Lie Groups].

- For $\theta \in \mathbb{R}/(2\pi)$, denote $\kappa_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$.

⌟

37 Algebraic Number Theory

Notation (28.3.37.1) [Numbers].

- For $X \in \mathbb{N}$, $[X]$ is the set of non-negative integers no greater than X.
- For $X \in \mathbb{Z}_+$, $\{X\}$ is the set of positive integers no greater than X.
- $\mathbf{P}$ is the set of rational primes.
- $\mathbb{P}$ is the algebra consisting of periods.
- Don't use "#" as an abbreviation of "number" or "numbers".
- $\square$ is an abbreviation of "square" or "a square number". This is obsolete and I strongly suggest not using this notation, for one reason it doesn't specify square of what numbers, and for the other reason it may be confused with unrecognizable codes.
- For $n \in \mathbb{Z}^\times$, use $\mathbb{Z}/(n)$ instead of $\mathbb{Z}/n$ or $\mathbb{Z}/n\mathbb{Z}$.
- Use p to denote a prime number.
- Use ℓ instead of l or q to denote a second prime number <u>when p is present</u>.

⌟

Notation (28.3.37.2) [Common Functions]. For $n \in \mathbb{Z}_+$,

- $\phi(n) = \#(\mathbb{Z}/(n))^*$.

⌟

Notation (28.3.37.3) [Number Theory].

- Use ϖ instead of π to denote a uniformizer in a valuation ring to avoid confusion with the frequently used π.
- In number theory/arithmetic geometry, try to use F to denote a global field, K a CDVR and k a finite field or general field.
- For $p \in \mathbf{P}$, use $\overline{\mathbb{Q}_p}$ instead of $\overline{\mathbb{Q}}_p$ to denote the fixed algebraic closure of $\mathbb{Q}_p$.
- For $p \in \mathbf{P}$, $\mathbb{Q}_{p^n}$ is the unique unramified extension of $\mathbb{Q}_p$ of the degree n contained in $\overline{\mathbb{Q}}_p$, and $\mathbb{Z}_{p^r} = \mathcal{O}_{\mathbb{Q}_{p^n}}$.
- $\{\zeta_n, n \in \mathbb{Z}_+\}$ is a compatible system of roots of unity in $\overline{\mathbb{Q}}$, and $\zeta_4 = \mathrm{i}$.

⌟

Notation (28.3.37.4) [Global Fields]. For an extension of global fields E/F,

- F_0 is the constant field of F.

- Use `GField` to denote the set of global fields. Use `FField` to denote the set of global function fields, use `NField` to denote the set of global number fields. `GField` $/F$ is the set of global fields over F.
- $\mathcal{O}_F$ is the ring of integers of F.
- Σ_F is the set of places of F. Σ_F^{fin} is the set of finite places of F. Σ_F^{∞} is the set of infinite places of F. $\Sigma_F^{\mathbb{R}}$ is the set of real places of F, $\Sigma_F^{\mathbb{C}}$ is the set of complex places of F.
- For a finite extension L/F and $v \in \Sigma_F^{\mathrm{fin}}$, Σ_L^v is the set of finite places over v.
- For $x \in \mathcal{O}_F$, let $\Sigma_F^x \subset \Sigma_F^{\mathrm{fin}}$ denote the set of finite places dividing x.
- For $v \in \Sigma_F^{\mathrm{fin}}$, $(R_v, \mathfrak{m}_v, k_v)$ is the valuation ring of v, and $||v|| = \#k_v$.
- $\mathrm{Unr}_{E/F}, \mathrm{Ram}_{E/F}, \mathrm{Spl}_{E/F}$ is the set of finite places of F unramified, ramified, splitting in E resp.. $\mathrm{Spl}_{E/F/F_0}$ is the set of finite places of F_0 s.t. every place of F over p splits in E.

⌟

Notation (28.3.37.5) [Local Fields].

- Use `LField` to denote the set of local fields. Use p-`LField` to denote the set of p-adic local fields. Use p-`FField` to denote the set of p-adic number fields. Use p-`NField` to denote the set of p-adic number fields. Use `ArchField` to denote the set $\{\mathbb{R}, \mathbb{C}\}$.

⌟

Notation (28.3.37.6) [Analysis on Adeles and Ideles].

- For a local field K, $V \in \mathcal{V}\mathrm{ect}/K$, $\mathcal{S}(V)$ is the space of Bruhat-Schwartz Functions on V.
- For a global field F, V a finite free module over $\mathbf{A}_F$, $\mathcal{S}(V)$ is the space of Bruhat-Schwartz functions on V.

⌟

38 Arithmetic Geometry

Notation (28.3.38.1) [Perfectoid Spaces].

- Use old `\mathcal`(aka. `\mrs`) to denote adic spaces.

⌟

39 Representation Theory

Notation (28.3.39.1) [Representations]. Let $G \in \mathcal{T}\mathrm{op}\,\mathcal{G}\mathrm{rp}$, $L \in \mathcal{T}\mathrm{op}\,\mathcal{CR}\mathrm{ing}$,

- $\mathrm{Rep}_L(G)$ is the category of continuous representations of G with coefficients in L. $\mathrm{Rep}_{\mathbb{C}}(G)$ is also denoted by $\mathrm{Rep}(G)$.
- $\mathrm{Irr}_L(G)$ is the category of irreducible representations of G with coefficients in L. $\mathrm{Irr}_{\mathbb{C}}(G)$ is also denoted by $\mathrm{Irr}(G)$.
- $\mathrm{Rep}^{\mathrm{alg}}(G)$ is the category of smooth complex representations of G. $\mathrm{Irr}^{\mathrm{alg}}(G)$ is the category of irreducible smooth complex representations of G.
- For $(\rho, V) \in \mathrm{Rep}_L^{\mathrm{alg}}(G)$, let $(\rho^\vee, V^\vee)$ denote the contragradient representation: $\rho^\vee(g) = \rho(g)^{-t}$.

⌟

40 L-Functions

Notation (28.3.40.1) [L-Functions].

- Use ζ for a zata-function, i.e. a function that is usually a rational function in the indeterminant T.
- Use L for an L-function, i.e. a function that is usually a meromorphic function in $s \in \mathbb{C}$ with Euler products.

⌟

41 Combinatorics

Notation (28.3.41.1) [Combinatorics Numbers].

- For $n, m \in \mathbb{N}, m \leq n$,

$$n! = \begin{cases} 1 & , n = 0 \\ \prod_{k=1}^{n} k & , n > 0 \end{cases}, \quad \binom{n}{m} = \frac{n!}{(n-m)!m!}$$

- For $n, m \in \mathbb{N}, m \leq n$ and $p \in \mathbf{P}, q \in p^{\mathbb{Z}_+}$,

$$[n]_p = \begin{cases} 1 & , n = 0 \\ \frac{q^n - 1}{q - 1} & , n > 0 \end{cases}, \quad [n]!_q = \begin{cases} 1 & , n = 0 \\ \prod_{k=1}^{n} [k]_q & , n > 0 \end{cases}, \quad \begin{bmatrix} n \\ m \end{bmatrix} = \frac{[n]!_q}{[n-m]!_q [m]!_q}$$

⌟

Bibliography

[Ada04] C. C. Adams, The knot book. An elementary introduction to the mathematical theory of knots. Revised reprint of the 1994 original. American Mathematical Society, Providence, RI, 2004. xiv+307 pp.

[ALS91] A. Björner, L. Lovász and P. W. Shor, Chip-firing games on graphs. European J. Combin. 12 (1991), no. 4, 283–291.

[AAG99] I. Anshel, M. Anshel and D. Goldfeld, An algebraic method for public-key cryptography. Math. Res. Lett. 6 (1999), no. 3-4, 287–291.

[A-B95] J. L. Alperin and Rowen B. Bell, Groups and Representations.

[AKS04] M. Agrawal, N. Kayal and N. Saxena, Primes is in P. Ann. of Math. (2) 160 (2004), no. 2, 781–793.

[AGP02] M. Aguilar, S. Gitler and C. Prieto, Algebraic topology from a homotopical point of view.

[AGP94] W. R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers. Ann. of Math. (2) 139 (1994), no. 3, 703–722.

[Ahl78] L. V. Ahlfors, Complex analysis. An introduction to the theory of analytic functions of one complex variable. Third edition. International Series in Pure and Applied Mathematics. McGraw-Hill Book Co., New York, 1978. xi+331 pp.

[A-T92] N. Alon and M. Tarsi, Colorings and orientations of graphs. Combinatorica 12 (1992), no. 2, 125–134.

[And65] G. E. Andrew, A simple proof of Jacobi's triple product identity. Proceedings of the American Mathematical Society. 16 (2): 333.

[A-E45] N. H. Anning and P. Erdös, Integral distances. Bull. Amer. Math. Soc. 51 (1945), 598–600.

[Arn89] V. Arnol'd, Mathematical methods of classical mechanics. Translated from the Russian by K. Vogtmann and A. Weinstein. Second edition. Graduate Texts in Mathematics, 60. Springer-Verlag, New York, 1989. xvi+508 pp.

[A-T67] E. Artin and J. Tate, Class field theory. W. A. Benjamin, Inc., New York-Amsterdam 1968 xxvi+259 pp.

[Ati64] M. F. Atiyah, K-theory. Lecture notes by D. W. Anderson W. A. Benjamin, Inc., New York-Amsterdam 1967 v+166+xlix pp.

[Ati88] M. F. Atiyah, Topological quantum field theories. Inst. Hautes Études Sci. Publ. Math. No. 68 (1988), 175–186 (1989).

[A-M69] M. F. Atiyah and I. G. MacDonald, Introduction to commutative algebra. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969 ix+128 pp.

[B-D69] A. Baker and H. Davenport, The equations $3x^22 = y^2$ and $8x^27 = z^2$. Quart. J. Math. Oxford Ser. (2) 20 (1969), 129–137.

[B-N07] M. Baker and S. Norine, Riemann-Roch and Abel-Jacobi theory on a finite graph. Adv. Math. 215 (2007), no. 2, 766–788.

[Beh46] F. A. Behrend, On sets of integers which contain no three terms in arithmetical progression. Proc. Nat. Acad. Sci. U.S.A. 32 (1946), 331–332.

[Bei85] A. A. Beilinson, Higher regulators and values of L-functions. J Math Sci 30, 2036 – 2070 (1985).

[Ber02] Berger, p-adic Representations and differential equations, 2002.

[Ber93] V. G. Berkovich, ÉtaleCohomology for non-Archimedean analytic spaces, Inst. Hautes E ´tudes Sci. Publ. Math. (1993), no. 78, 5–161 (1994).

[B-Z76] I. N.Bernshtein and A. V. Zelevinskii, Representations of the Group $GL(n, F)$ where F is a Non-Archimedean Local Field.

[Bha17] B. Bhatt, Lecture notes for a class on Perfectoid Spaces.

[Bha17a] B. Bhatt, The Hodge-Tate Decomposition via Perfectoid Spaces, Arizona Winter School 2017.

[B-J11] B. Bhatt and A. J. de Jong, Crystalline Cohomology and De Rham Cohomology, https://www.math.columbia.edu/~dejong/papers/crystalline-comparison.pdf.

[Blo00] S. J. Bloch, Higher Regulators, Algebraic K-Theory, and Zeta Functions of Elliptic Curves.

[BGHZ] J.H. Bruinier, G. van der Geer, G. Harder and D. Zagier, The 1-2-3 of modular forms. Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004. Edited by Kristian Ranestad. Universitext. Springer-Verlag, Berlin, 2008. x+266 pp.

[BGR84] S. Bosch, U. Güntzer and R. Remmert, Non-Archimedean analysis, Grundlehren der Mathematischen Wissenschaften, Fundamental Principles of Mathematical Sciences, vol. 261, Springer-Verlag, Berlin, 1984, A systematic approach to rigid analytic geometry.

[BGK06] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order. J. London Math. Soc. (2) 73 (2006), no. 2, 380–398.

[B-G06] E. Bombieri and W. Gubler, Heights in Diophantine geometry. New Mathematical Monographs, 4. Cambridge University Press, Cambridge, 2006. xvi+652 pp.

[BLR90] S. Bosch, W. Lutkebohmert and M. Raynaud, Néron Models, Springer-Verlag, Berlin, 1990.

[Bog80] F. A. Bogomolov, Points of finite order on an abelian variety. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 44 (1980), no. 4, 782–804, 973.

[Bon11] C. Bonnafé, Representations of $SL_2(\mathbb{F}_q)$, 2011.

[Bor69] A. Borel, A. 1969. Introduction aux groupes arithmétiques. Publications de l'Institut de Mathématique de l'Universiteéde Strasbourg, XV. Actualités Scientifiques et Industrielles, No. 1341. Hermann, Paris.

[Bor94] F. Borceux. Handbook of categorical algebra. 1, volume 50 of Encyclopedia of Math- ematics and its Applications. Cambridge University Press, Cambridge, 1994. Basic category theory.

[Bor97] A. Borel, Automorphic Forms on $SL_2(\mathbb{R})$, 1997.

[Bor11] J. Borger, The basic geometry of Witt vectors, I: The affine case, Algebra and Number Theory 5 (2011), 231–285.

[Bor10] J. Le Borgne, Optimisation du théoréme d'Ax – Sen – Tate et application a'un calcul de cohomologie. galoisienne p-adique, Ann. Inst. Fourier, Grenoble 60 (2010), 1105–1123

[Bos15] S. Bosch, Lectures on Formal and Rigid Geometry.

[Bru13] J. Brundan, Quiver Hecke Algebras and Categorification.

[B-S02] M. Brin and G. Stuck, Introduction to Dynamical Systems.

[B-S14] B. Bhatt and P. Scholze, The pro-étale topology for schemes. Astérisque No. 369 (2015), 99–201.

[B-S19] B. Bhatt and P. Scholze, Prisms and prismatic cohomology, https://arxiv.org/abs/1905.08229(2019).

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves. II, J. Reine Angew. Math. 218 (1965), 79-108.

[B-K20] D. R. Heath-Brown and S. Konyagin, New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum. Q. J. Math. 51 (2000), no. 2, 221–235.

[Bug12] Y. Bugeaud, Distribution modulo one and Diophantine approximation. Cambridge Tracts in Mathematics, 193. Cambridge University Press, Cambridge, 2012. xvi+300 pp.

[Bum98] D. Bump, Automorphic Forms and Representations.

[Bus19] C.J. Bushnell, Arithmetic of Cuspidal Representations.

[B-K93] C. J. Bushnell and P. C. Kutzko, The Admissible Dual of GL(N) via Compact Open Subgroups, Annals of Math. Studies, vol. 129, Princeton University Press, 1993.

[C-G93] L. Carleson and T. W. Gamelin, Complex dynamics. Universitext: Tracts in Mathematics. Springer-Verlag, New York, 1993. x+175 pp.

[Car05] R. W. Carter, Lie algebras of finite and affine type. Cambridge Studies in Advanced Mathematics, 96. Cambridge University Press, Cambridge, 2005. xviii+632 pp.

[Car17] A. Caraiani, Lecture notes on Perfectoid Shimura Varieties.

[Car19] X. Caruso, An introduction to p-adic Period Rings.http://arxiv.org/abs/1908.08424v1(2019).

[Cas95] W. Casselman, Introduction to the the Category of Admissible Representations of p-Adic Groups (1995).

[C-S07] M. Chudnovsky and P. Seymour, The roots of the independence polynomial of a clawfree graph. J. Combin. Theory Ser. B 97 (2007), no. 3, 350–357.

[C-E72] V. Chvátal and P. Erdös, A note on Hamiltonian circuits. Discrete Math. 2 (1972), 111–113.

[C-G97] N. Chriss and Ginzburg, Representation Theory and Complex Geometry.

[Con06] B. Conrad, Chow's K/k-Image and K/k-Trace and the Lang-Néron Differential.

[C-G83] J. H. Conway and C. McA. Gordon, Knots and links in spatial graphs. J. Graph Theory 7 (1983), no. 4, 445–453.

[C-Z02] P. Corvaja and U. Zannier, A subspace theorem approach to integral points on curves. C. R. Math. Acad. Sci. Paris 334 (2002), no. 4, 267–271.

[CMOS] The Chicago manual of style, 16th edition, University Of Chicago Press, 2010.

[Nap] E. Chen, An Infinitely Large Napkin, https://web.evanchen.cc/napkin.html.

[C-S67] S. Chowla and A. Selberg, On Epstein's zeta-function. J. Reine Angew. Math. 227 (1967), 86–110.

[Cog00] J. W. Cogdell, Notes on L-Functions for GL_n.

[Con15] Various Seminar notes on Étale cohomology, Conrad.

[Cox13] D. A. Cox, Primes of the form x2+ny2. Fermat, class field theory, and complex multiplication. Second edition. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2013. xviii+356 pp.

[Dar99] H. Darmon, A proof of the full Shimura-Taniyama-Weil conjecture is announced. Notices Amer. Math. Soc. 46 (1999), no. 11, 1397–1401.

[DSV03] G. Davidoff, P. Sarnak and A. Valette, Elementary number theory, group theory, and Ramanujan graphs. London Mathematical Society Student Texts, 55. Cambridge University Press, Cambridge, 2003. x+144 pp.

[Del77] P. Deligne, Variétés de Shimura: interprétation modulaire, et techniques de construction de modéles canoniques, in Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 247–289, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979.

[Del79] P. Deligne, Valeurs de fonctions L et périodes d'intégrales. (French) With an appendix by N. Koblitz and A. Ogus. Proc. Sympos. Pure Math., XXXIII, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 313–346, Amer. Math. Soc., Providence, R.I., 1979.

[Del90] P. Deligne, Catégories tannakiennes, The Grothendieck Festschrift, Vol. II, 111–195, Progr. Math., 87, Birkhäuser Boston, Boston, MA, 1990.

[Deu58] M. Deuring, Die Klassenkörper der komplexen Multiplikation. (German) Enzyklopädie der mathematischen Wissenschaften mit Einschluss ihrer Anwendungen, Band I 2, Heft 10, Teil II (Article I 2, 23) B. G. Teubner Verlagsgesellschaft, Stuttgart 1958, 60 pp.

[D-M69] P. Deligne and D. Mumford, The irreducibility of the space of curves of given genus. Inst. Hautes Études Sci. Publ. Math. No. 36 (1969), 75–109.

[D-F99] P. Deligne and D. S. Freed, Classical field theory. Quantum fields and strings: a course for mathematicians, Vol. 1, 2 (Princeton, NJ, 1996/1997), 137 – 225, Amer. Math. Soc., Providence, RI, 1999.

[D-R99] P. Deligne and K. A. Ribet, Notes on supersymmetry (following Joseph Bernstein). Quantum fields and strings: a course for mathematicians, Vol. 1, 2 (Princeton, NJ, 1996/1997), 41–97, Amer. Math. Soc., Providence, RI, 1999.

[D-L76] P. Deligne and G. Lustig, Representations of reductive groups over finite fields. Ann. of Math. (2) 103 (1976), no. 1, 103–161.

[D-J92] D. Deutsch and R. Jozsa, Rapid solution of problems by quantum computation. Proc. Roy. Soc. London Ser. A 439 (1992), no. 1907, 553–558.

[DLLZ19] H. Diao, K.-W. Lan, R. Liu and X. Zhu, Logarithmic Riemann-Hilbert correspondences for rigid varieties. J. Amer. Math. Soc. 36 (2023), no. 2, 483–562.

[D-S05] F. Diamond and J. Shurman, A first course in modular forms. Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005. xvi+436 pp.

[Dic13] L. E. Dickson, Finiteness of the Odd Perfect and Primitive Abundant Numbers with n Distinct Prime Factors. Amer. J. Math. 35 (1913), no. 4, 413–422.

[Die17] R. Diestel, Graph theory. Fifth edition. Graduate Texts in Mathematics, 173. Springer, Berlin, 2017. xviii+428 pp.

[Dri85] V. G. Drinfeld, Hopf algebras and the quantum Yang-Baxter equation. Dokl. Akad. Nauk SSSR 283 (1985), no. 5, 1060–1064.

[Dri86] V. G. Drinfeld, Quantum groups. Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986), 798–820, Amer. Math. Soc., Providence, RI, 1987.

[Dri21] V. G. Drinfeld, Prismatization, https://arxiv.org/pdf/2005.04746.pdf (2021).

[Dud14] R. M. Dudley, Uniform central limit theorems. Second edition. Cambridge Studies in Advanced Mathematics, 142. Cambridge University Press, New York, 2014. xii+472 pp.

[D-P98] A. Dujella and A. Pethö, A generalization of a theorem of Baker and Davenport. Quart. J. Math. Oxford Ser. (2) 49 (1998), no. 195, 291–306.

[E-Z85] M. Eichler and D. Zagier, The theory of Jacobi forms. Progress in Mathematics, 55. Birkhäuser Boston, Inc., Boston, MA, 1985. v+148 pp.

[Eke91] A. K. Ekert, Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. 67 (1991), no. 6, 661–663.

[E-G17] J. Ellenberg and D. Gijswijt, On large subsets of Fnq with no three-term arithmetic progression. Ann. of Math. (2) 185 (2017), no. 1, 339–343.

[EGNO15] P. Etingof and S. Gelaki and D. Nikshych and V. Ostrik, Tensor Categories.

[EGZ61] P. Erdös; A. Ginzburg; A. Ziv, Theorem in the additive number theory. Bull. Res. Council Israel Sect. F 10F (1961), no. 1, 41–43.

[Elk73] R. Elkik, Solutions d'équations à coefficients dans un anneau hensélien, Annales Scientifiques de l'École Normale Superieure 6 (1973), 553–603.

[Elk87] N. Elkies, The Existence of Infinitely Many Supersingular Primes for Every Elliptic Curve over $\mathbb{Q}$, Inventiones Mathematicae, 89 (3) (1987), 561-567.

[Erd45] P. Erdös, On a lemma of Littlewood and Offord. Bull. Amer. Math. Soc. 51 (1945), 898–902.

[Erd45a] P. Erdös, Integral distances. Bull. Amer. Math. Soc. 51 (1945), 996.

[Erd46] P. Erdös, On sets of distances of n points. Amer. Math. Monthly 53 (1946), 248–250.

[Erd47] P. Erdös, Some remarks on the theory of graphs. Bull. Amer. Math. Soc. 53 (1947), 292–294.

[Erd59] P. Erdös, Graph theory and probability. Canadian J. Math. 11 (1959), 34–38.

[EKR61] P. Erdös, C. Ko and R. Rado, Intersection theorems for systems of finite sets. Quart. J. Math. Oxford Ser. (2) 12 (1961), 313–320.

[E-S6] P. Erdösand A. H. Stone, On the structure of linear graphs. Bull. Amer. Math. Soc. 52 (1946), 1087–1091.

[E-S35] P. Erdösand G. Szekeres, A combinatorial problem in geometry. Compositio Math. 2 (1935), 463–470.

[E-S02] J-H. Evertse and H. P. Schlickewei, A quantitative version of the absolute subspace theorem. J. Reine Angew. Math. 548 (2002), 21–127.

[Eve96] J-H. Evertse, An improvement of the quantitative subspace theorem. Compositio Math. 101 (1996), no. 3, 225–311.

[E-Z83] P. Erdösand E. Szemerédi, On sums and products of integers. Studies in pure mathematics, 213–218, Birkhäuser, Basel, 1983.

[E-T41] P. Erdösand P. Rurán, On a problem of Sidon in additive number theory, and on some related problems. J. London Math. Soc. 16 (1941), 212–215.

[Eti21] P. Etingof, notes on Lie Algebras and Lie Groups, 2021.

[Fak03] Questions on self maps of algebraic varieties. J. Ramanujan Math. Soc. 18 (2003), no. 2, 109–122.

[Fal86] G. Faltings, Finiteness Theorems for Abelian Varieties over Number Fields.

[Fal94] The general case of S. Lang's conjecture. Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), 175–182. Perspect. Math., 15, Academic Press, San Diego, CA, 1994.

[Fol99] G. B. Folland, Real analysis. Modern techniques and their applications. Second edition. Pure and Applied Mathematics (New York). A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1999. xvi+386 pp.

[Fol15] G. B. Folland, A course in Abstract Harmonic Analysis, Second edition.

[Fon94] J-M. Fontaine, Le corps des périodes p-adiques. (French) with an appendix by Pierre Colmez. Périodes p-adiques (Bures-sur-Yvette, 1988). Astérisque No. 223 (1994), 59–111.

[Fu11] L. Fu, Étale cohomology theory.

[Ful98] William Fulton, Intersection theory, 2ed., Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, vol. 2, Springer-Verlag, 1998.

[F-W94] G. Faltings and G. Wüstholz, Diophantine approximations on projective spaces. Invent. Math. 116 (1994), no. 1-3, 109–138.

[Gal95] F. Galvin, The list chromatic index of a bipartite multigraph. J. Combin. Theory Ser. B 63 (1995), no. 1, 153–158.

[Gan07] W. T. Gan, automorphic forms and automorphic representations.

[G-G13] J. von zur Gathen and J. Gerhard, Modern computer algebra. Third edition. Cambridge University Press, Cambridge, 2013. xiv+795 pp.

[G-M03] S. I. Gelfand and Y. I. Manin, Methods in Homological Algebra.

[G-S17] P. Gille and T. Szamuely, Central Simple Algebras and Galois Cohomology, second edition, 2017.

[Gol79] D. Goldfeld, Conjectures on elliptic curves over quadratic fields. Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), pp. 108–118, Lecture Notes in Math., 751, Springer, Berlin, 1979.

[G-H11] D. Goldfeld and J. Hundley, Automorphic Representations and L-Functions for the General Linear Group.

[G-J72] R. Godement and H. Jacquet, Zeta Functions on Simple Algebras.

[G-M16] C. Godsil and K. Meagher, Erdös-Ko-Rado theorems: algebraic approaches. Cambridge Studies in Advanced Mathematics, 149. Cambridge University Press, Cambridge, 2016. xvi+335.

[G-G78] C. D. Godsil and I. Gutman, On the matching polynomial of a graph. Algebraic methods in graph theory, Vol. I, II (Szeged, 1978), pp. 241–249, Colloq. Math. Soc. János Bolyai, 25, North-Holland, Amsterdam-New York, 1981.

[Gol74] D. Goldfeld, A simple proof of Siegel's theorem. Proc. Nat. Acad. Sci. U.S.A. 71 (1974), 1055.

[Gol85] D. Goldfeld, Gauss's class number problem for imaginary quadratic fields. Bull. Amer. Math. Soc. (N.S.) 13 (1985), no. 1, 23–37.

[Gre99] R. Greenberg, Iwasawa theory for elliptic curves. Arithmetic theory of elliptic curves (Cetraro, 1997), 51–144, Lecture Notes in Math., 1716, Springer, Berlin, 1999.

[G-H94] P. Griffith and J. Harris, Principles of algebraic geometry. Reprint of the 1978 original. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1994. xiv+813 pp.

[Gro89] B. H. Gross, Kolyvagin's work on modular elliptic curves. L-functions and arithmetic (Durham, 1989), 235 – 256, London Math. Soc. Lecture Note Ser., 153, Cambridge Univ. Press, Cambridge, 1991.

[Gro66] A. Grothendieck, On the de Rham cohomology of algebraic varieties. Inst. Hautes Études Sci. Publ. Math. No. 29 (1966), 95–103.

[Gro15] M. Groth, A short course on ∞-Categories, https://arxiv.org/abs/1007.2925v2.

[G-S83] D. Goldfeld and P. Sarnak, Sums of Kloosterman sums. Invent. Math. 71 (1983), no. 2, 243–250.

[G-P74] V. Guillemin and A. Pollack, Differential topology. Prentice-Hall, Inc., Englewood Cliffs, N.J., 1974. xvi+222 pp.

[Har20] G. H. Hardy, Note on a theorem of Hilbert. Math. Z. 6 (1920), no. 3-4, 314–317.

[HLP88] G. H. Hardy, Inequalities. Reprint of the 1952 edition. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1988. xii+324 pp.

[Har14] M. Harris, Automorphic Galois representations and the cohomology of Shimura varieties, Proceedings of the ICM 2014.

[Har77] Hartshorne, Algebraic Geometry.

[Hat02] A. Hatcher, Algebraic Topology.

[Hel78] S. Helgason, Differential Geometry, Lie Groups, and Symmetric Spaces, volume 80 of Pure and Applied Mathematics. Academic Press Inc., New York.(1978)

[H-M67] A. J. W. Hilton and E. C. Milner, Some intersection theorems for systems of finite sets. Quart. J. Math. Oxford Ser. (2) 18 (1967), 369–384.

[Hon68] T. Honda, Isogeny classes of abelian varieties over finite fields. J. Math. Soc. Japan 20 (1968), 83–95.

[Hub93] R. Huber, Continuous Valuations, Math. Z. 212 (1993), 455–477.

[Hub94] R. Huber, A Generalization of Gormal Schemes and Rigid Analytic Varieties, Math. Z. 217 (1994), 513–551.

[Hub96] R. Huber, Étale Cohomology of Rigid Analytic Varieties and Adic Spaces, Aspects of Mathematics, E30, Friedr. Vieweg & Sohn, Braunschweig, 1996.

[Hum90] James Humphreys, Reflection Groups and Coxeter Groups.

[H-K71] K. Hoffman and R. Kunze, Linear algebra. Second edition Prentice-Hall, Inc., Englewood Cliffs, N.J. 1971 viii+407 pp.

[Huy05] D. Huybrechts, Complex geometry. An introduction. Universitext. Springer-Verlag, Berlin, 2005. xii+309 pp.

[Huy16] D. Huybrechts, Lectures on K3 Surfaces.

[H-L10] D. Huybrechts and M. Lehn, The geometry of moduli spaces of sheaves. Second edition. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 2010. xviii+325 pp.

[Igu58] J. Igusa, Class Number of a Definite Quaternion with Prime Discriminant. Proc. Nat. Acad. Sci. U.S.A., 44:312-314, 1958.

[Iha81] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields. J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (1981), no. 3, 721–724 (1982).

[Jan92] U. Jannsen, Motives, Numerical Equivalence, and Semi-Simplicity. Inventiones mathematicae, 107(1):447-452, 1992.

[Jec03] T. Jech, Set theory. The third millennium edition, revised and expanded. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. xiv+769 pp.

[J-L70] H. Jacquet and R. P. Langlands, Automorphic forms on GL(2). Lecture Notes in Mathematics, Vol. 114. Springer-Verlag, Berlin-New York, 1970. vii+548 pp.

[Jon20] Jonathan Pottharst, Harder-Narasimhan Theory.

[Joy02] A. Joyal. Quasi-categories and Kan complexes. J. Pure Appl. Algebra, 175(1-3):207-222, 2002. Special volume celebrating the 70th birthday of Professor Max Kelly.

[Kat04] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms. Cohomologies p-adiques et applications arithmétiques. III. Astérisque No. 295 (2004), ix, 117–290.

[Kat73] N. M. Katz, p-adic properties of modular schemes and modular forms. In: Kuijk, W., Serre, JP. (eds) Modular functions of one variable III. Lecture Notes in Mathematics, vol 350. Springer, Berlin, Heidelberg.

[Ked19] K. S. Kedlaya, Sheaves, stacks, and shtukas, Perfectoid Spaces: Lecturesfrom the 2017 Arizona Winter School (Bryden Cais, ed.), Mathematical Surveys and Monographs, vol. 242, Amer. Math. Soc., Providence, RI, 2019, pp. 58–205.

[Ker] The Kerodon authors, Kerodon, https://kerodon.net.

[K-W09b] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture. I. Invent. Math. 178 (2009), no. 3, 485–504.

[K-W09c] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture. II. Invent. Math. 178 (2009), no. 3, 505–586.

[Kle94] S. L. Kleiman, The standard conjectures, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 3–20.

[Kle05] S. L. Kleinman, The Picard scheme.

[K-L15] K. S. Kedlaya and R. Liu, "Relative p-adic Hodge theory: Foundations", Astérisque 371 (2015).

[K-M74] N. Katz, W. Messing, Some consequences of the Riemann hypothesis for varieties over finite fields. Invent. Math. 23 (1974), 73-77.

[K-M85] N. M. Katz and B. Mazur, Arithmetic Moduli of Elliptic Curves,(1985).

[K-W01] R. Kiehl and R. Weissauer, Weil conjectures, perverse sheaves and l'adic Fourier transform. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, 42. Springer-Verlag, Berlin, 2001. xii+375 pp.

[Kna96] A. W. Knapp, Lie Groups beyond an introduction.

[Kos59] B. Kostant, The Three Dimensional Sub-Group and the Betti Numbers of a Complex Simple Lie Group, Amer. Jour. of Math., 81(1959), 973-1032.

[Kos63] B. Kostant, Lie Group Representations on Polynomial Rings, Amer. J. Math., 85(1963), 327-404.

[Kos65] B. Kostant, Eigenvalues of a Laplacian and Commutative Lie Subalgebras, Topology, 13(1965),147-159.

[Kos81] B. Kostant, A Lie Algebra Generalization of the Amitsur-Levitski Proposition, Adv. in Math., 40(1981), No. 2, 155-175.

[Kos97] B. Kostant, Clifford Algebra Analogue of the Hopf-Koszul-Samelson Proposition, the ρ-Decomposition, $C(g) = \operatorname{End} V_\rho \otimes C(P)$, and the $\mathfrak{g}$-Module Structure of $\wedge\mathfrak{g}$, Adv. in Math., 125(1997), 275-350.

[K-W09] B. Kostant and N. Wallach, On a Proposition of Ranee Brylinski, Contemporary Mathematics, 490(2009), 105-142.

[Kot85] R. E. Kottwitz, Isocrystals with additional structure, Composition Math. 56 (1985), no. 2, 201-220.

[Kub76] D. S. Kubert, Universal bounds on the torsion of elliptic curves, Proe. London Math. Soc. (3), 33 (1976), i93-237.

[Kur06] N. Kurokawa, Zeta functions over $\mathbb{F}_1$. Proc. Japan Acad. Ser. A Math. Sci. 81 (2005), no. 10, 180–184 (2006).

[Lam05] T. Y. Lam, Introduction to Quadratic Forms over Fields.

[Lan20] K.-W. Lan, An example-based introduction to Shimura Varieties.

[L-W54] S. Lang and A. Weil, Number of points of varieties in finite fields. Amer. J. Math. 76 (1954), 819–827.

[Lan73] S. Lang, Elliptic functions. With an appendix by J. Tate. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Amsterdam, 1973. xii+326 pp.

[Lan83] S. Lang, Fundamentals of Diophantine geometry. Springer-Verlag, New York, 1983. xviii+370 pp.

[Lan87] S. Lang, Elliptic functions. With an appendix by J. Tate. Second edition. Graduate Texts in Mathematics, 112. Springer-Verlag, New York, 1987. xii+326 pp.

[Lan93] S. Lang, Real and functional analysis. Third edition. Graduate Texts in Mathematics, 142. Springer-Verlag, New York, 1993. xiv+580 pp.

[Lan94] S. Lang, Algebraic number theory. Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994. xiv+357 pp.

[Lan95] S. Lang, Differential and Riemannian manifolds. Third edition. Graduate Texts in Mathematics, 160. Springer-Verlag, New York, 1995. xiv+364 pp.

[Lan99] S. Lang, Fundamentals of differential geometry. Graduate Texts in Mathematics, 191. Springer-Verlag, New York, 1999. xviii+535 pp.

[Lan02] S. Lang, Algebra. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002. xvi+914 pp.

[Lan70] R.P. Langlands, Problems in the Theory of Automorphic Forms, Lectures in modern analysis and applications III, Lectures Notes in Math., vol.170, Springer Verlag, 1970, pp. 18-86.

[L-B00] G. Laumon and L. Moret-Bailly, Champs algébriques. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 39. Springer-Verlag, Berlin, 2000. xii+208 pp.

[Lee13] John M. Lee, Introduction to smooth manifolds. Second edition. Graduate Texts in Mathematics, 218. Springer, New York, 2013. xvi+708 pp.

[Li04] 李忠, 复分析导引, 北京: 北京大学出版社, 2004.11.

[Liu02] Q. Liu, Algebraic Geometry and Arithmetic Curves, 2002.

[L-T65] J. Lubin, J. Tate, Formal Complex Multiplication in Local Fields, Annals of Mathematics (81), (1965), 380-387.

[L-S88] A. Lubotzky and P. R. Sarnak, Ramanujan graphs. Combinatorica 8 (1988), no. 3, 261–277.

[Lur09] J. Lurie, Higher Topos Theory, Annals of Mathematics Studies 170, Princeton University Press, Princeton (2009).

[Lur11] J. Lurie. Higher algebra. https://www.math.ias.edu/~lurie/, 2011. Preprint.

[Mac98] MacLane, S. 1998. Categories for the working mathematician, volume 5 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition.

[Mah57] K. Mahler, On the fractional parts of the powers of a rational number. II. Mathematika 4 (1957), 122–124.

[M-P05] Y. I. Manin and A. A. Panchishkin, Introduction to modern number theory. Fundamental problems, ideas and theories. Translated from the Russian. Second edition. Encyclopaedia of Mathematical Sciences, 49. Springer-Verlag, Berlin, 2005. xvi+514 pp.

[MSS15] A. W. Marcus, D. A. Spielman and N. Srivastava, Interlacing families I: Bipartite Ramanujan graphs of all degrees. Ann. of Math. (2) 182 (2015), no. 1, 307–325.

[MSS15a] A. W. Marcus, D. A. Spielman and N. Srivastava, Interlacing families II: Mixed characteristic polynomials and the Kadison-Singer problem. Ann. of Math. (2) 182 (2015), no. 1, 327–350.

[Mar02] D. Marker, Model theory. An introduction. Graduate Texts in Mathematics, 217. Springer-Verlag, New York, 2002. viii+342 pp.

[Mar06] D. Marker, A remark on Zilber's pseudoexponentiation. J. Symbolic Logic 71 (2006), no. 3, 791–798.

[Mat12] A. Mathew, "Simplicial commutative rings, I", http://math.uchicago.edu/~amathew/SCR.pdf.

[Mat80] H. Matsumura, Commutative Algebra, Second Edition.

[May99] J. P. May, A concise course in Algebraic Topology.

[Maz76] B. Mazur, Rational points on modular curves. Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 107–148. Lecture Notes in Math., Vol. 601, Springer, Berlin, 1977.

[Maz78] B. Mazur, Modular curves and the Eisenstein ideal. With an appendix by Mazur and M. Rapoport. Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186 (1978).

[M-T73] B. Mazur and J. Tate, Points of order 13 on elliptic curves, Inventiones math., 22 (I973), 4t-49.

[Mil08] J. S. Milne, Abelian varieties, version 2.0.

[Mil11] J. S. Milne, Shimura varieties and moduli.

[Mil12] J. S. Milne, Motives – Grothendieck's dream, Version 2.04.

[Mil13] J. S. Milne, Lie Algebras, Algebraic Groups and Lie Groups.

[Mil13b] J. S. Milne, Lectures on Étale Cohomology, Version 2.21.

[Mil17] J. S. Milne, Algebraic Groups.

[Mil17b] J. S. Milne, Introduction to Shimura Varieties.

[Mil17c] J. S. Milne, Modular Functions and Modular Forms.

[Mil17d] J. S. Milne, Algebraic Number Theory, Version 3.0.7.

[Mil20] J. S. Milne, Class Field Theory, Version4.03.

[Mil20b] J. S. Milne, Complex multiplication, Version0.10.

[Mil63] J. W. Milnor, Morse theory. Based on lecture notes by M. Spivak and R. Wells, Annals of Mathematics Studies, No. 51 Princeton University Press, Princeton, N.J. 1963 vi+153 pp.

[M-S74] J. W. Milnor and J. D. Stasheff, Characteristic classes. Annals of Mathematics Studies, No. 76. Princeton University Press, Princeton, N. J.; University of Tokyo Press, Tokyo, 1974. vii+331 pp.

[Mum70] D. Mumford, Abelian varieties, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Oxford University Press, Oxford, 1970, with appendices by C. P. Ramanujan and Yuri Manin.

[Mur93] J. P. Murre, On a conjectural filtration on the Chow groups of an algebraic variety. I. The general conjectures and some examples. Indag. Math. (N.S.) 4 (1993), no. 2, 177–188.

[Mor19] Sophie Morel, Adic Spaces.

[Mor15] Witte Morris, D. 2015. Introduction to Arithmetic Groups. Deductive Press, CA. https://arxiv.org/abs/math/0106063.

[Mun00] J. R. Munkres, Topology. Second edition. Prentice Hall, Inc., Upper Saddle River, NJ, 2000. xvi+537 pp.

[N-T91] Y. Nakkajima and Y. Taguchi, A generalization of the Chowla-Selberg formula. J. Reine Angew. Math. 419 (1991), 119–124.

[Nas50] J. F. Jr. Nash, Equilibrium points in n-person games. Proc. Nat. Acad. Sci. U.S.A. 36 (1950), 48–49.

[Nas51] J. F. Jr. Nash, Non-cooperative games. Ann. of Math. (2) 54 (1951), 286–295.

[Neu99] J. Neukirch, Algebraic number theory. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der mathematischen Wissenschaften, 322. Springer-Verlag, Berlin, 1999. xviii+571 pp.

[Neu15] J. Neukirch, Class field theory, the Bonn Lecture, Newly edited by Alexander Schmidt, Translated from the German by F. Lemmermeyer and W. Snyder, Online Edition 2.0, May 2015.

[Nit05] N. Nitsure, Construction of Hilbert and Quot schemes. Fundamental algebraic geometry, 105–137, Math. Surveys Monogr., 123, Amer. Math. Soc., Providence, RI, 2005.

[Ols69] J. E. Olson, A combinatorial problem on finite Abelian groups. I. J. Number Theory 1 (1969), 8–10.

[Ols16] M. Olsson, Algebraic Spaces and Stacks.

[Pap94] C. H. Papadimitriou, Computational complexity. Addison-Wesley Publishing Company, Reading, MA, 1994. xvi+523 pp.

[P-W06] J. Pila and A. J. Wilkie, The rational points of a definable set. Duke Math. J. 133 (2006), no. 3, 591–616.

[P0l11] P. Pollack, On Dickson's theorem concerning odd perfect numbers. Amer. Math. Monthly 118 (2011), no. 2, 161–164.

[Poo] B. Poonen, Practical suggestions For mathematical writing, https://math.mit.edu/~poonen/papers/writing.pdf.

[Poo14] B. Poonen, p-Adic interpolation of iterates. Bull. Lond. Math. Soc. 46 (2014), no. 3, 525-527.

[Poo15] B. Poonen, Tate's thesis, 2015.

[PriCom] The Princeton companion to mathematics. Edited by Timothy Gowers, June Barrow-Green and Imre Leader. Princeton University Press, Princeton, NJ, 2008. xxii+1034 pp.

[Pro76] C. Procesi, The invariant theory of $n \times n$ matrices, Adv.in Math,19(1976), 306-381.

[P-R94] V. Platonov and A. Rapinchuk, Algebraic Groups and Number Theory.

[Qui67] D. G. Quillen, Homotopical Algebra, Lecture Notes in Mathematics 43, Springer-Verlag, Berlin, 1967.

[RST93] N. Robertson, P.D. Seymour and R. Thomas, Linkless embeddings of graphs in 3-space. Bull. Amer. Math. Soc. (N.S.) 28 (1993), no. 1, 84–89.

[Roh84] D. E. Rohrlich, On L-functions of elliptic curves and cyclotomic towers. Invent. Math. 75 (1984), no. 3, 409–423.

[Rom07] S. Roman, Advanced Linear Algebra, third edition.

[Rab14] J. Rabinoff, The Theory of Witt Vectors, http://arxiv.org/abs/1409.7445v1.

[R-D70] F. K. C. Rankin and H. P. F. Swinnerton-Dyer, On the zeros of Eisenstein series. Bull. London Math. Soc. 2 (1970), 169–170.

[Rap95] M. Rapoport, Non-archimedean period domains, Proceedings of the International Congress of Mathematicians1994, 1995.

[Rub96] K. Rubin, Euler systems and modular elliptic curves. Galois representations in arithmetic algebraic geometry (Durham, 1996), 351 − 367, London Math. Soc. Lecture Note Ser., 254, Cambridge Univ. Press, Cambridge, 1998.

[Rub00] K. Rubin, Euler systems. Annals of Mathematics Studies, 147. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000. xii+227 pp.

[Rud76] W. Rudin, Principles of mathematical analysis. Third edition. International Series in Pure and Applied Mathematics. McGraw-Hill Book Co., New York-Auckland-Düsseldorf, 1976. x+342 pp.

[Rud91] W. Rudin, Functional analysis. Second edition. International Series in Pure and Applied Mathematics. McGraw-Hill, Inc., New York, 1991. xviii+424 pp.

[R-V99] D. Ramakrishna and R. J. Valenza, Fourier Analysis on Number Fields.

[RSA78] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Comm. ACM 21 (1978), no. 2, 120–126.

[Sch70] W. M. Schmidt, Simultaneous approximation to algebraic numbers by rationals. Acta Math. 125 (1970), 189–201.

[Sch96] W. M. Schmidt, Heights of points on subvarieties of $\mathbb{G}_m^n$. Number theory (Paris, 1993–1994), 157 – 187, London Math. Soc. Lecture Note Ser., 235, Cambridge Univ. Press, Cambridge, 1996.

[Sch12] P. Scholze, Perfectoid Spaces, Publications Mathématiques de l'IHÉS 116 (2012), 245–313.

[Sch13] P. Scholze, p-adic Hodge theory for rigid-analytic varieties, Forum Math. Pi 1 (2013), e1, 77pp.

[Sch13b] R. Schwartz, The Dehn-Sdler theorem explained, 2013.

[Sch17] P. Scholze, Étale Cohomology of Diamonds.

[Sen80] S. Sen, Continuous cohomology and p-adic Galois representations, Invent. Math., 62 (1980), 89–116.

[Ser55] J. -P. Serre, Faisceaux algébriques cohérents, Ann. of Math. 61 (1955), 197–278.

[Ser67] J. -P. Serre, Complex multiplication. Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 292–296, Thompson, Washington, D.C., 1967.

[Ser72] J. P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inventiones-math., 15 (I972), 259-33 I.

[Ser73] J. -P. Serre, A course in arithmetic. Translated from the French. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973. viii+115 pp.

[Ser77] J. -P. Serre, Linear Representations of Finite Groups.

[Ser79] J. -P. Serre, Local Fields, Graduate Texts in Mathematics 67, Springer-Verlag, New York-Berlin, (1979).

[Ser87] J.-P. Serre, Complex semisimple Lie algebras. Translated from the French by G. A. Jones. Reprint of the 1987 edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2001. x+74 pp.

[Sha74] J. Shalika, The Multiplicity One Theorem on GL(n), Ann. Math. 100 (1974), 171-193.

[Sha79] A. Shamir, How to share a secret. Comm. ACM 22 (1979), no. 11, 612–613.

[Sho94] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring. 35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994), 124 – 134, IEEE Comput. Soc. Press, Los Alamitos, CA, 1994.

[Sho97] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. 26 (1997), no. 5, 1484–1509.

[Sie35] C. L. Siegel, Über die analytische Theorie der quadratischen Formen. Ann. of Math. (2) 36 (1935), no. 3, 527–606.

[Sie42] C. L. Siegel, Iteration of analytic functions. Ann. of Math. (2) 43 (1942), 607–612.

[Sil11] A. Silverberg, Ranks "cheat sheet", (2011), http://math.uci.edu/~asilverb/connectionstalk.pdf.

[Sil86] J. H. Silverman, Heights and elliptic curves. Arithmetic geometry (Storrs, Conn., 1984), 253–265, Springer, New York, 1986.

[Sil99] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994. xiv+525 pp.

[Sil07] J. H. Silverman, The arithmetic of dynamical systems. Graduate Texts in Mathematics, 241. Springer, New York, 2007. x+511 pp.

[Sil16] J. H. Silverman, The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp.

[Sol00] J. Solymosi, Note on integral distances. U.S.-Hungarian Workshops on Discrete Geometry and Convexity (Budapest, 1999/Auburn, AL, 2000). Discrete Comput. Geom. 30 (2003), no. 2, 337–342.

[Sou04] C. Soulé, Les varétés sur le corps á un élément. Mosc. Math. J. 4 (2004), no. 1, 217–244, 312.

[Sta67] H. M. Stark, A complete determination of the complex quadratic fields of class-number one, Michigan Math. J. 14 (1967), 1-27.

[Sta] The Stacks Project Authors, Stacks Project, https://stacks.math.columbia.edu.

[S-S03] E. M. Stein and R. Shakarchi, Complex analysis. Princeton Lectures in Analysis, 2. Princeton University Press, Princeton, NJ, 2003. xviii+379 pp.

[Sul85] D. Sullivan, Quasiconformal homeomorphisms and dynamics. I. Solution of the Fatou-Julia problem on wandering domains. Ann. of Math. (2) 122 (1985), no. 3, 401–418.

[Suw19] M. Suwama, Supersingular primes for elliptic curves over $\mathbb{Q}$.

[S-W20] P. Scholze and J. Weinstein, Berkeley lectures on p-adic geometry. Annals of Mathematics Studies, 207. Princeton University Press, Princeton, NJ, 2020. x+250 pp.

[Sze79] E. Szeméredi, Regular partitions of graphs. Problémes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976), pp. 399–401, Colloq. Internat. CNRS, 260, CNRS, Paris, 1978.

[Sze97] L. A. Székely, Crossing numbers and hard Erdös problems in discrete geometry. Combin. Probab. Comput. 6 (1997), no. 3, 353–358.

[S-T83] E. Szemérediand Jr. W. T. Trotter, Extremal problems in discrete geometry. Combinatorica 3 (1983), no. 3-4, 381–392.

[Tar88] G. Tardos, Polynomial bound for a chip firing game on graphs. SIAM J. Discrete Math. 1 (1988), no. 3, 397–398.

[Tat65] J. Tate, Fourier analysis in number fields, and Hecke's zeta-functions. 1967 in Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965) pp. 305–347 Thompson, Washington, D.C.

[Tat65b] J. Tate, Algebraic cycles and poles of zeta functions. Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963) pp. 93–110 Harper & Row, New York 1965.

[Tat66] J. Tate, Endomorphisms of abelian varieties over finite fields. Invent. Math. 2 (1966), 134–144.

[Tat75] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil. Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 33–52. Lecture Notes in Math., Vol. 476, Springer, Berlin, 1975.

[Tat91] Conjectures on algebraic cycles in l-adic cohomology. Motives (Seattle, WA, 1991), 71–83, Proc. Sympos. Pure Math., 55, Part 1, Amer. Math. Soc., Providence, RI, 1994.

[Tho94] C. Thomassen, Every planar graph is 5-choosable. J. Combin. Theory Ser. B 62 (1994), no. 1, 180–181.

[Tin20] Y. Tian, Algebraic Geometry, Private Communication.

[T-W06] 谭小江和武胜健, 复变函数简明教程, 北京: 北京大学出版社, 2006.2.

[Vak17] R. Vakil, The Rising Sea: Foundations of Algebraic Geometry.

[Ver96] J.-L. Verdier, Des catégories dérivées des catégories abéliennes. With a preface by Luc Illusie. Edited and with a note by Georges Maltsiniotis. Astérisque No. 239 (1996), xii+253 pp. (1997).

[Vis08] A. Vistoli, Notes on Grothendieck Topologies, Fibered Categories and Descent Theory.

[Viz64] V. G. Vizing, On an estimate of the chromatic class of a p-graph. (Russian) Diskret. Analiz 1964, no. 3, 25–30.

[Viz76] V. G. Vizing, Coloring the vertices of a graph in prescribed colors. Diskret. Analiz 1976, no. 29, Metody Diskret. Anal. v Teorii Kodov i Shem, 3–10, 101.

[Voe02] V. Voevodsky, Motivic cohomology groups are isomorphic to higher Chow groups in any characteristic. Int. Math. Res. Not. 2002, no. 7, 351–355.

[Voi02] C. Voisin, Hodge theory and complex algebraic geometry. I. Translated from the French original by Leila Schneps. Cambridge Studies in Advanced Mathematics, 76. Cambridge University Press, Cambridge, 2002. x+322 pp.

[Voi03] C. Voisin, Hodge theory and complex algebraic geometry. II. Translated from the French by Leila Schneps. Cambridge Studies in Advanced Mathematics, 77. Cambridge University Press, Cambridge, 2003. x+351 pp.

[Wed14] T. Wedhorn, Introduction to Adic Spaces, http://www3.mathematik.tu-darmstadt.de/hp/algebra/wedhorn-torsten/lehre.html, 2014.

[Wei94] C. A. Weibel, An introduction to homological algebra. Cambridge Studies in Advanced Mathematics, 38. Cambridge University Press, Cambridge, 1994. xiv+450 pp.

[Wei19] C. A. Weibel, Vladimir Voevodsky. Notices Amer. Math. Soc. 66 (2019), no. 4, 526–533.

[Wei48] A. Weil, On some exponential sums. Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204–207.

[Weil50] A. Weil, Number-Theory and Algebraic Geometry, in Proceedings of the International Congress of mathematicians 1950 II, 1950.

[Wu09] 武胜健, 数学分析 • 第一册, 北京: 北京大学出版社, 2009.8.

[Wu10] 武胜健, 数学分析 • 第二册, 北京: 北京大学出版社, 2010.2.

[Yam22] Yuri Yamamoto, On Mackey Decomposition for locally profinite groups, https://arxiv.org/abs/2203.14262.

[Yao17] Zijian Yao, Notes on the Local Langlands Program for GL_n.

[Zag75] D. Zagier, Nombres de classes et formes modulaires de poids 3/2. (French. English summary) C. R. Acad. Sci. Paris Sér. A-B 281 (1975), no. 21, Ai, A883–A886.

[Zag89] D. Zagier, Polylogarithms, Dedekind zeta functions and the algebraic K-theory of fields. Arithmetic algebraic geometry (Texel, 1989), 391–430, Progr. Math., 89, Birkhäuser Boston, Boston, MA, 1991.

[Zag94] D. Zagier, Values of zeta functions and their applications. First European Congress of Mathematics, Vol. II (Paris, 1992), 497–512, Progr. Math., 120, Birkhäuser, Basel, 1994.

[Zag07] D. Zagier, The dilogarithm function. Frontiers in number theory, physics, and geometry. II, 3–65, Springer, Berlin, 2007.

[Zha18] Wei Zhang, Periods, cycles, and L-functions: a relative trace formula approach Proceedings ICM-2018, Rio.

[Zhou08] 周明强, 实变函数论, 2 版, 北京: 北京大学出版社, 2008.5.

[Zil05] B. Zilber, Pseudo-exponentiation on algebraically closed fields of characteristic zero. Ann. Pure Appl. Logic 132 (2005), no. 1, 67–95.

[Zin84] Zink, Cartier Theory of Commutative Formal Groups.

MORE TO BE ADDED

References are https://math.mit.edu/~zzyzhang/list.html.

Articles

2010-2014

J. Arthur, L-functions and automorphic representations, Proceedings of the ICM 2014.

M. Emerton, Completed cohomology and the p-adic Langlands program, Proceedings of the ICM 2014.

W. T. Gan, Theta correspondence: recent progress and applications, Proceedings of the ICM 2014.

V. Lafforgue, Introduction to chtoucas for reductive groups and to the global Langlands parameterization, Arxiv 2014.

G. Lusztig, Algebraic and geometric methods in representation theory, Arxiv 2014.

R. Kottwitz, B(G) for all local and global fields, Arxiv 2014.

D. Gaitsgory, A "strange" functional equation for Eisenstein series and miraculous duality on the moduli stack of bundles, Arxiv 2014.

M. Rapoport, E. Viehmann, Towards a theory of local Shimura varieties, Munster J. Math. 7 (2014), 273-326.

M. Rapoport, U. Terstiege, and S. Wilson. The supersingular locus of the shimura variety for GU(1, n 鋻 1) over a ramified prime. Mathematische Zeitschrift, 276(3-4):1165-1188, 2014.

S. S. Kudla and M. Rapoport. Special cycles on unitary Shimura varieties II: Global theory. J. Reine Angew. Math., 697:91-157, 2014.

Y. Liu, Relative trace formulae toward Bessel and Fourier-Jacobi periods of unitary groups, Manuscripta Mathematica, 145 (2014), 1-69.

L. Illusie, Grothendieck at Pisa: crystals and Barsotti-Tate groups, Colloquium de Giorgi 2013 and 2014, U. Zannier, ed., Scuola Normale Superiore di Pisa 2015, 79-107.

S. S. Kudla and M. Rapoport, An alternative description of the Drinfeld p-adic half-plane, Annales de l 鈥檌 nstitut Fourier 64, no. 3 (2014), 1203-1228.

W. Zhang, Automorphic period and the central value of Rankin-Selberg L-function, J. Amer. Math. Soc. 27 (2014), no. 2, 541-612.

W. Zhang, Fourier transform and the global Gan-Gross-Prasad conjecture for unitary groups. Ann. of Math. (2) 180 (2014), no. 3, 971-1049.

J. Thorne, Raising the level for GLn. Forum Math. Sigma 2 (2014), Paper No. e16, 35 pp.

Lapid, E., M 铆 nguez, A.: On a determintal formula of Tadi 麓 c. Am. J. Math. 136(1), 111-142 (2014).

K. Buzzard and T. Gee, The conjectural connections between automorphic representations and Galois representations, Automorphic forms and Galois representations. Vol. 1, London Math. Soc. Lecture Note Ser., vol. 414, Cambridge Univ. Press, Cambridge, 2014, pp. 135-187.

S. Lysenko, Geometric Waldspurger periods II, Arxiv 2013.

Spherical Varieties and Automorphic Representations, Oberwolfach Report 24/2013.

S. Sankaran, Unitary cycles on Shimura curves and the Shimura lift I, Doc. Math. 18 (2013), 1403-1464.

M. Rapoport, U. Tersteige, and W. Zhang, on the arithmetic fundamental lemma in the miniscule case. Compos. Math. 149 no. 10, (2013), 1631-1666.

P. Scholze, J. Weinstein, Moduli of p-divisible groups, Cambridge Journal of Mathematics 1 (2013), 145–237.

Andrew J. Blumberg, David Gepner, and Gon 莽 alo Tabuada, A universal characterization of higher algebraic K-theory, Geom. Topol. 17 (2013), no. 2, 733-838. MR 3070515.

X. Yuan, S. Zhang, W. Zhang. The Gross-Zagier formula on Shimura curves. No.184. Princeton University Press, 2013.

W. Zhang, Harmonic analysis for relative trace formula. Automorphic representations and L-functions, 681-696, Tata Inst. Fundam. Res. Stud. Math., 22, Tata Inst. Fund. Res., Mumbai, 2013.

E. Viehmann and T. Wedhorn, Ekedahl-Oort and Newton strata for Shimura varieties of PEL type, Math. Ann. 356 (2013), 1493-1550.

X. He, Normality and Cohen-Macaulayness of local models of Shimura varieties, Duke Math. J. 162 (2013), 2509-2523

M. Harris. L-functions and periods of adjoint motives. Algebra and Number Theory, (7):117-155, 2013.

Pappas G., Zhu X., Local models of Shimura varieties and a conjecture of Kottwitz, Invent. Math. 194, 2013, 147-254

D. Ben-Zvi and D. Nadler. Loop spaces and representations. Duke Math. J. 162 (2013), no. 9, 1587-1619.

A. Kret, Stratification de Newton des variétés de Shimura et formule des traces de Arthur-Selberg, PhD thesis, Université Paris-Sud, 2013.

Y. Liu, Arithmetic inner product formula for unitary groups, ProQuest LLC, Ann Arbor, MI, 2012. Thesis (Ph.D.), Columbia University.

B. H. Gross, Parahorics, 2012.

K-W. Lan and J. Suh, Vanishing theorems for torsion automorphic sheaves on compact PEL-type Shimura varieties. Duke Math. J. 161 (2012), no. 6, 1113-1170.

W. Zhang, On arithmetic fundamental lemmas, Invent. Math. 188(1), 197-252 (2012).

D. Maulik, B. Poonen, Neron-Severi groups under specialization. Duke Math. J. 161 (2012), no. 11, 2167–2206.

B. Howard, Complex multiplication cycles and Kudla 鈥揜 apoport divisors, Ann. of Math. (2) 176 (2012), 1097-1171.

D. Kazhdan, Y. Varshavsky, On endoscopic transfer of Deligne Lusztig functions, Duke Math. J. 161 (2012), no. 4, 675-732.

W. T. Gan, B. H. Gross, and D. Prasad, Symplectic local root numbers, central critical L values, and restriction problems in the representation theory of classical groups, Astérisque 346 (2012), 1-109.

A. Caraiani, Local-global compatibility and the action of monodromy on nearby cycles, Duke Math. J. 161 (2012), no. 12, 2311-2413.

Y. Sakellaridis, Spherical varieties and integral representations of L-functions, Algebra Number Theory 6 (2012), no. 4, 611-667.

U. Gortz, M. Hoeve, Ekedahl-Oort strata and Kottwitz-Rapoport strata, J. Algebra 351, pp. 160-174, 2012.

Y. Liu, On quadratic distinction of automorphic sheaves. Int. Math. Res. Not. IMRN 2012.

H. He, J. Hoffman. Picard groups of Siegel modular 3-folds and 胃-liftings. J. Lie Theory, 22(3):769-801, 2012.

Z. Yun, Langlands duality and global Springer theory, Compositio. Math. 148 (2012), 835-867.

Ulrich Görtz and Chia-Fu Yu, The supersingular locus in Siegel modular varieties with Iwahori level structure, Math. Ann. 353 (2012), no. 2, 465-498. MR2915544

O. Lorscheid, Algebraic groups over the field with one element, Mathematische Zeitschrift volume 271, pages 117-138.

David Lawrence Roe, The local langlands correspondence for tamely ramified groups, ProQuest LLC, Ann Arbor, MI, 2011. Thesis (Ph.D.) 鈥揌 arvard University. MR2898606

P. Scholze, The Langlands-Kottwitz method for the modular curve, Int. Math. Res. Not. 2011, no. 15, 3368–3425.

Z. Yun, The fundamental lemma of Jacquet-Rallis in positive characteristics, Duke Math. J. 156 (2011), no. 2, 167-228.

Ching-Li Chai and Frans Oort, Monodromy and irreducibility of leaves, Ann. of Math. (2) 173 (2011), no. 3, 1359-1396. MR 2800716

S. S. Kudla and M. Rapoport, Special cycles on unitary Shimura varieties I. Unramified local theory. Invent. Math., 184(3):629-682, 2011.

I. Vollaard, T. Wedhorn, The supersingular locus of the Shimura variety of GU(1,n-1) II, Invent. Math. 184 (2011), 591-627.

U. Terstiege. Intersections of arithmetic Hirzebruch-Zagier cycles. Math. Ann., 349(1):161-213, 2011.

C. Yu, Geometry of the Siegel modular threefold with paramodular level structure, Proc. Amer. Math. Soc. 139 (2011), no. 9, 3181-3190.

A. Minguez, Unramified representations of unitary groups, chapitre du livre 鈥淪 tabilisation de la formule des traces, variétés de Shimura, et applications arithmétiques-. Int. Press of Boston. (2011).

I. Vollaard, The supersingular locus of the Shimura variety for GU(1, s), Canad. J. Math. 62 (2010), no. 3, 668-720.

P. Boyer, Conjecture de monodromie-poids pour quelques variétés de Shimura unitaires, Compos. Math., 146 (2010), 367-403.

S. Harashita, Ekedahl-Oort strata contained in the supersingular locus and Deligne-Lusztig varieties. J. Algebr. Geom. 19(2010), no. 3, 419-438.

D. Gaitsgory and D. Nadler, Spherical varieties and Langlands duality, Mosc. Math. J. 10 (2010), no. 1, 65-137.

D. Arinkin, R. Bezrukavnikov, Perverse coherent sheaves, Mosc. Math. J. 10 (2010), no. 1, 3-29, 271.

B. Bhatt, Derived direct summands. Thesis (Ph.D.)Princeton University. 2010. 124 pp.

M. Hoeve, Stratifications on moduli spaces of abelian varieties and Deligne-Lusztig varieties, Ph.D. thesis, Universiteit van Amsterdam (2010).

U. Gortz, C.-F. Yu, Supersingular Kottwitz-Rapoport strata and Deligne-Lusztig varieties, J. Inst. Math. Jussieu 9 (2) (2010), 357-390.

2000s

W. Zhang, X. Yuan, S. Zhang, The Gross-Kohnen-Zagier theorem over totally real fields, Compositio Math

G. Chenevier, L. Clozel, Corps de nombres peu ramifiés et formes automorphes autoduales, J. Amer. Math. Soc. 22 (2009), 467-519.

W. Zhang, Modularity of generating functions of special cycles on Shimura varieties. Thesis (Ph.D.)Colum

T. Haines, Base change fundamental lemma for central elements in parahoric Hecke algebras, Duke Math. J. 149 (2009), pp. 569-643.

J. H. Bruinier and T. Yang, Faltings heights of CM cycles and derivatives of L-functions, Invent. Math. 177 (2009), no. 3, 631-681.

U. Gortz On the connectedness of Deligne-Lusztig varieties, Represent. Theory 13 (2009), 1-7.

G. Pappas and M. Rapoport, Local models in the ramified case, III. Unitary groups, J. Inst. Math. Jussieu 8 (2009), 507-564.

G. Pappas and M. Rapoport, Twisted loop groups and their affine flag varieties, Adv. Math. 219 (2008), 118-198. With an appendix by T. Haines and M. Rapoport.

T. Haines, M. Rapoport: On parahoric subgroups, Adv. Math. 219, 188-198, 2008.

E. Mantovan, On non-basic Rapoport-Zink spaces, Ann. Sci. 麓 Ec. Norm. Sup 麓 er. (4) 41 (2008), no. 5, 671-716.

T. Ikeda, Periods Of Automorphic Forms And L-Values (Automorphic Representations, Automorphic Forms, L-functions, and Related Topics), (2008), 1617: 138-147

R. Taylor and T. Yoshida, Compatibility of local and global Langlands correspondences, J. Amer. Math. Soc. 20 (2007), no. 2, 467-493.

Burgos Gil, J. I.; Kramer, J.; K 藹 uhn, U.: Cohomological arithmetic Chow rings. J. Inst. Math. Jussieu 6 (2007), 1-172.

E. Lau, On degenerations of D-shtukas, Duke Math. J. 140 (2007) 351-389.

J.I. Burgos Gil, J. Kramer, and U. K 篓 uhn, Cohomological arithmetic Chow rings, J. Inst. Math. Jussieu 6 (2007), no. 1, 1-172. MR 2285241

J. W. Morgan and G. Tian, Ricci flow and the Poincaré conjecture. Clay Mathematics Monographs, 3. American Mathematical Society, Providence, RI; Clay Mathematics Institute, Cambridge, MA, 2007. xlii+521 pp.

S. S. Kudla, M. Rapoport, and T. Yang, Modular forms and special cycles on Shimura curves, Annals of Mathematics Studies, vol. 161, Princeton University Press, Princeton, NJ, 2006.

R. Bezrukavnikov, Noncommutative Counterparts of the Springer Resolution, ICM 2006 Report.

T. Ito, Hasse invariants for some unitary Shimura varieties, Oberwolfach Report 28/2005 (C. Denniger, P. Schneider, and A. Scholl, eds.), Euro. Math. Soc. Publ. House, 2005, pp. 1565-1568.

T. Ito, Weight-monodromy conjecture for p-adically uniformized varieties, Invent. Math. 159 (2005), no. 3, 607-656.

E. Mantovan, On the cohomology of certain PEL-type Shimura varieties, Duke Math. J. 129 (2005), no. 3, 573-610.

O. Bultel, T. Wedhorn, Congruence relations for Shimura varieties associated to some unitary groups, J. Inst. Math. Jussieu 5 (2006), 229-261.

S. Lysenko, Moduli of metaplectic bundles on curves and theta-sheaves, Ann. Sci. Ecole Norm. Sup. (4) 39 (2006), no. 3, 415-466.

M. Kisin. Crystalline representations and F-crystals. In: Algebraic geometry and number theory. Springer, 2006, pp. 459-496.

J. Haines, Introduction to Shimura varieties with bad reduction of parahoric type. Harmonic analysis, the trace formula, and Shimura varieties, 583-642, Clay Math. Proc., 4, Amer. Math. Soc., Providence, RI, 2005.

G. Pappas, M. Rapoport- Local models in the ramified case. II: Splitting models.- , Duke Math. J. 127 (2005), no. 2, p. 193-250

Chia-Fu Yu. Basic points in the moduli spaces of PEL-type. MPIM-preprint 2005-113, 2005.

ARGOS Seminar on Intersections of Modular Correspondences, Held at the University of Bonn, Bonn, 2003-2004. Astrisque No. 312 (2007).

E. Lau, On generalized D-shtukas. PHD Dissertation, Rheinische Friedrich-Wilhelms-Universit 盲 t Bonn, Bonn, 2004.

Y. Varshavsky, Moduli spaces of principal F-bundles, Selecta Math. (N.S.) 10 (2004), no. 1, 131-166.

S. S. Kudla, M. Rapoport, and T. Yang. Derivatives of Eisenstein series and Faltings heights. Compos. Math., 140(4):887-951, 2004.

S. S. Kudla, Special Cycles and Derivatives of Eisenstein Series. In: Heegner Points and Rankin L-Series. Ed. by H. Darmon and S. W. Zhang. Mathematical Sciences Research Institute Publications. Cambridge University Press, 2004, pp. 243-270.

J. Marc Drezet, Luna 鈥檚 slice theorem and applications. Algebraic group actions and quotients, 39-89, Hindawi Publ. Corp., Cairo, 2004.

T. Saito, Weight spectral sequences and independence of l, J. Inst. Math. Jussieu 2 (2003), no. 4, 583-634.

F. Kato, An overview of the theory of p-adic uniformization. Appendix B of Y. Andre, Period Mappings and Differential Equations. From C to Cp, MSJ Memoirs, vol. 12. Mathematical Society of Japan, Tokyo (2003).

T. Konno, A note on the Langlands classification and irreducibility of induced representations of p-adic groups, Kyushu J. Math. 57 (2003), no. 2, 383-409,

N. Kr 盲 mer, Local models for Ramified unitary groups. Abh.Math.Semin.Univ.Hambg. 73, 67-80 (2003).

G. Faltings, Algebraic loop groups and moduli spaces of bundles. J. Eur. Math. Soc. (JEMS) 5 (2003), no. 1, 41-68.

L. Lafforgue, Chirurgie des grassmanniennes. (French) [Surgery on Grassmannians], CRM Monogr. Ser. 19, Amer. Math. Soc., Providence, 2003.

Tom Goodwillie, Calculus III, Taylor series, Geometry and Topology 7 (2003) 645-711.

J. H. Bruinier and M. Bundschuh. On Borcherds products associated with lattices of prime discriminant. Ramanujan J., 7(1-3):49-61, 2003. Rankin memorial issues.

S 酶 ren Have Hansen, Picard groups of Deligne-Lusztig varieties 鈥攚 ith a view toward higher codimensions, Beitr 娄 age Algebra Geom. 43 (2002), no. 1, 9-26. MR1913766

Th. Zink, The display of a formal p-divisible group, in: Cohomologies p-adiques et applications arithm 藺 etiques, I. Ast 藺 erisque 278 (2002), 127-248.

S. Kudla, Derivatives of Eisenstein series and generating functions for arithmetic cycles, Seminaire Bourbaki, 52 annee, 1999-2000, no. 876. Asterisque 276 (2002), 341-368.

P. Schneider and J. Teitelbaum. Locally analytic distributions and p-adic representation theory, with applications to GL2. Journal of the American Mathematical Society, 15(2):443-468, 2002.

T. Venkataramana, Lefschetz properties of subvarieties of Shimura varieties, in Current trends in number theory, pp. 265-270, Hindustan Book Agency, New Delhi, 2002.

S. DeBacker. Parametrizing nilpotent orbits via Bruhat-Tits theory. Ann. of Math. (2), 156(1):295-332, 2002.

L. Lafforgue, Chtoucas de Drinfeld et correspondance de Langlands, Invent. Math. 147 (2002), no. 1, 1-241.

E. Frenkel, D. Gaitsgory, and K. Vilonen. On the geometric Langlands conjecture. Journal of the American Mathematical Society, 15(2):367-417, 2002.

T. J. Haines and Ngo Bao Chau, Alcoves associated to special fibers of local models, Amer. J. Math. 124 (2002), no. 6, 1125-1152. MR 1939783

U. Görtz, On the flatness of models of certain Shimura varieties of PEL-type, Math. Ann. 321 (2001), no. 3, 689-727.

U. T. Hartl, Semi-stability and base change, Arch. Math. 77 (2001), 215-221.

M. Harris and R. Taylor, The geometry and cohomology of some simple Shimura varieties, with an appendix by V. Berkovich, Annals of Mathematics Studies, vol. 151 (Princeton University Press, Princeton, NJ, 2001).

D. Gaitsgory, Construction of central elements in the affine Hecke algebra via nearby cycles. Invent. Math, 144(2):253-280, 2001.

A. Bondal, D. Orlov. Reconstruction of a variety from the derived category and groups of autoequivalences. Compositio Math. 125 (2001), no. 3, 327-344.

H. Darmon, Integration on Hp 脳 H and arithmetic applications, Ann. of Math. 154(3) (2001), 589-639.

L. CLOZEL, H. OH, and E. ULLMO, Hecke operators and equidistribution of Hecke points, Invent. Math. 144 (2001), no. 2, 327-351.

W.-T. Gan, J. Hanke, and J.-K. Yu, On an exact mass formula of Shimura. Duke Math. J. 107 (2001), 103-133.

G. Pappas, On the arithmetic moduli schemes of PEL Shimura varieties, J. Algebraic Geom. 9 (2000), no. 3, 577-605.

S. Kudla and M. Rapoport, Height pairings on Shimura curves and p-adic uniformization. Invent. math., 142 (2000), pp. 153-222.

M. Rapoport, A positivity property of the Satake isomorphism. manuscripta math. 101, 153-166 (2000).

R. E. KOTTWITZ and M. RAPOPORT, Minuscule alcoves for GL(n) and GSp_{2n}, Manuscripta Math. 102 (2000), no. 4, 403-428.

1990s

Hu, J. (1999). Deformation to the normal bundle in arithmetic geometry (Order No. 9941488). Available from ProQuest Dissertations & Theses Global. (304573072).

J. P. Serre, André Weil. 6 May 1906-6 August 1998, Biographical Memoirs of Fellows of the Royal Society, Nov. 1999, Vol. 45 (Nov., 1999), pp. 520-529.

B. H. Gross, On the Satake isomorphism. In A. Scholl & R. Taylor (Eds.), Galois Representations in Arithmetic Algebraic Geometry (London Mathematical Society Lecture Note Series, pp. 223-238). Cambridge: Cambridge University Press, (1998).

L. Clozel and T. N. Venkataramana, Restriction of the holomorphic cohomology of a Shimura variety to a smaller Shimura variety, Duke Math. J. 95 (1998), 51-106.

M. Bertolini, H. Darmon, Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization, Invent. Math. 131, (1998), no.3, 453-491.

H. Stamm, On the reduction of the Hilbert-Blumenthal moduli scheme with $\Gamma_0(p)$ level structure, Forum Mathematicum 9 (1997), 405-455.

S. S. Kudla, Algebraic cycles on Shimura varieties of orthogonal type, Duke Math. J. 86 (1997), 39-78.

S. S. Kudla. Central derivatives of Eisenstein series and height pairings. Ann. of Math. (2), 146(3):545-646, 1997.

B. H. Gross, On the motive of a reductive group, Inventiones Mathematicae 130 (1997), no. 2, 287-313.

C. Simpson, The Hodge filtration on nonabelian cohomology, Algebraic geometry-Santa Cruz 1995, Proc. Sympos. Pure Math., vol. 62, Amer. Math. Soc., Providence, RI, 1997, pp. 217-281.

B. H. Gross, Reductive groups over Z, Invent. Math. 124 (1996), pp. 263-279.

J. P. Serre, Two letters on quaternions and modular forms (mod p), Israel J. Math. 95 (1996), 281-299.

A. J. de Jong, Smoothness, semi-stability and Alterations, Publ. Math. IHéS 83 (1996), 51-93.

A. Beilinson, V. Ginzburg, W. Soergel (1996). Koszul Duality Patterns in Representation Theory. Journal of the American Mathematical Society, 9(2), 473-527.

J. W. Morgan, The Seiberg-Witten equations and applications to the topology of smooth four-manifolds. Mathematical Notes, 44. Princeton University Press, Princeton, NJ, 1996. viii+128 pp.

A. J. de Jong, Crystalline Dieudonné module theory via formal and rigid geometry, Inst. Hautes 脡 tudes Sci. Publ. Math. (1995), no. 82, pp. 5-96.

M. J. Hopkins and B. H. Gross. Equivariant vector bundles on the Lubin-Tate moduli space. In Topology and representation theory (Evanston, IL, 1992), volume 158 of Contemp. Math., pages 23-88. Amer. Math. Soc., Providence, RI, 1994.

D. Vogan. The local Langlands conjecture. In: Representation theory of groups and algebras, Contemp. Math., vol. 145, pp. 305-379. American Mathematical Society, Providence, RI (1993).

B. H. Gross, K. Keating. On the intersection of modular correspondences, Inventiones Math. 112 (1993), 225-245.

Arxiv Mathematics (since February 1992)

J. Nekovar, On p-adic height pairings, séminaire de Théorie des Nombres, Paris 1990-1991, pages 127-202. Birkha 藹 user Boston, 1993.

P. Colmez, Périodes des vari ét és abéliennes á multiplication complexe, Ann. of Math. (2) 138 (1993), no. 3, 625-683.

R. Kottwitz, Points on Some Shimura Varieties Over Finite Fields, J. Amer. Math. Soc. 5 (1992), 373-444.

R. Kottwitz, On the p-adic representations associated to some simple Shimura varieties, Invent. Math. 108 (1992), 653-665.

S. Mildenhall, Cycles in a product of elliptic curves, and a group analogous to the class group, Duke Mathematical Journal 67 (2), 387-406, 1992.

J. F. Boutot and H. Carayol, Uniformisation p-adique des courbes de Shimura: les theoremes de Cerednik et de Drinfeld. Courbes modulaire et courbes de Shimura, Astérisque 196-197 (1991), pp. 45-158.

Tom Goodwillie, Calculus II, Analytic functors, K-Theory 5 (1991/92), no. 4, 295-332.

J. Arthur, A local trace formula, Inst. Hautes 艇 tudes Sci. Publ. Math. No. 73 (1991), 5-96.

P. Schneider and U. Stuhler. 鈥淭 he cohomology of p-adic symmetric spaces. In: Invent. Math. 105.1 (1991), pp. 47-122. issn: 0020-9910.

H. Gillet, C. Soule, Arithmetic intersection theory, Inst. Hautes Etudes Sci. Publ. Math. 72 (1990), 93-174.

S. Bloch, K. Kato, L-functions and Tamagawa numbers of motives. The Grothendieck Festschrift, Vol. I, 333-400, Progr. Math., 86, Birkhauser Boston, Boston, MA, 1990.

H. Carayol, Non-abelian Lubin-Tate theory, in: Automorphic Forms, Shimura Varieties, and L-functions (Academic Press, 1990), 15-39.

G. Lusztig. Intersection cohomology methods in representation theory, ICM 1990 report.

F. Shahidi, A proof of Langlands conjecture on Plancherel measures; complementary series for p-adic groups, Ann. Math. (2), 132 (1990), 273-330.

Tom Goodwillie, Calculus I, The first derivative of pseudoisotopy theory, K-Theory 4 (1990), no. 1, 1-27.

S. A. Mitchell. The Morava K-theory of algebraic K-theory spectra. K-Theory, 3(6):607-626, 1990.

1970-1980s

R. Pink. Arithmetical compactification of mixed Shimura varieties. PhD thesis, Bonner Mathematische Schriften, 1989.

J. Arthur, Unipotent automorphic representations: conjectures, Asterisque 171-172 (1989), 13-71.

D. Kazhdan and G. Laumon, Gluing of perverse sheaves and discrete series representations, Journ. of Geom. and Physics, 5 (1988), 63-120

I. Piatetski-Shapiro and S. Rallis, A new way to get Euler products, J. Reine Angew. Math. 392 (1988), 11

P. Deligne and D. Husemoller, Survey of Drinfeld modules, Contemporary Math, vol. 67, pp. 25-91, 1987.

G. Harder. Eisensteinkohomologie fu 藹 r Gruppen vom Typ GU(2, 1). Math. Ann., 278(1-4):563- 592, 1987.

B. H. Gross, W. Kohnen, D. Zagier, Heegner points and derivatives of L-series. II. Math. Ann. 278 (1987), no. 1-4, 497-562.

H. Gillet and C. Soulé, Intersection theory using Adams operations, Invent. Math. 90 (1987), no. 2, 243-277.

G. Laumon, Correspondance de Langlands géométrique pour les corps de fonctions, Duke Math. J. 54 (1987), no. 2, 309-359.

H. Jacquet, Sur un resultat de Waldspurger, Ann. Sci. Ecole Norm. Sup. (4) 19 (1986), no. 2, 185-229.

G. Harder, R. Langlands, M. Rapoport, Algebraische Zyklen auf Hilbert-Blumenthal-Flchen. J. Reine Angew. Math. 366 (1986), 53-120.

B. H. Gross, On canonical and quasi-canonical liftings. Inventiones mathematicae, 84(2):321-326, 1986.

Haastert, Burkhard, Die Quasiaffinit 盲 t der Deligne-Lusztig-Variet 盲 ten. (German) [The quasiaffinity of the Deligne-Lusztig varieties] J. Algebra 102 (1986), no. 1, 186-193.

W. van der Kallen, Descent for the K-theory of polynomial rings, Mathematische Zeitschrift 191 (1986), 405-415.

S. S. Kudla, Seesaw dual reductive pairs. In Automorphic forms of several variables (Katata, 1983), volume 46 of Progr. Math, pages 244-268. Birkha 藹 user Boston, Boston, MA, 1984.

P. Deligne, Intégration sur un cycle évanescent, Invent. Math. 76 (1984), no. 1, 129-143.

D. Vogan, G. Zuckerman, Unitary representations with nonzero cohomology, Compositio Math. 53 (1984), 51-90.

Bloch, S. Height pairings for algebraic cycles. J. Pure Appl. Algebra 34(2-3), 119-145 (1984). Proceedings of the Luminy Conference on Algebraic K-theory, Luminy, 1983.

O. Gabber, Sur la torsion dans la cohomologie l-adique d 鈥檜 ne variete, C. R. Acad. Sci., Paris, S 藿 er. I 297(1) (1983), p. 179-182.

J. S. Milne, The action of an automorphism of C on a Shimura variety and its special points, pp. 239-265. In Arithmetic and geometry, Vol. I. Birkha user Boston, Boston, MA, 1983.

D. J. Anick, A counterexample to a conjecture of Serre, Ann. of Math. 115 (1982); 1-33.

A. A. Beilinson, J. Bernstein, and P. Deligne. Faisceaux pervers. In Analysis and topology on singular spaces, I (Luminy, 1981), volume 100 of Astérisque, pages 5-171. Soc. Math. France, Paris, 1982.

S. Ralllis, Langlands' Functoriality and Weil representation, American Journal of Mathematics, Vol 104, No.3 (Jun. 1982), pp. 469-515.

J. Langlands and Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier. J. Math. Pures Appl. (9), 60(4):375-484, 1981.

J. Arthur, Automorphic Representations and Number Theory, Canadian Mathematical Society, Conf. Proc., Volume 1 (1981)

P. Deligne, La conjecture de Weil: II, Publications Mathématiques de l'IH 脡 S, Tome 52 (1980) , pp. 137-252.

STEVEN L. KLEIMAN, Relative duality for quasi-coherent sheaves Compositio Mathematica, tome 41, no 1 (1980), p. 39-60.

Kottwitz, R. E. (1980). Orbital Integrals on GL(3). American Journal of Mathematics, 102(2), 327-384.

D. Kazhdan, G. Lusztig, Schubert varieties and Poincare duality. Geometry of the Laplace operator (Proc. Sympos. Pure Math., Univ. Hawaii, Honolulu, Hawaii, 1979), pp. 185-203, Proc. Sympos. Pure Math., XXXVI, Amer. Math. Soc., Providence, R.I., 1980.

D. Eisenbud, Homological algebra on a complete intersection, with an application to group representations, Trans. Amer. Math. Soc. 260 (1980), 35-64.

R. Howe, Wave Front Sets of Representations of Lie Groups. In Automorphic Forms, Representation Theory and Arithmetic (Bombay, 1979), 117-40. Tata Institute of Fundamental Research Studies in Mathematics 10.

D. Kazhdan, G. Lusztig, Representations of Coxeter groups and Hecke algebras, Inventiones Mathematicae, 53 (2) (1979), 165-184.

P. Cartier, Representations of a p-adic groups: a survey, in Automorphic forms, representations and L-functions, Proc. Symp. Pure Math. Am. Math. Soc., Corvallis/Oregon 1977, Proc. Symp. Pure Math. 33 (1979), Part 1, 111-155.

J. Tits, Reductive groups over local fields, in Automorphic forms, representations and L-functions, Proc. Symp. Pure Math. Am. Math. Soc., Corvallis/Oregon 1977, Proc. Symp. Pure Math. 33 (1979), Part 1, 29-69.

Harish-Chandra, Admissible invariant distributions on reductive p-adic groups, in Lie Theories and their Applications (Proc. Ann. Sem. Canad. Math. Congr., Queen's Univ., Kingston, Ont., 1977), Queen 鈥檚 Papers in Pure Appl. Math. 48, Queen 鈥檚 Univ., Kingston, Ont., 1978, pp. 281-347.

D. Kazhdan. Some applications of the Weil representation. J. Analyse Mat., 32 :235-248, 1977.

D. Mumford, Hirzebruch 鈥檚 proportionality theorem in the noncompact case, Invent. Math. 42 (1977), 239-272.

M.-F. Vigneras, Series theta des formes quadratiques indefinies. In: Modular functions of one variable VI, Springer Lecture Notes 627 (1977), 227-239.

D. Sullivan, Infinitesimal computations in topology. Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 269–331 (1978).

G. Lusztig, Coxeter orbits and eigenspaces of Frobenius. Invent. Math., 38(2):101-159, 1976.

A. Borel, Admissible representations of a semi-simple group over a local field with vectors fixed under an Iwahori subgroup, Invent. Math. 35 (1976), 233-259.

V. G. Drinfeld, Coverings of p-adic symmetric domains, Funkcional. Anal. i Prilo 藝 zen. 10 (1976), no. 2, 29-40 (Russian).

R. Langlands, Some contemporary problems with origins in the Jugendtraum, Mathematical developments arising from Hilbert problems (De Kalb 1974), Proc. Sympos. Pure Math. XXVIII, Amer. Math. Soc., pp. 401-418, 1976.

F. Oort. Subvarieties of moduli spaces. Invent. Math., 24:95-119, 1974.

P. Deligne. Théorie de Hodge, III. Inst. Hautes Etudes Sci. Publ. Math., 44:5-77, 1974.

P. Deligne. La conjecture de Weil. I. Inst. Hautes Etudes Sci. Publ. Math., (43):273-307, (1974).

P. Deligne. and M. Rapoport, Les schémas de modules de courbes elliptiques, in Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 143–316. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

L. Illusie, Complexe Cotangent et Déformation I, II, Lecture Notes in Mathematics 239, 283, Springer-Verlag, 1971, 1972.

P. Deligne, Théorie de Hodge, II. Publications Mathématiques de L 鈥檌 nstitut des Hautes Scientifiques 40, 5-57 (1971).

1950-1970

Walter L. Baily, Jr., An exceptional arithmetic group and its Eisenstein series, Ann. of Math. (2) 91 (1970), 512-549.

P. Deligne, Theoreme de Lefschetz et criteres de degenerescence de suites spectrales. Publications Math ematiques de l 鈥檌 HES 35.1 (1968): 107-126.

R. Godement, Introduction a la Theorie de Langlands, Seminaire N. Bourbaki, 1968, exp. no 321, p. 115-144.

A. Grothendieck, Crystals and the de Rham cohomology of schemes. In Dix Exposes sur la Cohomologie des Schemas, volume 3 of Advanced Studies in Pure Mathematics, pages 306-358. North-Holland, Amsterdam, 1968.

J. Tate, p-divisible groups, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 158-183.

P. Deligne, Cohomologie 脿 support propre et construction du foncteur $f^!$, Appendix to Hartshorne, Residues and duality, Lecture Notes in Math., Vol. 20, Springer, Berlin, 1966.

M. Lazard, Groupes analytiques p-adiques, Publications Mathématiques de l'IH 脡 S, Tome 26 (1965), pp. 5-219.

A. Weil, Sur certains groupes d'operateurs unitaires, Acta Math. 111 (1964), 143-211.

G. E. Wall. On the conjugacy classes in the unitary, symplectic and orthogonal groups. J. Aust. Math. Soc., 3:1-62, 1963.

R. Jacobowitz, Hermitian Forms Over Local Fields. American Journal of Mathematics, 84(3), (1962), 441-465.

J. P. Serre, Sur la topologie des variétés algébriques en caractéristique p, Symposion Internacional de topologia algebraica (1958), pp. 24-53.

M. Lazard, Sur les groupes de Lie formels 脿 un param 猫 tre, Bulletin de la Société Mathématique de France, Tome 83 (1955), pp. 251-274.

Classical books

Hardy, G. H.; Wright, E. M. An introduction to the theory of numbers. Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, Oxford, 2008. xxii+621 pp.

M. Harris, R. Taylor, The geometry and cohomology of some simple Shimura varieties, Annals of Mathematics Studies, vol. 151, Princeton University Press, Princeton, NJ, 2001.

R. Kiehl and R. Weissauer, Weil Conjectures, Perverse Sheaves and l-adic Fourier Transform, (2001).

J. Kollar, S. Mori, Birational Geometry of Algebraic Varieties, (1998).

N. Chriss, V. Ginzburg, Representation theory and complex geometry, 1997.

G. Laumon, Cohomology of Drinfeld modular varieties, (1996).

L. C. Washington, Introduction to Cyclotomic Fields, 1996-12-5.

Casselman, note on p-adic groups, 1995.

S. Mac Lane, I. Moerdijk, Sheaves in Geometry and Logic - A first introduction to topos theory, Springer Verlag, 1992.

P. Deligne, J. S. Milne, A. Ogus, K. Shih, Hodge cycles, motives, and Shimura varieties, LNM 900, (1982).

A. Borel, W. Casselman (Editors), Automorphic Forms, Representations and. L-Functions, Parts 1 and 2, Corvallis proceedings (1979).

N. Koblitz, P-adic Numbers, P-adic Analysis, and Zeta-Functions, (1977).

S. G. Langton, Valuative Criteria for Families of Vector bundles on Algebraic varieties, Annals of Mathematics Vol.101. No.1(1975). pp.88-110.

A. Bousfield, D. Kan, Homotopy Limits, Completions and Localizations, (1972).

Shimura, Goro, Introduction to the arithmetic theory of automorphic functions. Reprint of the 1971 original. Publications of the Mathematical Society of Japan, 11. Kanô Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994. xiv+271 pp.

M. Raynaud, Anneaux locaux henséliens, (1970).

D. Quillen, homology of commutative rings, unpublished, MIT 1968.

Flatland: A Romance of Many Dimensions, (1884).

Index